

JINDŘICH BEČVÁŘ

LINEÁRNÍ ALGEBRA



matfyzpress

PRAHA 2010

Všechna práva vyhrazena. Tato publikace ani žádná její část nesmí být reprodukována nebo šířena v žádné formě, elektronické nebo mechanické, včetně fotokopíí, bez písemného souhlasu vydavatele.

© Jindřich Bečvář, 2010

© MATFYZPRESS, vydavatelství Matematicko-fyzikální fakulty
Univerzity Karlovy v Praze, 2010

ISBN 978-80-7378-135-4

ISBN 80-86732-57-6 (třetí vydání)

ISBN 80-85863-92-8 (druhé vydání)

ISBN 80-85863-61-8 (první vydání)

V lineární algebře se studují objekty tří typů: matice, prostory a algebraické formy. Teorie těchto objektů jsou navzájem těsně spjaty. Většina úloh lineární algebry připouští přirozenou formulaci v kterékoli z těchto tří teorií. Maticová formulace je obvykle nejvhodnější pro výpočetní stránku věci. V geometrii a mechanice vzniká většina úloh lineární algebry jako úlohy zkoumající algebraické formy. Nejhlubšího pochopení vnitřních souvislostí mezi různými úlohami lineární algebry se dosáhne pouze vyšetřováním odpovídajících lineárních prostorů, které jsou proto hlavním předmětem studia lineární algebry.

A. I. Mal'cev (1909–1967)¹

¹ *Osnovy linejnoj algebry*, třetí vydání z roku 1970, resp. čtvrté vydání z roku 1975, str. 9.

OBSAH

Předmluva	7
I. ALGEBRAICKÝ ÚVOD	
1. Množiny a zobrazení	9
2. Tělesa	18
3. Okruhy, obory integrity	27
4. Matice	32
5. Grupy	45
6. Permutace	51
II. VEKTOROVÉ PROSTORY	
7. Prostory a podprostory	61
8. Lineární závislost a nezávislost	78
9. Direktní součet	94
10. Homomorfismy	101
III. MATICE	
11. Maticová reprezentace homomorfismů	123
12. Hodnost matice, elementární úpravy	133
13. Soustavy lineárních rovnic	153
14. Determinanty	164
15. Metody výpočtu determinantů	185
IV. PODOBNOST	
16. Polynomiální matice	197
17. Charakteristický a minimální polynom, vlastní čísla a vlastní vektory	219
18. Podobnost, Jordanův kanonický tvar	235
19. Weyrova teorie charakteristických čísel	265
20. Soustavy lineárních diferenciálních rovnic s konstantními koeficienty	282

V. FORMY

21. Lineární formy	299
22. Semilineární formy na komplexních prostorech	322
23. Bilineární a kvadratické formy	326
24. Seskvilineární a kvadratické formy na komplexních prostorech	344
25. Hermitovské a symetrické formy	354

VI. SKALÁRNÍ SOUČIN

26. Unitární prostory	361
27. Unitární zobrazení	382
28. Gramovy matice a determinanty	388
29. Adjungované a samoadjungované homomorfismy	395
30. Formy na unitárních prostorech	406
31. Pseudoinverzní homomorfismy a matice	414

Literatura	433
------------------	-----

PŘEDMLUVA

Lineární algebra patří k základům vysokoškolské matematiky. Na jedné straně přirozeným způsobem navazuje na některé partie matematiky středoškolské a zařazuje je do uceleného systému, na druhé straně je důležitým východiskem dalších matematických disciplín. Proto bývá na vysokých školách zařazována do prvního ročníku.

Srovnáním většího počtu učebnic lineární algebry je možno snadno nahlédnout, že vymezení obsahu této disciplíny značně kolísá, že látku je možno pojmut nej-různějším způsobem a že jednotlivé celky lze téměř libovolně permutovat. Rovněž lze zaznamenat velké rozdíly v přístupu, ve výkladu a v míře obecnosti. Někdy je lineární algebra prezentována jako soubor receptů pro řešení jednoduchých úloh (soustavy lineárních rovnic o dvou, resp. třech neznámých, determinanty druhého a třetího řádu, aplikace na analytickou geometrii v rovině a prostoru atd.), jindy je vykládána jako teorie vektorových prostorů (obecně libovolné dimenze) nad komutativním tělesem, někdy dokonce jako určitá partie teorie modulů.

Tento učební text je z velké části věnován klasickým partiím lineární algebry. Snaží se podat lineární algebru jako ucelenou algebraickou teorii vektorových prostorů a jejich homomorfismů.² Byl sepsán na základě mnoholetých zkušeností s výukou; částečně vyšel ze skript *Vektorové prostory I, II, III*, která byla vydávána v SPN v letech 1978 až 1989. Výklad postupuje většinou standardním způsobem; na mnoha místech jsou však použity nepříliš obvyklé postupy, obraty a důkazy, kterými byly během let přednášky „vylepšovány“. Některé paragrafy (např. poslední paragraf o pseudoinverzních homomorfismech a maticích) jsou pojaty netradičně.

První část, která je nazvána *Algebraický úvod*, je přípravná. Obsahuje zejména definice některých základních pojmů obecné algebry, které jsou v dalším textu užívány, a řadu příkladů; větší pozornost je zde věnována tělesům, maticím a permutacím. Na několika málo místech se v dalším textu objeví v krátkých poznámkách i pojmy, které v úvodu vysvětleny nebyly (např. normální podgrupa, index podgrupy, jádro grupového homomorfismu apod.); tato skutečnost však není na újmu srozumitelnosti výkladu.

Následující kapitoly *Vektorové prostory*, *Matic*, *Podobnost*, *Formy* a *Skalární součin* jsou již zcela věnovány lineární algebře.

² Do značné míry tak může být průpravou pro následné studium obecné algebry, které je v současné době zařazeno do druhého ročníku.

Domnívám se, že není na škodu, obsahuje-li učební text i partie, které nejsou přímo obsahem kursovní přednášky (např. Weyrova teorie charakteristických čísel, racionální kanonické tvary matic), nebo partie, které ukazují využití lineární algebry v jiných disciplínách. Např. 20. paragraf demonstruje roli, kterou hraje Jordanův kanonický tvar, vlastní čísla a vlastní vektory při řešení soustav lineárních diferenciálních rovnic s konstantními koeficienty. Snad budou tyto partie inspirací pro další studium, snad přispějí k rozšíření obzorů.

Příklady, které jsou v textu na mnoha místech uvedeny, usnadňují na jedné straně pochopení teoretických partií, na druhé straně demonstrují jednotlivé početní postupy. Několik příkladů využívá i poznatků (zejména z analýzy), které mohou být studentům v prvním semestru ještě cizí; většina z nich je však probírána během prvního ročníku studia.

V seznamu literatury jsou uvedeny zejména klasické učebnice a učební texty, které u nás v minulých letech podstatným způsobem výuku lineární algebry ovlivňovaly.

V tomto učebním textu předpokládáme, že čtenář umí řešit soustavy lineárních rovnic některým ze způsobů, které se probírají na střední škole; ve 13. a 14. paragrafu se pak naučí řešit soustavy lineárních rovnic pomocí Gaussova eliminačního algoritmu, Cramerova pravidla a dalšími způsoby.

Děkuji M. Hykšové, M. Němečkové a M. Ernestové, které s přípravou tohoto textu pomohly.

Jindřich Bečvář

I. ALGEBRAICKÝ ÚVOD

1. MNOŽINY A ZOBRAZENÍ

V tomto paragrafu připomeneme některé základní matematické pojmy a jejich vlastnosti, zavedeme několik symbolů a termínů; navíc stručně uvedeme některá důležitá fakta o množinách.

V celém textu budeme užívat následující označení:

\mathbb{P} — množina všech prvočísel,

\mathbb{N} — množina všech přirozených čísel, tj. $\mathbb{N} = \{1, 2, 3, \dots\}$,

\mathbb{Z} — množina všech celých čísel,

\mathbb{Q} — množina všech racionálních čísel,

\mathbb{R} — množina všech reálných čísel,

\mathbb{C} — množina všech komplexních čísel.

Budeme užívat i tzv. *kvantifikátory*; můžeme je chápat jako symboly pro následující slovní označení:

\forall — pro každé , \exists — existuje .

V celém textu budeme předpokládat znalost základních poznatků o množinách a množinových operacích (*podmnožina, sjednocení, průnik, rozdíl, kartézský součin* apod.).

Zdůrazněme, že nelze uvažovat *množinu všech množin* — to vede k logickým sporům; proto se na několika místech objeví termín *třída všech množin*.

Poznamenejme, že od množiny je třeba odlišovat *soubor*; zatímco množina obsahuje prvky navzájem různé, v souboru se mohou prvky i vícekrát opakovat. Např. $\{1, 1, 2, 1, 3, 2, 2, 3, 2, 3\}$ je soubor, který obsahuje prvek 1 třikrát, prvek 2 čtyřikrát a prvek 3 třikrát.

Často se setkáme s tzv. indexovaným souborem. Jsou-li Λ a X množiny, pak

$$\{x_\alpha ; \alpha \in \Lambda\} , \quad \text{resp.} \quad \{x_\alpha\}_{\alpha \in \Lambda}$$

je *indexovaný soubor* prvků množiny X , jestliže $x_\alpha \in X$ pro každé $\alpha \in \Lambda$ (indexy probíhají množinu Λ); znamená to, že každému $\alpha \in \Lambda$ je jednoznačně přiřazen prvek $x_\alpha \in X$. Znovu zdůrazněme, že jednotlivé prvky x_α nemusí být navzájem různé.

V následujícím odstavci budeme definovat zobrazení a některé jeho speciální typy; tyto pojmy je třeba dobře pochopit, závisí na tom porozumění celého dalšího textu.

1.1. Definice. *Zobrazením* f množiny A do množiny B rozumíme předpis, který každému prvku $a \in A$ přiřazuje právě jeden prvek $f(a) \in B$.

Zobrazení f se nazývá *prosté*, resp. *injektivní* (též *injekce*), jestliže různé prvky množiny A zobrazuje na různé prvky množiny B , tj.

$$\forall a_1, a_2 \in A \quad a_1 \neq a_2 \implies f(a_1) \neq f(a_2) .$$

Řekneme, že zobrazení f je zobrazením množiny A na množinu B , resp. *surjektivním* zobrazením (též *surjekce*), jestliže na každý prvek množiny B se zobrazí alespoň jeden prvek množiny A , tj.

$$\forall b \in B \quad \exists a \in A \quad f(a) = b .$$

Zobrazení, které je současně injektivní a surjektivní (tj. prosté a na), se nazývá *vzájemně jednoznačné*, resp. *bijektivní* (též *bijekce*). Bijektivní zobrazení f množiny A na množinu B je tedy charakterizováno touto podmínkou: pro každé $b \in B$ existuje právě jediný prvek $a \in A$, pro který je $f(a) = b$.

1.2. Příklady.

(i) Zobrazení, které každému číslu $n \in \mathbb{Z}$ přiřazuje číslo $-n$, je bijekce množiny \mathbb{Z} na množinu \mathbb{Z} .

(ii) Zobrazení, které každému číslu $n \in \mathbb{Z}$ přiřazuje číslo $2n$, je injekce množiny \mathbb{Z} do množiny \mathbb{Z} . Toto zobrazení není surjekce, a tedy ani bijekce.

(iii) Zobrazení, které každému číslu $n \in \mathbb{Z}$ přiřazuje číslo $|n|+1$, je surjekce množiny \mathbb{Z} na množinu \mathbb{N} . Toto zobrazení není injekce, a tedy ani bijekce.

(iv) Zobrazení, které každému číslu $x \in \mathbb{R}$ přiřazuje číslo x^3 , je bijekce množiny \mathbb{R} na množinu \mathbb{R} .

(v) Zobrazení, které každému číslu $x \in \mathbb{R}$ přiřazuje číslo x^2 , je surjekce množiny \mathbb{R} na množinu všech nezáporných reálných čísel. Toto zobrazení není injekcí, a tedy ani bijekcí.

(vi) Zobrazení, které každému číslu $x \in \mathbb{R}$ přiřazuje číslo e^x , je injekce množiny \mathbb{R} do množiny \mathbb{R} . Toto zobrazení je možno chápat jako bijekci množiny \mathbb{R} na množinu všech kladných reálných čísel.

(vii) Indexovaný soubor $\{x_\alpha ; \alpha \in \Lambda\}$, kde pro každé α je $x_\alpha \in X$, není nic jiného než zobrazení množiny Λ do množiny X .

(viii) Zobrazení množiny A na množinu A , které každému prvku $a \in A$ přiřadí stejný prvek a , je bijekce. Je to tzv. *identita*, značí se většinou symbolem 1_A .

(ix) Zobrazení kartézského součinu $A \times A$ do množiny A je tzv. *binární operace* na množině A . Každým dvěma prvkům x, y množiny A je přiřazen jednoznačně určený prvek této množiny; často se označuje $x \cdot y$, xy , $x + y$ apod. Zdůrazněme, že obecně závisí na pořadí prvků x, y , tj. nemusí vždy být $x \cdot y = y \cdot x$.

Nechť f je zobrazení množiny A do množiny B .

Jestliže se prvek $a \in A$ zobrazuje na prvek $b = f(a) \in B$, pak říkáme, že je prvek b *obrazem* prvku a a prvek a *vzorem* prvku b .

Obrazem podmnožiny A' množiny A nazýváme množinu

$$f(A') = \{b \in B; \exists a \in A' \ b = f(a)\} .$$

Obraz $f(A)$ množiny A bývá rovněž označován symbolem $\text{Im } f$.

Úplným vzorem podmnožiny B' množiny B nazýváme množinu

$$\{a \in A; f(a) \in B'\} .$$

Složení zobrazení f množiny A do množiny B a zobrazení g množiny B do množiny C dostaneme zobrazení množiny A do množiny C , které značíme gf . Velmi jednoduše lze ukázat, že složením injekcí, resp. surjekcí, resp. bijekcí je injekce, resp. surjekce, resp. bijekce. Poznamenejme, že skládání zobrazení je asociativní, tj. pro zobrazení f množiny A do množiny B , zobrazení g množiny B do množiny C a zobrazení h množiny C do množiny D je

$$h(gf) = (hg)f .$$

Nechť f je bijekce množiny A na množinu B . Zobrazení, které každému prvku $b \in B$ přiřazuje prvek $a \in A$, pro který je $f(a) = b$, je bijekcí množiny B na množinu A ; nazývá se *inverzní zobrazení* k zobrazení f a značí se f^{-1} .

Nechť f je zobrazení množiny A do množiny B . Toto zobrazení můžeme přirozeným způsobem *zúžit* na zobrazení libovolně zvolené podmnožiny A' množiny A ; získáme zobrazení f' množiny A' do množiny B , které je na množině A' definováno „stejně“ jako zobrazení f , tj.

$$\forall a \in A' \quad f'(a) = f(a) .$$

Zobrazení f můžeme rovněž přirozeným způsobem *zúžit* na zobrazení množiny A do libovolné podmnožiny B'' množiny B , která obsahuje množinu $f(A)$. Toto zobrazení f'' je na množině A definováno „stejně“ jako zobrazení f , tj.

$$\forall a \in A \quad f''(a) = f(a) .$$

1.3. Definice. *Relací* na množině A rozumíme každou podmnožinu ϱ kartézského součinu $A \times A$; jestliže $(x, y) \in \varrho$, pak píšeme $x\varrho y$. Relace ϱ se nazývá

– *reflexivní*, jestliže

$$\forall x \in A \quad x\varrho x ;$$

– *symetrická*, jestliže

$$\forall x, y \in A \quad x\varrho y \implies y\varrho x ;$$

– *antisymetrická*, jestliže

$$\forall x, y \in A \quad x\varrho y, y\varrho x \implies x = y ;$$

– *tranzitivní*, jestliže

$$\forall x, y, z \in A \quad x\varrho y, y\varrho z \implies x\varrho z .$$

1.4. Definice. *Ekvivalenci* na množině A rozumíme každou relaci, která je reflexivní, symetrická a tranzitivní.

Nechť ρ je ekvivalence na množině A . Jestliže je $x\rho y$ (a tedy i $y\rho x$), pak říkáme, že prvky x, y jsou *ekvivalentní*.

1.5. Definice. *Disjunktním rozkladem* množiny A budeme rozumět každý systém \mathfrak{A} neprázdných podmnožin množiny A , které jsou navzájem disjunktí a jejichž sjednocením je celá množina A .

Každý prvek množiny A tedy leží právě v jediné podmnožině systému \mathfrak{A} .

Mezi ekvivalencemi na množině A a disjunktími rozklady této množiny existuje vzájemně jednoznačné přiřazení (bijekce).

Nechť je dána na množině A ekvivalence ρ . Uvažujeme-li ke každému prvku $a \in A$ podmnožinu všech prvků množiny A , které jsou s ním ekvivalentní, tj. podmnožinu $\{x \in A; x\rho a\}$, získáme disjunktí rozklad množiny A . Hovoříme o disjunktím rozkladu, který je určen danou ekvivalencí — příslušným podmnožinám se většinou říká *třídy ekvivalence* ρ . Disjunktí rozklad množiny A určený ekvivalencí ρ se většinou označuje A/ρ (čteme „ A podle ρ “); často se též hovoří o *faktorové množině* A/ρ množiny A podle ekvivalence ρ .

Je-li dán disjunktí rozklad množiny A , prohlásíme za ekvivalentní ty prvky množiny A , které leží ve stejné podmnožině daného rozkladu. Hovoříme o ekvivalenci určené daným disjunktím rozkladem.

1.6. Příklady.

(i) Velmi jednoduchým příkladem ekvivalence je rovnost. Uvažujeme-li např. rovnost na množině \mathbb{N} všech přirozených čísel, je odpovídajícím disjunktím rozkladem rozklad množiny \mathbb{N} na jednoprvkové množiny $\{1\}$, $\{2\}$, $\{3\}$ atd.

(ii) Disjunktím rozkladem množiny \mathbb{Z} je rozklad na sudá a lichá čísla

$$\mathbb{Z} = \{ \dots, -4, -2, 0, 2, 4, \dots \} \cup \{ \dots, -5, -3, -1, 1, 3, 5, \dots \}.$$

Tomuto rozkladu odpovídá ekvivalence, při které jsou navzájem ekvivalentní ta čísla, která mají stejnou *paritu*.

(iii) Zvolme pevně přirozené číslo n . Na množině \mathbb{Z} uvažujme relaci $\equiv \pmod{n}$, která je definována takto:

$$\text{pro } a, b \in \mathbb{Z} \text{ je } a \equiv b \pmod{n}, \text{ jestliže pro nějaké } k \in \mathbb{Z} \text{ je } a - b = kn.$$

Např. $7 \equiv 3 \pmod{4}$, $6 \equiv 71 \pmod{5}$, $-3 \equiv 6 \pmod{3}$. Relace $\equiv \pmod{n}$ je reflexivní, symetrická a tranzitivní, hovoříme o *ekvivalenci modulo* n . Čísla a, b jsou tedy ekvivalentní modulo n právě tehdy, když dávají při dělení číslem n stejný nezáporný zbytek. Např. čísla 3, 8, 18, 33, -2, -22, -37 jsou ekvivalentní modulo 5, neboť dávají při dělení číslem 5 zbytek 3.

Disjunktční rozklad množiny \mathbb{Z} , který odpovídá ekvivalenci $\equiv \pmod{n}$, neboli faktorová množina $\mathbb{Z}/\equiv \pmod{n}$ má právě n prvků; sestává z následujících podmnožin množiny \mathbb{Z} (tříd ekvivalence $\equiv \pmod{n}$):

$$\begin{aligned} & \{ \dots, -4n, -3n, -2n, -n, 0, n, 2n, 3n, 4n, \dots \}, \\ & \{ \dots, -3n+1, -2n+1, -n+1, 1, n+1, 2n+1, 3n+1, \dots \}, \\ & \{ \dots, -3n+2, -2n+2, -n+2, 2, n+2, 2n+2, 3n+2, \dots \}, \\ & \dots\dots\dots \\ & \{ \dots, -2n-2, -n-2, -2, n-2, 2n-2, 3n-2, 4n-2, \dots \}, \\ & \{ \dots, -2n-1, -n-1, -1, n-1, 2n-1, 3n-1, 4n-3, \dots \}. \end{aligned}$$

Při dělení číslem n dávají všechna čísla v jednotlivých třídách po řadě nezáporné zbytky $0, 1, 2, \dots, n-1$.

Faktorová množina $\mathbb{Z}/\equiv \pmod{n}$ se většinou označuje symbolem \mathbb{Z}_n . Její prvky, tj. výše uvedené množiny, se často značí pomocí nejmenších nezáporných čísel, která jsou v nich obsažena, např. symboly $\bar{0}, \bar{1}, \dots, \overline{n-1}$. Velmi často se však pruhy vynechávají a píše se

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}.$$

Poznamenejme, že každá dvě celá čísla jsou ekvivalentní modulo 1, příslušný disjunktční rozklad množiny \mathbb{Z} je jednoprvkový (tj. množina \mathbb{Z} se vlastně „nerozloží“, $\mathbb{Z}_1 = \{0\}$). Dvě celá čísla jsou ekvivalentní modulo 2 právě tehdy, mají-li stejnou paritu; příslušný rozklad množiny \mathbb{Z} je dvouprvkový (viz příklad (ii)), $\mathbb{Z}_2 = \{0, 1\}$.

Připomeňme ještě, že se místo *ekvivalence modulo n* často říká *rovnost modulo n* a místo $a \equiv b \pmod{n}$ se píše $a = b \pmod{n}$.

1.7. Definice. *Uspořádáním* na množině A rozumíme každou relaci, která je reflexivní, antisymetrická a tranzitivní. *Uspořádanou množinou* rozumíme množinu s daným uspořádáním.

Nechť A je uspořádaná množina s uspořádáním ρ ; jestliže je $a\rho b$ a $a \neq b$, pak říkáme, že a je *menší než b* a že b je *větší než a* .

Prvek $a \in A$ se nazývá *maximálním prvkem* množiny A , jestliže v množině A neexistuje prvek, který je větší než a , tj. jestliže

$$\forall x \in A \quad a\rho x \implies x = a;$$

prvek $a \in A$ se nazývá *minimálním prvkem* množiny A , jestliže v množině A neexistuje prvek, který je menší než a , tj. jestliže

$$\forall x \in A \quad x\rho a \implies x = a.$$

Prvek $a \in A$ se nazývá *největším prvkem* množiny A , jestliže je větší než kterýkoli jiný prvek množiny A , tj.

$$\forall x \in A \quad x \rho a ;$$

prvek $a \in A$ se nazývá *nejmenším prvkem* množiny A , jestliže je menší než kterýkoli jiný prvek množiny A , tj.

$$\forall x \in A \quad a \rho x .$$

Uspořádání ρ se nazývá *úplné*, jestliže pro každé $x, y \in A$ je buď $x \rho y$ nebo $y \rho x$. Množina s úplným uspořádáním se nazývá *úplně uspořádaná množina*.

Poznamenejme, že největší, resp. nejmenší prvek může v uspořádané množině existovat nejvýše jeden; největší prvek je současně maximálním, nejmenší prvek je současně minimálním prvkem. Maximální prvek však nemusí být největším prvkem, minimální prvek nemusí být nejmenším prvkem. Maximálních, resp. minimálních prvků může v množině existovat více, nemusí však existovat žádný. V úplně uspořádané množině pojmy maximálního prvku a největšího prvku splývají, totéž platí pro pojmy minimálního a nejmenšího prvku.

Nechť A je uspořádaná množina s uspořádáním ρ a necht' A' je její podmnožina. Podmnožina A' je potom uspořádanou množinou s uspořádáním ρ' , které je definováno jako průnik relace ρ s kartézským součinem $A' \times A'$. Hovoříme o *zúžení* nebo *restrikci* uspořádání množiny A na podmnožinu A' . Některé podmnožiny uspořádané množiny mohou být úplně uspořádané, často se nazývají *řetězce*.

Podmnožina A' uspořádané množiny A se nazývá *shora*, resp. *zdola omezená*, existuje-li prvek $a \in A$ s vlastností

$$\forall x \in A' \quad x \rho a , \quad \text{resp.} \quad \forall x \in A' \quad a \rho x .$$

1.8. Příklady.

(i) Na množině \mathbb{N} všech přirozených čísel můžeme uvažovat relaci $|$ (dělitelnost), která je definována takto: pro $a, b \in \mathbb{N}$ je $a|b$, jestliže číslo a dělí číslo b . Je tedy např. $1|3$, $3|3$, $2|6$, $5|15$, $7|49$ apod. Relace $|$ je reflexivní, antisymetrická a tranzitivní, tj. jde o uspořádání. Toto uspořádání však není úplné, neboť např. není ani $3|5$ ani $5|3$. V množině \mathbb{N} neexistují maximální prvky, nejmenším prvkem je číslo 1. Množina všech sudých čísel, ani množina všech prvočísel není v množině \mathbb{N} shora omezená. Vzhledem k tomu, že má množina \mathbb{N} nejmenší prvek, je každá podmnožina množiny \mathbb{N} zdola omezená. Všechny mocniny čísla 2 (nebo libovolně zvoleného čísla) tvoří v množině \mathbb{N} řetězec.

Zúžíme-li uspořádání na podmnožinu $\mathbb{N}' = \{2, 3, 4, \dots\}$, snadno nahlédneme, že uspořádaná množina \mathbb{N}' má nekonečně mnoho minimálních prvků (jsou to právě všechna prvočísla) a nemá žádný maximální prvek. Množina \mathbb{P} všech prvočísel není v množině \mathbb{N}' shora ani zdola omezená.

(ii) Na množině \mathbb{N} všech přirozených čísel můžeme uvažovat relaci \leq ; jde o úplné uspořádání,

$$1 \leq 2 \leq 3 \leq 4 \leq \dots$$

Číslo 1 je nejmenším prvkem množiny \mathbb{N} , největší prvek neexistuje. Na množině \mathbb{Z} můžeme rovněž uvažovat relaci \leq ; opět jde o úplné uspořádání,

$$\dots \leq -3 \leq -2 \leq -1 \leq 0 \leq 1 \leq 2 \leq 3 \leq 4 \leq \dots$$

Uspořádaná množina \mathbb{Z} nemá ani největší ani nejmenší prvek.

Rovněž množina \mathbb{Q} všech racionálních čísel a množina \mathbb{R} všech reálných čísel jsou relací \leq úplně uspořádané.

(iii) Uvažujme množinu \mathfrak{A} všech podmnožin nějaké množiny A . Množina \mathfrak{A} je uspořádaná tzv. *inkluzí*, tj. relací \subseteq . Uspořádaná množina \mathfrak{A} má nejmenší prvek \emptyset a největší prvek A . Jestliže je množina A alespoň dvouprvková, není množina \mathfrak{A} úplně uspořádaná.

Následující tvrzení, tzv. Zornovo lemma, můžeme chápat jako axiom teorie množin.

1.9. Zornovo lemma. *Neprázdná uspořádaná množina, ve které je každý řetězec shora omezený, má maximální prvek.*

V následujících odstavcích popíšeme velmi stručně a bez důkazů základní představy o mohutnostech množin a kardinálních číslech.

1.10. Definice. Řekneme, že množiny X a Y mají stejnou *mohutnost*, jestliže existuje bijekce množiny X na množinu Y .

Třída všech množin se disjunktně rozloží na třídy množin stejné mohutnosti, v každé takovéto třídě jsou množiny, mezi kterými existuje bijekce. Navzájem různým třídám množin jsou přiřazeny navzájem různé symboly, tzv. *kardinální čísla*; kardinální čísla jsou tedy zprostředkovaně přiřazena i všem množinám: je-li množina X prvkem třídy, které je přiřazeno kardinální číslo α , pak říkáme, že množina X má *mohutnost*, resp. *kardinalitu* α a píšeme $|X| = \alpha$.

V jedné třídě uvažovaného disjunktního rozkladu třídy všech množin je pouze prázdná množina, ve druhé jsou právě všechny jednoprvkové množiny, v další třídě právě všechny dvouprvkové množiny atd.; odpovídající kardinální čísla je zvykem označovat symboly $0, 1, 2, \dots$. Prázdná množina, všechny jednoprvkové množiny, všechny dvouprvkové množiny atd., tj. množiny, které mají mohutnost 0, resp. 1, resp. 2 atd., se nazývají *konečné*; u konečné množiny většinou nehovoříme o mohutnosti, ale o *počtu prvků*. Např. množina \mathbb{Z}_n má n prvků, resp. mohutnost n ; je tedy $|\mathbb{Z}_n| = n$.

Množiny, které nejsou konečné, se nazývají *nekonečné*.

Nejjednodušší a nejsnáze „představitelnou“ nekonečnou množinou je množina \mathbb{N} všech přirozených čísel. Ta třída výše uvažovaného disjunktního rozkladu, ve které leží množina \mathbb{N} , obsahuje všechny tzv. *spočetné množiny*, tj. množiny, které mají stejnou mohutnost jako množina \mathbb{N} . Odpovídající kardinální číslo je zvykem značit symbolem \aleph_0 (čteme *alef nula*, alef je první písmeno hebrejské abecedy). Spočetnými množinami jsou dále např. množina všech prvočísel, množina všech celých čísel a množina všech racionálních čísel, tj.

$$|\mathbb{P}| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0 .$$

Spočetnými množinami jsou dále např. množina \mathbb{N}^2 všech dvojic přirozených čísel, množina \mathbb{Q}^n všech n -tic racionálních čísel ($n \in \mathbb{N}$) apod.

Existují však ještě další třídy uvažovaného disjunktního rozkladu třídy všech množin; leží v nich *nekonečné nespočetné* množiny. Takovými množinami jsou např. množina \mathbb{R} všech reálných čísel a množina \mathbb{C} všech komplexních čísel.

Kardinální čísla můžeme přirozeným způsobem uspořádat.

1.11. Definice. Nechť α, β jsou kardinální čísla. Budeme psát

$$\alpha \leq \beta ,$$

jestliže existují množiny X a Y , pro které je $|X| = \alpha$ a $|Y| = \beta$, a jestliže existuje prosté zobrazení množiny X do množiny Y .

Dá se dokázat, že tato definice nezávisí na konkrétní volbě množin X a Y a že relace \leq je na třídě všech kardinálních čísel *úplným uspořádáním*. Zřejmě je

$$0 \leq 1 \leq 2 \leq \dots \leq \aleph_0 \leq \dots ;$$

kardinální čísla α , pro která je $\alpha < \aleph_0$ (tj. $\alpha \leq \aleph_0$ a $\alpha \neq \aleph_0$), resp. $\aleph_0 \leq \alpha$, se nazývají *konečná*, resp. *nekonečná*; konečnými kardinálními čísly jsou právě všechna přirozená čísla a nula.

Poznamenejme, že jestliže je množina X podmnožinou množiny Y , potom je $|X| \leq |Y|$. Jestliže je X vlastní podmnožinou konečné množiny Y , pak je vždy $|X| < |Y|$. Každá nekonečná množina Y však má vlastní podmnožiny X , pro které je $|X| = |Y|$.

Kardinální čísla můžeme také sčítat.

1.12. Definice. Nechť α_λ , $\lambda \in \Lambda$, jsou kardinální čísla a X_λ , $\lambda \in \Lambda$, množiny, z nichž každé dvě jsou disjunktní a pro které je

$$|X_\lambda| = \alpha_\lambda$$

pro každé $\lambda \in \Lambda$. Součet kardinálních čísel α_λ , $\lambda \in \Lambda$, definujeme jako kardinální číslo sjednocení množin X_λ , $\lambda \in \Lambda$, tj.

$$\sum_{\lambda \in \Lambda} \alpha_\lambda = \left| \bigcup_{\lambda \in \Lambda} X_\lambda \right| .$$

Poznamenejme, že definice součtu kardinálních čísel nezávisí na konkrétní volbě množin X_λ , $\lambda \in \Lambda$.

Kardinální čísla však nemůžeme bez obav odečítat; z rovnosti $\alpha + \beta = \alpha + \gamma$ nevyplývá rovnost $\beta = \gamma$; stačí uvážit případ $\alpha = \aleph_0$, $\beta = 1$, $\gamma = 2$.

1.13. Věta. *Je-li množina Y sjednocením množin Y_i , $i \in I$, potom je*

$$|Y| \leq \sum_{i \in I} |Y_i|. \quad \square$$

Uvědomme si, že mohou nastat případy, kdy neplatí rovnost; množiny Y_i totiž nemusí být po dvou disjunktní, tj. mohou se „překrývat“.

Definujme nyní násobení kardinálních čísel.

1.14. Definice. Nechť α , β jsou kardinální čísla a X , Y množiny, pro které je

$$|X| = \alpha \quad \text{a} \quad |Y| = \beta.$$

Součin $\alpha \cdot \beta$ kardinálních čísel α a β definujeme jako kardinální číslo, které je mohutností kartézského součinu $X \times Y$, tj.

$$\alpha \cdot \beta = |X \times Y|.$$

Dá se dokázat, že takto definovaný součin kardinálních čísel nezávisí na konkrétní volbě množin X , Y .

Důležité tvrzení, které není triviální, je zformulováno v následující větě.

1.15. Věta. *Jestliže je α nekonečné kardinální číslo, potom je*

$$\aleph_0 \cdot \alpha = \alpha. \quad \square$$

2. TĚLESA

2.1. Definice. Množina T se dvěma binárními operacemi " + " a " · " se nazývá *těleso*, jestliže je alespoň dvouprvková a platí následující axiomy:

- (i) $\forall a, b, c \in T \quad (a + b) + c = a + (b + c)$,
- (ii) $\forall a, b \in T \quad a + b = b + a$,
- (iii) $\exists 0 \in T \quad \forall a \in T \quad a + 0 = a$,
- (iv) $\forall a \in T \quad \exists -a \in T \quad a + (-a) = 0$,
- (v) $\forall a, b, c \in T \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- (vi) $\exists 1 \in T \quad \forall a \in T \quad 1 \cdot a = a \cdot 1 = a$,
- (vii) $\forall a \in T, a \neq 0 \quad \exists a^{-1} \in T \quad a \cdot a^{-1} = a^{-1} \cdot a = 1$,
- (viii) $\forall a, b, c \in T \quad a \cdot (b + c) = a \cdot b + a \cdot c$,
- (ix) $\forall a, b, c \in T \quad (a + b) \cdot c = a \cdot c + b \cdot c$.

Jestliže je navíc splněn axióm

$$(x) \forall a, b \in T \quad a \cdot b = b \cdot a,$$

pak hovoříme o *komutativním tělese* nebo o *poli*.

Axiomy (i) a (ii) popisují tzv. asociativitu a komutativitu sčítání. Prvek 0, jehož existenci zaručuje axióm (iii), se nazývá *nulový prvek* tělesa T . Prvek $-a$ z axiómu (iv) se nazývá *opačný prvek* k prvku a . Místo $a + (-b)$ budeme psát krátce $a - b$.

Axióm (v) popisuje asociativitu násobení. Prvek 1, jehož existenci zaručuje axióm (vi), se nazývá *jednotkový prvek* tělesa T . Prvek a^{-1} z axiómu (vii) se nazývá *inverzní prvek* k prvku a .

Axiomy (viii) a (ix) jsou tzv. distributivní zákony; svazují obě binární operace na množině T . Jestliže je těleso komutativní, tj. platí-li axióm (x), jsou axiomy (viii) a (ix) ekvivalentní a stačí předpokládat platnost jen jednoho z nich.

V definici 2.1 požadujeme, aby mělo těleso alespoň dva prvky; v opačném případě by byl jednotkový prvek roven nulovému.

Poznamenejme, že se dá snadno dokázat, že nulový prvek existuje v tělese právě jediný, že rovněž jednotkový prvek existuje v tělese právě jediný, že ke každému prvku tělesa existuje právě jediný opačný prvek a ke každému nenulovému prvku existuje právě jediný inverzní prvek.

2.2. Definice. Nechť T je těleso. Podmnožina T' tělesa T se nazývá *podtěleso*, má-li tyto vlastnosti:

- (i) $0, 1 \in T'$,
- (ii) jestliže $a, b \in T'$, potom $a + b, a \cdot b, -a \in T'$,
- (iii) jestliže $0 \neq a \in T'$, potom $a^{-1} \in T'$.

Má-li podmnožina T' tělesa T vlastnosti (i) – (iii), je (spolu se zúženými operacemi " + " a " · " na podmnožinu T') tělesem podle definice 2.1.

2.3. Příklady.

(i) Množina \mathbb{Q} všech racionálních čísel s obvyklým sčítáním a násobením je komutativní těleso.

(ii) Množina \mathbb{R} všech reálných čísel s obvyklým sčítáním a násobením je komutativní těleso.

(iii) Množina \mathbb{C} všech komplexních čísel s obvyklým sčítáním a násobením je komutativní těleso.

(iv) Těleso \mathbb{Q} všech racionálních čísel je podtělesem tělesa \mathbb{R} všech reálných čísel a těleso \mathbb{R} je podtělesem tělesa \mathbb{C} všech komplexních čísel. Tělesa \mathbb{Q} , \mathbb{R} , \mathbb{C} jsou nekonečná.

(v) Ani množina \mathbb{N} všech přirozených čísel, ani množina \mathbb{Z} všech celých čísel s obvyklým sčítáním a násobením není tělesem.

2.4. Počítání v tělese. *Nechť T je těleso. Potom platí:*

- (i) $\forall a \in T \quad 0 \cdot a = 0$,
- (ii) $\forall a, b \in T \quad (-a) \cdot b = a \cdot (-b) = -a \cdot b, \quad (-1) \cdot a = -a$,
- (iii) $\forall a, b, c \in T \quad (a - b) \cdot c = a \cdot c - b \cdot c$,
- (iv) $\forall a \in T, a \neq 0 \quad \forall b \in T, b \neq 0 \quad a \cdot b \neq 0$,
- (v) $1 \neq 0$.

Důkaz.

(i) Podle axiomů 2.1(iii) a (ix) je

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a .$$

Proto je podle 2.1(iv)

$$0 \cdot a + (-0 \cdot a) = (0 \cdot a + 0 \cdot a) + (-0 \cdot a) ,$$

podle axiomů 2.1(iv), (i) a (iii) je nyní

$$0 = 0 \cdot a .$$

(ii) Podle výše dokázaného tvrzení (i), axiomu 2.1(iv),(ix) je

$$0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b .$$

Podle 2.1(iii),(iv) a (i) je nyní

$$\begin{aligned} -a \cdot b &= -a \cdot b + 0 = -a \cdot b + (a \cdot b + (-a) \cdot b) = \\ &= (-a \cdot b + a \cdot b) + (-a) \cdot b = 0 + (-a) \cdot b = (-a) \cdot b . \end{aligned}$$

Podobně se dokáže rovnost

$$-a \cdot b = a \cdot (-b) .$$

Jednoduchým důsledkem právě dokázaného tvrzení je rovnost

$$-a = (-1) \cdot a .$$

(iii) Podle úmluvy, 2.1(ix) a výše dokázaného tvrzení (ii) je

$$(a - b) \cdot c = (a + (-b)) \cdot c = a \cdot c + (-b) \cdot c = a \cdot c + (-b \cdot c) = a \cdot c - b \cdot c .$$

(iv) Předpokládejme, že $a \neq 0$, $b \neq 0$ a $a \cdot b = 0$. Podle 2.1(vii) existuje k prvku b inverzní prvek b^{-1} . Podle tvrzení (i), předpokladu a axiomů 2.1(v), (vii), (vi) je

$$0 = 0 \cdot b^{-1} = (a \cdot b) \cdot b^{-1} = a \cdot (b \cdot b^{-1}) = a \cdot 1 = a$$

a to je ve sporu s předpokladem. Proto je $a \cdot b \neq 0$.

(v) Podle definice 2.1 v tělese T existuje nenulový prvek a (T je alespoň dvouprvkové). Jestliže je $1 = 0$, potom je podle tvrzení (i) a 2.1(vi)

$$0 = 0 \cdot a = 1 \cdot a = a$$

a to spor s předpokladem. \square

Podobným způsobem můžeme dokázat řadu dalších pravidel pro počítání v tělese.

Připomeňme ještě, že znaménko "·" operace násobení budeme v řadě případů vynechávat a psát např. ab místo $a \cdot b$.

2.5. Příklad. Necht n je přirozené číslo. Na množině $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ definujme dvě binární operace, *sčítání a násobení modulo n* .

Součtem modulo n , resp. *součinem modulo n* prvků $a, b \in \mathbb{Z}_n$ je nejmenší nezáporný zbytek při dělení obyčejného součtu, resp. obyčejného součinu celých čísel a, b číslem n . Např.

$$\begin{aligned} 5 + 4 &= 2 \pmod{7}, & 3 + 6 &= 1 \pmod{8}, & 7 + 8 &= 4 \pmod{11}, \\ 5 \cdot 4 &= 6 \pmod{7}, & 3 \cdot 6 &= 2 \pmod{8}, & 7 \cdot 6 &= 9 \pmod{11}, \end{aligned}$$

neboť

$$\begin{aligned} 5 + 4 &= 1 \cdot 7 + 2, & 3 + 6 &= 1 \cdot 8 + 1, & 7 + 8 &= 1 \cdot 11 + 4, \\ 5 \cdot 4 &= 2 \cdot 7 + 6, & 3 \cdot 6 &= 2 \cdot 8 + 2, & 7 \cdot 6 &= 3 \cdot 11 + 9. \end{aligned}$$

Uvedme ještě tabulky pro sčítání a násobení modulo 5 a 6, tj. tabulky binárních operací "+" a "·" v \mathbb{Z}_5 a \mathbb{Z}_6 :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Ukážeme, že pro množinu \mathbb{Z}_n se sčítáním a násobením modulo n platí kromě axiому (vii) všechny axiomy z definice 2.1.

Poměrně snadno se usoudí, že operace sčítání i násobení modulo n jsou komutativní a asociativní a že jsou svázány distributivním zákonem; stačí si uvědomit, že sčítání a násobení celých čísel tyto vlastnosti má a že ke zbytkům při dělení číslem n je možno „přejít kdykoliv“. Pro názornost dokážeme asociativitu násobení modulo n ; ukážeme, že pro prvky $a, b, c \in \mathbb{Z}_n$ je

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \pmod{n}.$$

Pišme

$$ab = kn + x \quad \text{a} \quad bc = ln + y,$$

kde $k, l \geq 0$ jsou celá čísla a $0 \leq x, y < n$, a dále

$$xc = rn + u \quad \text{a} \quad ay = sn + v,$$

kde $r, s \geq 0$ jsou celá čísla a $0 \leq u, v < n$. Nyní je

$$(a \cdot b) \cdot c = x \cdot c = u \pmod{n} \quad \text{a} \quad a \cdot (b \cdot c) = a \cdot y = v \pmod{n}.$$

Dále je

$$(ab)c = (kn + x)c = (kc + r)n + u \quad \text{a} \quad a(bc) = a(ln + y) = (al + s)n + v.$$

Protože pro celá čísla a, b, c platí rovnost $(ab)c = a(bc)$, je $u = v$. Násobení v množině \mathbb{Z}_n je tedy asociativní.

Číslo 0 je nulovým prvkem vzhledem ke sčítání, číslo 1 je jednotkovým prvkem vzhledem k násobení. Opačným prvkem k prvku $0 \neq a \in \mathbb{Z}_n$ je zřejmě prvek $n - a$ (např. 1 a 5, resp. 2 a 4, resp. 3 a 3 jsou navzájem opačné prvky v \mathbb{Z}_6 , 5 a 4, resp. 6 a 3 jsou navzájem opačné prvky v \mathbb{Z}_9 ; opačným prvkem k 0 je 0 v každém \mathbb{Z}_n).

2.6. Věta. *Množina \mathbb{Z}_n se sčítáním a násobením modulo n je komutativním tělesem právě tehdy, když je n prvočíslo.*

Důkaz. Jestliže n je číslo složené, je $n = ab$, kde $1 < a, b < n$ jsou přirozená čísla. Potom je však

$$a \cdot b = 0 \pmod{n}$$

a podle 2.4(iv) není \mathbb{Z}_n těleso.

V příkladu 2.5 jsme ukázali, že pro množinu \mathbb{Z}_n se sčítáním a násobením modulo n platí kromě axiому (vii) všechny axiomy z definice 2.1. Zbývá ukázat, že je-li n prvočíslo, platí i axióm (vii). Předpokládejme tedy, že $n = p$ je prvočíslo.

Jestliže pro $a, b, c \in \mathbb{Z}_p$, $a \neq 0$, $b \neq c$, je

$$a \cdot b = a \cdot c \pmod{p},$$

potom mají čísla ab a ac stejné zbytky při dělení prvočíslem p , tj.

$$ab - ac = a(b - c) = kp$$

(předpokládáme, že $b > c$). Protože je p prvočíslo, dělí p buď číslo a nebo číslo $b - c$. To však není možné, neboť $0 < a < p$ a $0 < b - c < p$.

Jestliže je tedy $a \in \mathbb{Z}_p$ nenulový prvek, potom jsou součiny $a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)$ navzájem různé a jsou to tedy všechny prvky množiny \mathbb{Z}_p . Pro nějaké $b \in \mathbb{Z}_p$ je tedy $a \cdot b = 1$, tj. b je v \mathbb{Z}_p inverzním prvkem k prvku a . Množina \mathbb{Z}_p se sčítáním a násobením modulo p je tedy komutativní těleso. \square

2.7. Poznámka. Druhá část důkazu předchozí věty má *existenční charakter*. Ukázali jsme, že k nenulovému prvku $a \in \mathbb{Z}_p$ inverzní prvek *existuje*, ale *nezkonstruovali* jsme ho. Opačný prvek k prvku a jsme naproti tomu zkonstruovali — je to prvek $p - a$.

Konstruktivní důkaz existence inverzního prvku k nenulovému prvku $a \in \mathbb{Z}_p$ lze snadno provést s pomocí následujícího známého výsledku.

Malá Fermatova věta: *Nechť p je prvočíslo a a přirozené číslo, které je s prvočíslem p nesoudělné. Potom*

$$a^{p-1} = 1 \pmod{p}.$$

Podle Malé Fermatovy věty je a^{p-2} inverzním prvkem k prvku a , neboť

$$a \cdot a^{p-2} = a^{p-1} = 1 \pmod{p}.$$

Např. v \mathbb{Z}_5 je $3^3 = 2$ inverzním prvkem k prvku 3, v \mathbb{Z}_7 je $2^5 = 4$ inverzním prvkem k prvku 2.

Podle věty 2.6 jsou tedy

$$\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \dots$$

komutativní tělesa; konečných těles tedy existuje nekonečně mnoho.

Poznamenejme ještě, že ke každému prvočíslu p a každému přirozenému číslu n existuje v určitém smyslu jediné těleso, které má p^n prvků, a jiná konečná tělesa neexistují.³ Tento výsledek však není jednoduché dokázat.

2.8. Příklad. Čtyřprvkové těleso získáme (případ $p = n = 2$), definujeme-li binární operace " + " a " · " na množině $\{0, 1, a, b\}$ následujícími tabulkami:

³ Přesně: Každé konečné těleso má p^n prvků pro nějaké $p \in \mathbb{P}$ a $n \in \mathbb{N}$. Každá dvě tělesa o p^n prvcích jsou izomorfní.

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

\cdot	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

2.9. Příklad. Prvky tvaru $a+bi+cj+dk$, kde a, b, c, d jsou reálná čísla a i, j, k speciální symboly, se nazývají *kvaterniony*. Na množině \mathbb{H} všech kvaternionů zavedeme dvě binární operace, sčítání " $+$ " a násobení " \cdot ".

Kvaterniony sčítáme „po složkách“:

$$(a+bi+cj+dk) + (a'+b'i+c'j+d'k) = (a+a') + (b+b')i + (c+c')j + (d+d')k .$$

Kvaterniony násobíme „distributivně“ s pomocí tabulky pro násobení symbolů i, j, k :

\cdot	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

Násobení symbolů i, j, k se snadno pamatuje. Chápejme trojici (i, j, k) jako *cyklus*; součin dvou sousedních symbolů tohoto cyklu v pořadí zleva doprava je roven třetímu symbolu (např. $i \cdot j = k$, resp. $k \cdot i = j$) a součin dvou sousedních symbolů v opačném pořadí je roven záporně vzatému třetímu symbolu (např. $j \cdot i = -k$, resp. $i \cdot k = -j$). Navíc je, podobně jako v komplexním oboru, $i^2 = j^2 = k^2 = -1$. Tedy

$$\begin{aligned} & (a+bi+cj+dk) \cdot (a'+b'i+c'j+d'k) = \\ & = aa' + ab'i + ac'j + ad'k + ba'i - bb' + bc'k - bd'j + \\ & + ca'j - cb'k - cc' + cd'i + da'k + db'j - dc'i - dd' = \\ & = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + \\ & + (ac' + ca' + db' - bd')j + (ad' + da' + bc' - cb')k . \end{aligned}$$

Sčítání kvaternionů je zřejmě asociativní a komutativní, nulovým prvkem je kvaternion $0 = 0 + 0i + 0j + 0k$ a opačným kvaternionem ke kvaternionu

$a + bi + cj + dk$ je kvaternion $-a - bi - cj - dk$. Mechanickým výpočtem je možno dokázat asociativitu násobení kvaternionů; stačí však prověřit asociativitu násobení symbolů i, j, k . Oba distributivní zákony zřejmě platí.

Jednotkovým prvkem vzhledem k násobení je kvaternion

$$1 = 1 + 0i + 0j + 0k ;$$

velmi snadno je možno prověřit, že inverzním kvaternionem k nenulovému kvaternionu $a + bi + cj + dk$ je kvaternion

$$(a^2 + b^2 + c^2 + d^2)^{-1} \cdot (a - bi - cj - dk) .$$

Násobení kvaternionů je zřejmě nekomutativní, jak je vidět již z tabulky pro násobení symbolů i, j, k , např.

$$i \cdot j = k \neq -k = j \cdot i .$$

Množina \mathbb{H} všech kvaternionů spolu se sčítáním a násobením je tedy nekomutativním tělesem. Komutativní tělesa $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ jsou podtělesy nekomutativního tělesa \mathbb{H} ,

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} .$$

Uvažujme nyní posloupnost prvků tělesa T , která vznikne postupným sčítáním jednotkového prvku, tj. posloupnost

$$1, \quad 1 + 1, \quad 1 + 1 + 1, \quad 1 + 1 + 1 + 1, \quad \dots .$$

V této posloupnosti se může, ale nemusí objevit nulový prvek tělesa T . V prvním případě nás bude zajímat „první výskyt nuly“, tj. nejmenší počet jedniček, které musíme sečíst, abychom nulový prvek dostali.

2.10. Definice. Nechť T je těleso. Jestliže n je nejmenší přirozené číslo, pro které je

$$\underbrace{1 + 1 + \dots + 1}_n = 0 ,$$

potom říkáme, že *charakteristika* tělesa T je n , resp. že T je *těleso charakteristiky* n . Jestliže takové přirozené číslo neexistuje, potom říkáme, že *charakteristika* tělesa T je 0, resp. že T je *těleso charakteristiky* 0.

2.11. Věta. *Charakteristika tělesa je buď nula nebo prvočíslo.*

Důkaz. Předpokládejme, že charakteristikou tělesa T je složené číslo n . Pišme $n = ab$, kde $1 < a, b < n$. Potom je

$$\underbrace{(1 + 1 + \cdots + 1)}_{a \text{ krát}} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{b \text{ krát}} = \underbrace{1 + 1 + \cdots + 1}_{n \text{ krát}} = 0 .$$

Podle 2.4(iv) je buď

$$\underbrace{(1 + 1 + \cdots + 1)}_{a \text{ krát}} = 0 \quad \text{nebo} \quad \underbrace{(1 + 1 + \cdots + 1)}_{b \text{ krát}} = 0$$

a to je ve sporu s definicí charakteristiky. \square

Jestliže má těleso T charakteristiku p , potom jsou prvky

$$1, \quad 1 + 1, \quad \dots, \quad \underbrace{1 + 1 + \cdots + 1}_{(p-1) \text{ krát}}$$

nenulové a navzájem různé; většinou je označujeme symboly $1, 2, \dots, p-1$. Není obtížné ukázat, že tvoří podtěleso tělesa T , které je prakticky totožné (v algebře se říká *izomorfní*) s tělesem \mathbb{Z}_p .

Jestliže má těleso T charakteristiku 0, potom jsou prvky

$$1, \quad 1 + 1, \quad 1 + 1 + 1, \quad 1 + 1 + 1 + 1, \quad \dots$$

nenulové a navzájem různé; většinou je označujeme symboly $1, 2, 3, 4, \dots$. K těmto prvkům existují v tělese T opačné prvky, které značíme $-1, -2, -3, -4, \dots$, a inverzní prvky, které většinou značíme

$$1 = \frac{1}{1}, \quad \frac{1}{2}, \quad \frac{1}{3}, \quad \frac{1}{4}, \quad \dots$$

V tělese T musí dále existovat součiny výše uvedených prvků, tj. prvky

$$r \cdot \frac{1}{s}, \quad \text{kteř značíme} \quad \frac{r}{s} .$$

Není obtížné ukázat, že všechny tyto prvky tvoří podtěleso tělesa T , které je prakticky totožné (v algebře se říká *izomorfní*) s tělesem \mathbb{Q} .

2.12. Příklady. Tělesa $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a \mathbb{H} mají charakteristiku 0. Těleso \mathbb{Z}_p má charakteristiku p . Čtyřprvkové těleso z příkladu 2.8 má charakteristiku 2, jeho podtělesem je těleso \mathbb{Z}_2 .

2.13. Příklad. Nechtě r je pevně zvolené nenulové reálné číslo. Na množině \mathbb{R} definujeme binární operace " \circ " a " \diamond " takto:

$$a \circ b = a + b + \frac{1}{r}, \quad a \diamond b = a + b + abr .$$

Není obtížné dokázat, že množina \mathbb{R} s operacemi " \circ " a " \diamond " je komutativní těleso charakteristiky 0. Zároveň je užitečné si uvědomit, že na množině \mathbb{R} je možno definovat strukturu tělesa nekonečně mnoha způsoby (pro různá r).

3. OKRUHY, OBORY INTEGRITY

3.1. Definice. Množina R se dvěma binárními operacemi $+$ a \cdot (sčítání a násobení) se nazývá *okruh*, jestliže platí následující axiomy:

- (i) $\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$,
- (ii) $\forall a, b \in R \quad a + b = b + a$,
- (iii) $\exists 0 \in R \quad \forall a \in R \quad a + 0 = a$,
- (iv) $\forall a \in R \quad \exists -a \in R \quad a + (-a) = 0$,
- (v) $\forall a, b, c \in R \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- (viii) $\forall a, b, c \in R \quad a \cdot (b + c) = a \cdot b + a \cdot c$,
- (ix) $\forall a, b, c \in R \quad (a + b) \cdot c = a \cdot c + b \cdot c$.

Pokud platí axióm

- (vi) $\exists 1 \in R \quad \forall a \in R \quad 1 \cdot a = a \cdot 1 = a$,

pak hovoříme o *okruhu s jednotkovým prvkem*.

Pokud platí axióm

- (x) $\forall a, b \in R \quad a \cdot b = b \cdot a$,

pak hovoříme o *komutativním okruhu*.

Platí-li axiomy (x) a (vi), hovoříme o *komutativním okruhu s jednotkovým prvkem*.

Pokud v okruhu s jednotkovým prvkem existuje k prvku a prvek a^{-1} , pro který je

$$a \cdot a^{-1} = a^{-1} \cdot a = 1,$$

pak říkáme, že je prvek a *invertibilní* a že a^{-1} je *inverzním prvkem* k prvku a .

Poznamenejme, že jsme z metodických důvodů v definici 3.1 užili pro axiomy okruhu stejné číslování jako pro axiomy tělesa (resp. komutativního tělesa) v definici 2.1.

Axiomy (i) a (ii) vyjadřují *asociativitu* a *komutativitu* sčítání. Prvek 0, jehož existenci zaručuje axióm (iii), se nazývá *nulový prvek* okruhu R . Prvek $-a$ z axiómu (iv) se nazývá *opačný prvek* k prvku a . Místo $a + (-b)$ budeme opět psát $a - b$.

Axióm (v) vyjadřuje *asociativitu* násobení. Poznamenejme, že se vyšetřují i tzv. *neasociativní okruhy*; v jejich definici právě axióm (v) chybí. Axióm (x) představuje *komutativitu* násobení.

Axiomy (viii) a (ix) jsou *distributivní zákony*; svazují obě binární operace na množině R . Jestliže jde o komutativní okruh, tj. platí-li axióm (x), jsou axiomy (viii) a (ix) ekvivalentní a stačí předpokládat platnost jen jednoho z nich.

Prvek 1 z axiómu (vi), se nazývá *jednotkový prvek* okruhu R . Hovoříme-li o okruhu s jednotkovým prvkem, předpokládáme vždy, že je alespoň dvouprvkový, tj. že $1 \neq 0$.

3.2. Definice. Komutativní okruh s jednotkovým prvkem se nazývá *obor integrity*, jestliže platí axióm

$$(vii)^* \quad \forall a \in T, a \neq 0 \quad \forall b \in T, b \neq 0 \quad a \cdot b \neq 0 .$$

3.3. Poznámka.

(i) Nenulové prvky a, b okruhu R , pro které je $a \cdot b = 0$, se nazývají *netriviální dělitelé nuly*.⁴ Oborem integrity je tedy každý komutativní okruh s jednotkovým prvkem, ve kterém nejsou netriviální dělitelé nuly.

(ii) Připomeňme, že v tělese neexistují netriviální dělitelé nuly; v 2.4(iv) jsme viděli, že z axiómu existence inverzních prvků vyplývá neexistence netriviálních dělitelů nuly, tj. z axiómu (vii) plyne axióm (vii)*. Obor integrity je tedy „mezistupněm“ mezi komutativním okruhem s jednotkovým prvkem a komutativním tělesem.

(iii) Podobně jako v předchozím paragrafu (viz 2.4) je možno dokázat některá pravidla pro počítání v okruhu. Např.

$$\forall a \in R \quad 0 \cdot a = a \cdot 0 = 0 ,$$

$$\forall a, b, c \in R \quad (a - b) \cdot c = a \cdot c - b \cdot c , \quad a \cdot (b - c) = a \cdot b - a \cdot c .$$

(iv) Jestliže pro prvek a okruhu R platí

$$\forall b, c \in R \quad a \cdot b = a \cdot c \quad \implies \quad b = c ,$$

pak říkáme, že prvkem a je v okruhu R možno *krátit zleva*. Podobně se zavádí *krácení zprava*. Snadno je možno dokázat, že je-li prvek a v okruhu R invertibilní, je jím možno krátit zleva i zprava.

3.4. Příklady.

(i) Každé těleso je okruhem s jednotkovým prvkem.

(ii) Každé komutativní těleso je oborem integrity. Viz 2.4(iv) a 3.3(ii). Dá se dokázat, že každý konečný obor integrity je komutativním tělesem; tento důkaz jsme v podstatě provedli (v konkrétním případě) v 2.6.

(iii) Množina \mathbb{Z} všech celých čísel s obvyklým sčítáním a násobením je oborem integrity, není však tělesem. Invertibilními prvky v oboru integrity \mathbb{Z} jsou pouze prvky 1, -1.

(iv) Množina $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ všech tzv. *Gaussových celých čísel*⁵ s obvyklým sčítáním a násobením je oborem integrity, není však tělesem. Inverzní

⁴ Jestliže je $a \cdot b = c$, pak se někdy prvky a, b nazývají *dělitelé* prvku c . Odtud *dělitelé nuly*.

⁵ Gaussova celá čísla jsou právě ta komplexní čísla, jejichž obě složky jsou celočíselné; v Gaussově rovině jsou reprezentována všemi vrcholy jednotkové čtvercové sítě. Počítá se s nimi stejně jako s čísly komplexními.

komplexní číslo ke Gaussovu celému číslu již nemusí být Gaussovým celým číslem. Invertibilními prvky v oboru integrity $\mathbb{Z}[i]$ jsou pouze 1, -1 , i , $-i$.

(v) Množina $T[x]$ všech polynomů jedné neurčité x nad tělesem T s obvyklým sčítáním a násobením je oborem integrity.

Polynomem jedné neurčité x nad tělesem T rozumíme v algebře formální výraz

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,$$

kde $a_0, a_1, \dots, a_n \in T$ jsou *koeficienty*, x je tzv. *neurčitá a* $n \in \{0, 1, 2, \dots\}$. Jestliže je $a_0 \neq 0$, nazývá se a_0 *vedoucím koeficientem* a číslo n *stupněm* výše uvedeného polynomu. Polynomy prvního, druhého a třetího stupně mají tedy tvar

$$a_0x + a_1, \quad a_0x^2 + a_1x + a_2, \quad a_0x^3 + a_1x^2 + a_2x + a_3,$$

kde $a_0 \neq 0$; každý nenulový prvek $a \in T$ je polynomem nultého stupně. Nulový prvek tělesa T je tzv. *nulový polynom*, kterému obvykle stupeň nepřipisujeme.

Polynomy sčítáme „přirozeným způsobem“, tj. sčítáme členy se stejnými mocninami x ; např. pro polynomy z $\mathbb{R}[x]$

$$(5x^4 - 3x^3 + 2x - 4) + (2x^3 + 5x^2 + x + 2) = 5x^4 - x^3 + 5x^2 + 3x - 2.$$

Polynomy násobíme pomocí distributivního zákona, tj. každý člen s každým. Např.

$$(5x^4 - 3x^3 + 2x - 4) \cdot (2x^3 + 5x^2 + x + 2) = 10x^7 + 19x^6 - 10x^5 + 11x^4 - 4x^3 - 18x^2 - 8.$$

Povšimněme si, že stupeň součinu dvou polynomů je roven součtu jejich stupňů; proto nemůže být součin dvou nenulových polynomů polynomem nulovým. Sčítání a násobení polynomů množiny $T[x]$ má všechny vlastnosti požadované v definici oboru integrity.

Polynomy z $\mathbb{R}[x]$ můžeme chápat — jak je obvyklé — jako funkce jedné reálné proměnné x .

(vi) Množina \mathbb{Z}_n se sčítáním a násobením modulo n , kde n je číslo složené, je komutativním okruhem s jednotkovým prvkem; v tomto okruhu existují netriviální dělitelé nuly. Je-li p prvočíslo, je \mathbb{Z}_p komutativní těleso. Viz 2.5 až 2.7.

(vii) Množina všech reálných funkcí definovaných na intervalu (a, b) spolu s obvyklým sčítáním a násobením funkcí je komutativním okruhem s jednotkovým prvkem. Není však oborem integrity.

Připomeňme, že součtem, resp. součinem dvou funkcí f, g definovaných na intervalu (a, b) je funkce, která má v každém $x \in (a, b)$ hodnotu $f(x) + g(x)$, resp. $f(x) \cdot g(x)$. Uvědomme si, že existují nenulové funkce, jejichž součinem je funkce nulová.

(viii) Množina \mathbb{N} všech přirozených čísel se sčítáním a násobením není okruhem, neboť není splněn např. axióm (iii), tj. neexistuje nulový prvek. Množina $\mathbb{N} \cup \{0\}$ všech celých nezáporných čísel rovněž není okruhem, neboť není splněn axióm (iv), tj. neexistují opačné prvky.

Důležité příklady okruhů — okruhy matic — poznáme v následujícím paragrafu.

3.5. Definice. Nechť R je okruh. Podmnožina R' okruhu R se nazývá *podokruh*, má-li tyto vlastnosti:

- (i) $0 \in R'$,
- (ii) jestliže $a, b \in R'$, potom $a + b, a \cdot b, -a \in R'$.

Poznamenejme, že v předchozí definici mohou být R i R' různými typy okruhů, např. komutativními či nekomutativními tělesy, obory integrity nebo jen okruhy. Tuto problematiku nebudeme hlouběji rozebírat, naznačíme ji jen na příkladech; jde nám pouze o procvičení výše definovaných pojmů.

3.6. Příklady.

(i) Množina $2\mathbb{Z} = \{2z; z \in \mathbb{Z}\}$ všech sudých čísel, množina $3\mathbb{Z} = \{3z; z \in \mathbb{Z}\}$ všech celých čísel dělitelných třemi, obecně množina $n\mathbb{Z} = \{nz; z \in \mathbb{Z}\}$, kde $n \in \{0, 1, 2, \dots\}$, je podokruhem oboru integrity \mathbb{Z} . Není obtížné ukázat, že jiné podokruhy oboru integrity \mathbb{Z} nemá. Obor integrity \mathbb{Z} nemá žádný vlastní podobor integrity, neboť podokruhy $n\mathbb{Z}$, kde $n \neq 1$, nemají jednotkový prvek. $0\mathbb{Z} = \{0\}$ je tzv. *nulový podokruh*.

(ii) Obor integrity $\mathbb{Z}[i]$ je podoborem integrity komutativního tělesa \mathbb{C} , resp. nekomutativního tělesa \mathbb{H} .

(iii) Obor integrity \mathbb{Z} je podoborem integrity oboru integrity $\mathbb{Z}[i]$, resp. podoborem integrity komutativních těles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a nekomutativního tělesa \mathbb{H} . Výše uvedené okruhy $n\mathbb{Z}$, $n = 2, 3, \dots$, jsou rovněž podokruhy komutativních těles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a nekomutativního tělesa \mathbb{H} .

(iv) Těleso T je podtělesem oboru integrity $T[x]$; těleso T je totiž podmnožinou v $T[x]$, která je tvořena všemi polynomy nultého stupně a nulovým polynomem. Invertibilními prvky v $T[x]$ jsou právě všechny nenulové prvky tělesa T .

(v) Množina $\mathbb{Z}[\sqrt{2}]$ všech reálných čísel tvaru $a + b\sqrt{2}$, kde $a, b \in \mathbb{Z}$, je podobor integrity tělesa \mathbb{R} .

(vi) Množina $\mathbb{Q}[\sqrt{2}]$ všech reálných čísel tvaru $a + b\sqrt{2}$, kde $a, b \in \mathbb{Q}$, je podtělesem tělesa \mathbb{R} . Obdobné příklady získáme, zaměníme-li $\sqrt{2}$ např. $\sqrt{3}, \sqrt{5}$ apod.

(vii) Množina $\mathbb{Z}[i\sqrt{2}]$ všech komplexních čísel tvaru $a + bi\sqrt{2}$, kde $a, b \in \mathbb{Z}$, je podobor integrity tělesa \mathbb{C} .

(viii) Množina $\mathbb{Q}[i\sqrt{2}]$ všech komplexních čísel tvaru $a + bi\sqrt{2}$, kde $a, b \in \mathbb{Q}$, je podtělesem tělesa \mathbb{C} . Obdobné příklady získáme, zaměníme-li $\sqrt{2}$ např. $\sqrt{3}, \sqrt{5}$ apod.

(ix) Množina $\mathbb{Q}[i]$ všech komplexních čísel tvaru $a + bi$, kde $a, b \in \mathbb{Q}$, je podtělesem tělesa \mathbb{C} .

(x) Množina všech kvaternionů s celočíselnými koeficienty, tj. množina všech prvků tvaru $a + bi + cj + dk$, kde $a, b, c, d \in \mathbb{Z}$, je podoborem integrity tělesa \mathbb{H} .

(xi) Množina všech kvaternionů s racionálními koeficienty, tj. množina všech prvků tvaru $a + bi + cj + dk$, kde $a, b, c, d \in \mathbb{Q}$, je podtělesem tělesa \mathbb{H} .

(xii) Množina všech kvaternionů s komplexními koeficienty, tj. množina prvků tvaru $a + bI + cJ + dK$, kde $a, b, c, d \in \mathbb{C}$, je nekomutativním okruhem s jednotkovým prvkem, který má netriviální dělitele nuly (a není tedy oborem integrity ani tělesem); je totiž např.

$$(1 + iI) \cdot (-1 + iI) = 0 .$$

(xiii) Nechť R je okruh (těleso). Množina $R \times R$, na které jsou definovány operace sčítání a násobení po složkách, tj.

$$(a, b) + (c, d) = (a + c, b + d) , \quad (a, b) \cdot (c, d) = (ac, bd) ,$$

je okruh. Je-li okruh R komutativní, je okruh $R \times R$ komutativní; má-li okruh R jednotkový prvek 1, je prvek $(1, 1)$ jednotkovým prvkem okruhu $R \times R$. Je-li okruh R alespoň dvouprvkový, má okruh $R \times R$ netriviální dělitele nuly; pro $0 \neq a \in R$ je totiž

$$(a, 0) \cdot (0, a) = (0, 0) .$$

(xiv) Nechť X je množina a $\mathfrak{P}(X)$ množina všech jejích podmnožin (tzv. *potenční množina*). Na množině $\mathfrak{P}(X)$ uvažujme dvě binární operace, symetrickou diferenci „ \div “ a průnik „ \cap “; připomeňme, že pro podmnožiny A, B množiny X je

$$A \div B = (A \setminus B) \cup (B \setminus A) .$$

Množina $\mathfrak{P}(X)$ s těmito operacemi je komutativní okruh s jednotkovým prvkem. Sčítáním je symetrická diference, nulovým prvkem je prázdná množina, každá podmnožina A množiny X je opačným prvkem sama k sobě. Násobením je průnik, jednotkovým prvkem je množina X . Invertibilním prvkem tohoto okruhu je pouze množina X .

4. MATICE

4.1. Definice. Necht X je neprázdná množina a m, n přirozená čísla. *Maticí typu $n \times m$ nad množinou X* budeme rozumět obdélníkové schéma

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix},$$

kde $a_{ij} \in X$ pro každé $i = 1, \dots, n$ a každé $j = 1, \dots, m$; tuto matici budeme značit též $(a_{ij})_{n \times m}$ nebo jednodušeji (a_{ij}) . Jestliže je $m \neq n$, pak hovoříme o *obdélníkové matici typu $n \times m$* ; jestliže je $m = n$, hovoříme o *čtvercové matici řádu n* . Dále říkáme, že prvek a_{ij} stojí v matici na místě ij .

Dvě matice nad množinou X považujeme za *totožné* a říkáme, že se *rovnají*, jestliže mají stejný typ a jestliže jejich prvky na odpovídajících místech jsou stejné. V obvyklém smyslu užíváme termíny *řádek matice* a *sloupec matice*; matice typu $n \times m$ má tedy n řádků a m sloupců. U čtvercové matice (a_{ij}) řádu n tvoří *hlavní diagonálu* posloupnost $a_{11}, a_{22}, \dots, a_{nn}$ a *vedlejší diagonálu* posloupnost $a_{n1}, a_{n-1,2}, \dots, a_{1n}$.⁶

Uvědomme si, že každou matici (a_{ij}) typu $n \times m$ nad množinou X můžeme považovat za zobrazení množiny $\{1, 2, \dots, n\} \times \{1, 2, \dots, m\}$ do množiny X ; každé dvojici (i, j) , kde $1 \leq i \leq n$ a $1 \leq j \leq m$, toto zobrazení přiřazuje prvek $a_{ij} \in X$. Takto se někdy pojem matice zavádí.

4.2. Příklady.

(i) Nad množinou $X = \{\clubsuit, \diamond, \heartsuit, \spadesuit\}$ uvažujme matice

$$A = \begin{pmatrix} \clubsuit & \diamond \\ \heartsuit & \diamond \\ \spadesuit & \clubsuit \\ \clubsuit & \heartsuit \end{pmatrix}, \quad B = \begin{pmatrix} \spadesuit & \clubsuit & \heartsuit \\ \heartsuit & \spadesuit & \clubsuit \end{pmatrix}.$$

Matice A je typu 4×2 a matice B je typu 2×3 ; obě tyto matice jsou obdélníkové.

(ii) Nad množinou \mathbb{N} všech přirozených čísel uvažujme matice

$$C = \begin{pmatrix} 2 & 1 & 1 & 2 & 5 \\ 1 & 2 & 1 & 1 & 8 \\ 1 & 1 & 2 & 4 & 9 \end{pmatrix} \quad \text{a} \quad D = \begin{pmatrix} 2 & 1 & 1 & 5 \\ 1 & 2 & 1 & 7 \\ 1 & 1 & 2 & 5 \\ 9 & 8 & 6 & 6 \end{pmatrix}.$$

⁶ Termín *hlavní diagonála* se někdy užívá i u obdélníkových matic. Začíná v „levém horním rohu“ matice, ale nekončí v „pravém dolním rohu“.

Matice C je obdélníková typu 3×5 , matice D je čtvercová řádu 4.

V matematice hrají důležitou roli matice nad číselnými obory celých, racionálních, reálných, resp. komplexních čísel a obecněji matice nad tělesy či okruhy. Pro takovéto matice je totiž možno rozumným způsobem definovat sčítání a násobení.

V dalším textu budeme pro jednoduchost vyšetřovat matice nad komutativními okruhy. Definujme nyní sčítání a násobení takovýchto matic.

4.3. Definice. Nechť $A = (a_{ij})$ a $B = (b_{ij})$ jsou matice typu $n \times m$ nad komutativním okruhem R . *Součtem* těchto dvou matic budeme rozumět matici

$$A + B = (a_{ij} + b_{ij})$$

typu $n \times m$, která má na místě ij součet prvků stojících v maticích A a B na místě ij ; říkáme, že matice sčítáme *po složkách*.

Nechť $A = (a_{is})$ je matice typu $n \times m$ a $B = (b_{sj})$ matice typu $m \times k$ nad komutativním okruhem R . *Součinem* matic A, B (v tomto pořadí) budeme rozumět matici

$$A \cdot B = \left(\sum_{s=1}^m a_{is} b_{sj} \right)$$

typu $n \times k$, která má na místě ij součet součinů odpovídajících prvků i -tého řádku matice A a j -tého sloupce matice B ; řádky matice A mají totiž stejný počet prvků jako sloupce matice B .

Zdůrazněme, že součet $A + B$ matic A, B je definován jen tehdy, mají-li matice A, B stejný typ; součet $A + B$ má pak stejný typ jako matice A, B .

Součin $A \cdot B$ matic A, B je definován jen tehdy, má-li matice A stejný počet sloupců jako matice B řádků; součin $A \cdot B$ má pak stejný počet řádků jako matice A a stejný počet sloupců jako matice B . V celém následujícím textu již budeme většinou vynechávat symbol „ \cdot “ a místo $A \cdot B$ budeme psát stručněji AB .

4.4. Příklad. Jestliže

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & -1 & 1 \\ 1 & 2 & -2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & -1 \\ 2 & 3 & 1 \\ 3 & 1 & 0 \end{pmatrix}$$

jsou matice nad tělesem \mathbb{R} všech reálných čísel (nebo nad oborem integrity \mathbb{Z} všech celých čísel), potom je

$$\begin{aligned} A + B &= \begin{pmatrix} 3 & 1 & 0 \\ 1 & 3 & 1 \end{pmatrix}, \\ AC &= \begin{pmatrix} 1 \cdot 1 + 2 \cdot 2 - 1 \cdot 3 & 1 \cdot 0 + 2 \cdot 3 - 1 \cdot 1 & 1 \cdot (-1) + 2 \cdot 1 - 1 \cdot 0 \\ 0 \cdot 1 + 1 \cdot 2 + 3 \cdot 3 & 0 \cdot 0 + 1 \cdot 3 + 3 \cdot 1 & 0 \cdot (-1) + 1 \cdot 1 + 3 \cdot 0 \end{pmatrix} = \\ &= \begin{pmatrix} 2 & 5 & 1 \\ 11 & 6 & 1 \end{pmatrix}, \end{aligned}$$

$$BC = \begin{pmatrix} 3 & -2 & -3 \\ -1 & 4 & 1 \end{pmatrix}.$$

Součty $A + C$, $B + C$ a součiny AB , BA , CA , CB nejsou definovány.

4.5. Poznámka. Násobení matic nám může připadat — ve srovnání se sčítáním — velmi zvláštní a umělé. Ukážeme však, že právě takto definované násobení má smysl.

Uvažujme dvě tzv. *lineární substituce*

$$\begin{aligned} x &= ax' + by' , & x' &= ex'' + fy'' , \\ y &= cx' + dy' , & y' &= gx'' + hy'' , \end{aligned}$$

které můžeme symbolicky vyjádřit maticemi

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} , \quad \begin{pmatrix} e & f \\ g & h \end{pmatrix} .$$

Složíme-li tyto dvě substituce, tj. vyjádříme-li x a y v závislosti na x'' a y'' , dostaneme substituci

$$\begin{aligned} x &= (ae + bg)x'' + (af + bh)y'' , \\ y &= (ce + dg)x'' + (cf + dh)y'' , \end{aligned}$$

která je reprezentována maticí

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} .$$

Skládání lineárních substitucí tedy odpovídá násobení matic.

Tato souvislost bude později vyjádřena vztahem mezi násobením matic a skládáním homomorfismů vektorových prostorů (viz 11.4).

4.6. Věta. *Pro sčítání a násobení matic platí:*

- (i) *Sčítání matic je asociativní a komutativní.*
- (ii) *Násobení matic je asociativní.*
- (iii) *Násobení matic není komutativní.*
- (iv) *Násobení matic je distributivní vzhledem ke sčítání.*

Důkaz. (i) Jsou-li A, B, C matice téhož typu nad komutativním okruhem R , potom je zřejmé

$$(A + B) + C = A + (B + C) , \quad A + B = B + A .$$

Tyto rovnosti vyplývají z asociativního a komutativního zákona pro operaci sčítání v okruhu R . Na místě ij stojí totiž v uvedených maticích prvky

$$(a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij}) , \quad a_{ij} + b_{ij} = b_{ij} + a_{ij} .$$

(ii) Nechť $A = (a_{ij})$, $B = (b_{jr})$, $C = (c_{rs})$ jsou matice typu $k \times l$, $l \times m$, $m \times n$ nad okruhem R . Matice AB má na místě ir prvek

$$\sum_{j=1}^l a_{ij} b_{jr} ,$$

matice $(AB)C$ má tedy na místě is prvek

$$\sum_{r=1}^m \left(\sum_{j=1}^l a_{ij} b_{jr} \right) c_{rs} .$$

Matice BC má na místě js prvek

$$\sum_{r=1}^m b_{jr} c_{rs}$$

a matice $A(BC)$ má tedy na místě is prvek

$$\sum_{j=1}^l a_{ij} \left(\sum_{r=1}^m b_{jr} c_{rs} \right) .$$

Podle distributivního zákona pro operace sčítání a násobení v okruhu R je však

$$\sum_{r=1}^m \left(\sum_{j=1}^l a_{ij} b_{jr} \right) c_{rs} = \sum_{j=1}^l a_{ij} \left(\sum_{r=1}^m b_{jr} c_{rs} \right) ,$$

takže je $(AB)C = A(BC)$.⁷

(iii) Vzhledem k tomu, že např. pro matice

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad \text{a} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

je

$$AB = \begin{pmatrix} 2 & 3 \\ 4 & 7 \end{pmatrix} \quad \text{a} \quad BA = \begin{pmatrix} 3 & 4 \\ 4 & 6 \end{pmatrix} ,$$

není násobení matic komutativní.

Uvědomme si ještě, že pro dané matice C , D může být definován součin CD a nemusí být definován součin DC ; pokud jsou definovány oba součiny, jsou CD a DC čtvercové matice, které však nemusí mít stejný řád. Oba součiny existují

⁷ Zkuste z metodických důvodů tuto rovnost prověřit pro čtvercové matice řádu 2.

a mají stejný řád právě tehdy, když jsou C a D čtvercové matice stejného řádu. Pokud je potom $CD = DC$, hovoříme o *záměnných* nebo *komutujících* maticích.

(iv) Nechť $A = (a_{ij})$ je matice typu $n \times m$ a $B = (b_{jr})$, $C = (c_{jr})$ matice typu $m \times k$ nad okruhem R . Matice $A(B + C)$ má na místě ir prvek

$$\sum_{j=1}^m a_{ij}(b_{jr} + c_{jr}) ,$$

matice $AB + AC$ má na místě ir prvek

$$\sum_{j=1}^m a_{ij}b_{jr} + \sum_{j=1}^m a_{ij}c_{jr} .$$

Vzhledem k početním zákonům platným v okruhu R jsou si tyto prvky rovny, takže je $A(B + C) = AB + AC$. Stejným způsobem dokážeme platnost distributivního zákona $(A + B)C = AC + BC$. \square

4.7. Definice. *Nulovou maticí* typu $n \times m$ nad komutativním okruhem R budeme rozumět matici $O = (a_{ij})$, kde $a_{ij} = 0$ pro každé $i = 1, \dots, n$ a $j = 1, \dots, m$.

Opačnou maticí k matici $A = (a_{ij})$ typu $n \times m$ nad komutativním okruhem R budeme rozumět matici $-A = (-a_{ij})$ stejného typu.

Nulová matice má na všech místech nulový prvek okruhu R . Opačná matice $-A$ k matici A má na každém místě ij opačný prvek k prvku, který je na místě ij v matici A . Důkaz následujících tvrzení je zřejmý.

4.8. Věta. *Nechť O je nulová matice typu $n \times m$ nad komutativním okruhem R . Potom pro každou matici A typu $n \times m$ nad okruhem R je*

$$A + O = O + A = A \quad a \quad A + (-A) = (-A) + A = O . \quad \square$$

4.9. Definice. *Jednotkovou maticí* řádu n nad komutativním okruhem R s jednotkovým prvkem budeme rozumět matici $E = (\delta_{ij})$, kde

$$\delta_{ij} = \begin{cases} 1 & \text{pro } i, j = 1, \dots, n, i = j , \\ 0 & \text{pro } i, j = 1, \dots, n, i \neq j . \end{cases}$$

Symbol δ_{ij} se nazývá *Kroneckerovo delta*.

Důkaz následujícího tvrzení je zřejmý; stačí si uvědomit, jak se matice násobí.

4.10. Věta. *Nechť E je jednotková matice řádu n nad komutativním okruhem R s jednotkovým prvkem a nechť m je přirozené číslo. Potom pro každou matici A typu $n \times m$ nad okruhem R je $EA = A$ a pro každou matici B typu $m \times n$ nad okruhem R je $BE = B$. \square*

Nechť R je nějaký komutativní okruh a M množina všech matic nad okruhem R . Ani sčítání matic, ani násobení matic není binární operací na množině M , neboť není definován ani součet ani součin libovolně zvolených matic množiny M ; sčítání a násobení matic na množině M jsou tzv. *parciální operace*. Chceme-li sčítání a násobení matic uvažovat jako binární operace, musíme od množiny M přejít k „menší“ množině.

4.11. Věta. *Množina $R^{n \times n}$ všech čtvercových matic řádu n nad komutativním okruhem R tvoří spolu s operacemi sčítání a násobení okruh. Má-li okruh R jednotkový prvek, má i okruh $R^{n \times n}$ jednotkový prvek.*

Důkaz. Sčítání a násobení čtvercových matic řádu n je vždy definováno a výsledkem je opět matice řádu n ; jde tedy o binární operace na množině $R^{n \times n}$. Podle 4.6(i),(ii) a (iv) je sčítání asociativní a komutativní, násobení je asociativní a je se sčítáním svázáno distributivními zákony. Podle 4.8 je dále splněn i axiom nulového a opačného prvku. Množina $R^{n \times n}$ je tedy okruhem. Má-li okruh R jednotkový prvek, má podle 4.10 i okruh $R^{n \times n}$ jednotkový prvek. \square

Poznamenejme, že má-li okruh R alespoň dva prvky, má okruh $R^{n \times n}$ pro $n > 1$ netriviální dělitele nuly. Např. pro $0 \neq a \in R$ a $n = 2$ je

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Okruh $R^{1 \times 1}$ čtvercových matic řádu 1 je komutativní, neboť R je komutativní; okruh $R^{1 \times 1}$ se jen „nepodstatně liší“ od okruhu R (v algebře říkáme, že jsou tyto okruhy *izomorfní*). Okruh $T^{n \times n}$ čtvercových matic řádu $n > 1$ nad tělesem T není komutativní; pro $n = 2$ je např.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

4.12. Definice. *Nechť R je komutativní okruh s jednotkovým prvkem a A čtvercová matice řádu n nad R . Inverzní maticí k matici A budeme rozumět matici A^{-1} , pro kterou je $AA^{-1} = A^{-1}A = E$. Matice A , ke které inverzní matice existuje, se nazývá *invertibilní*.*

4.13. Příklady.

(i) Nechť R je okruh s jednotkovým prvkem. Jednotková matice E řádu n je invertibilní; je totiž $E^{-1} = E$, tj. E je sama k sobě inverzní.

Invertibilními maticemi jsou např. matice

$$A = \begin{pmatrix} 1 & 0 & a & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ a & b & 0 & 1 \end{pmatrix}.$$

Je totiž

$$A^{-1} = \begin{pmatrix} 1 & 0 & -a & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -a & -b & 0 & 1 \end{pmatrix}.$$

Dále je např.

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ ac-b & -c & 1 \end{pmatrix}.$$

(ii) Invertibilními maticemi nad tělesem reálných čísel \mathbb{R} jsou např. matice

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

Je totiž

$$A^{-1} = \begin{pmatrix} \frac{3}{4} & -\frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{3}{4} & -\frac{1}{4} \\ -\frac{1}{4} & -\frac{1}{4} & \frac{3}{4} \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}.$$

4.14. Věta. *Nechť R je komutativní okruh s jednotkovým prvkem a A, B invertibilní matice téhož řádu nad R . Potom je rovněž matice AB invertibilní a je*

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Důkaz. Předpokládejme, že A a B jsou invertibilní matice téhož řádu nad okruhem R . Potom je

$$(AB) \cdot (B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AEA^{-1} = AA^{-1} = E$$

a podobně $(B^{-1}A^{-1}) \cdot AB = E$. Matice AB a $B^{-1}A^{-1}$ jsou tedy navzájem inverzní. \square

V následující definici zavedeme tzv. *násobení matic skaláry*.

4.15. Definice. Nechť $A = (a_{ij})$ je matice typu $n \times m$ nad komutativním okruhem R a nechť $c \in R$ je libovolný prvek. c -násobkem matice A budeme rozumět matici

$$c \cdot A = (c \cdot a_{ij}) ,$$

typu $n \times m$, která má na místě ij c -násobek prvku, který v matici A stojí na místě ij .

Symbol „ \cdot “ budeme často vynechávat.

4.16. Příklad. Jestliže

$$C = \begin{pmatrix} 2 & 1 & 3 \\ 4 & -1 & 8 \\ 2 & 1 & 9 \end{pmatrix} \quad \text{a} \quad D = \begin{pmatrix} 2 & -1 & 2 & 5 \\ 3 & 7 & -1 & 7 \end{pmatrix}$$

jsou matice nad tělesem \mathbb{R} , potom

$$3C = \begin{pmatrix} 6 & 3 & 9 \\ 12 & -3 & 24 \\ 6 & 3 & 27 \end{pmatrix} \quad \text{a} \quad -2D = \begin{pmatrix} -4 & 2 & -4 & -10 \\ -6 & -14 & 2 & -14 \end{pmatrix} .$$

Na řádky, resp. sloupce matice A typu $n \times m$ se můžeme dívat jako na matice typu $1 \times m$, resp. $n \times 1$. Ve smyslu předcházející definice tedy můžeme hovořit o c -násobku řádku, resp. sloupce matice A .

Na násobení matic se můžeme podívat „sloupcově“ nebo „řádkově“. Obou těchto pohledů je často možno s úspěchem využít. Nechť $B = (b_{ik})$ je matice typu $p \times q$ a $C = (c_{kj})$ matice typu $q \times r$ nad okruhem R .

První sloupec matice BC je součtem c_{11} -násobku prvního sloupce matice B , c_{21} -násobku druhého sloupce matice B , \dots , c_{q1} -násobku posledního, tj. q -tého sloupce matice B . Obecně j -tý sloupec matice BC je součtem c_{1j} -násobku prvního sloupce matice B , c_{2j} -násobku druhého sloupce matice B , \dots , c_{qj} -násobku posledního, tj. q -tého sloupce matice B .

Obdobně je první řádek matice BC součtem b_{11} -násobku prvního řádku matice C , b_{12} -násobku druhého řádku matice C , \dots , b_{1q} -násobku posledního, tj. q -tého řádku matice C . Obecně j -tý řádek matice BC je součtem b_{j1} -násobku prvního řádku matice C , b_{j2} -násobku druhého řádku matice C , \dots , b_{jq} -násobku posledního, tj. q -tého řádku matice C .

Následující tvrzení vyplývají z vlastností maticových operací.

4.17. Věta. Nechť A, B jsou matice nad komutativním okruhem R , které je možno sečíst, resp. vynásobit; nechť $c, d \in R$. Potom platí:

- (i) $c(A + B) = cA + cB$,
- (ii) $(c + d)A = cA + dA$,
- (iii) $(cd)A = c(dA)$,
- (iv) $c(AB) = (cA)B = A(cB)$.

Jestliže má okruh R jednotkový prvek, potom

$$(v) \ 1A = A . \quad \square$$

V lineární algebře a v maticovém počtu hraje důležitou roli *transponování* matic.

4.18. Definice. Nechť $A = (a_{ij})$ je matice typu $n \times m$ nad komutativním okruhem R . *Transponovanou maticí* k matici A budeme rozumět matici $A^T = (b_{ji})$ typu $m \times n$, kde pro každé $i = 1, \dots, n$ a $j = 1, \dots, m$ je $b_{ji} = a_{ij}$.

4.19. Příklad. Transponovanými maticemi k maticím

$$C = \begin{pmatrix} 2 & 1 & 1 & 2 & 5 \\ 1 & 2 & 1 & 1 & 8 \\ 1 & 1 & 2 & 4 & 9 \end{pmatrix} \quad \text{a} \quad D = \begin{pmatrix} 2 & 1 & 1 & 5 \\ 1 & 2 & 1 & 7 \\ 1 & 1 & 2 & 5 \\ 9 & 8 & 6 & 6 \end{pmatrix} .$$

jsou matice

$$C^T = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \\ 2 & 1 & 4 \\ 5 & 8 & 9 \end{pmatrix} \quad \text{a} \quad D^T = \begin{pmatrix} 2 & 1 & 1 & 9 \\ 1 & 2 & 1 & 8 \\ 1 & 1 & 2 & 6 \\ 5 & 7 & 5 & 6 \end{pmatrix} .$$

Transponovaná matice vznikne „převrácením“ původní matice podle její hlavní diagonály, resp. záměnou řádků a sloupců.

Připomeňme znovu, že matice může mít pouze jediný sloupec nebo jediný řádek, např.

$$C = \begin{pmatrix} 2 \\ 3 \end{pmatrix} , \quad D = (8 \ 5 \ 3 \ 7) .$$

Potom

$$C^T = (2 \ 3) , \quad D^T = \begin{pmatrix} 8 \\ 5 \\ 3 \\ 7 \end{pmatrix} .$$

4.20. Věta. Nechť A, B jsou matice nad komutativním okruhem R , které je možno sečíst, resp. vynásobit, nechť $c \in R$. Potom platí:

- (i) $(A + B)^T = A^T + B^T$,
- (ii) $(AB)^T = B^T A^T$,
- (iii) $(cA)^T = cA^T$,
- (iv) $(A^T)^T = A$.

Jestliže je A čtvercová invertibilní matice, potom je matice A^T rovněž invertibilní a je

$$(v) \ (A^T)^{-1} = (A^{-1})^T .$$

Důkaz. Rovnosti uvedené v (i), (iii) a (iv) jsou zjevné.

Dokážeme rovnost (ii). Předpokládejme, že $A = (a_{is})$ je matice typu $n \times m$ a $B = (b_{sj})$ je matice typu $m \times k$ nad okruhem R . Matice $(AB)^T$ typu $k \times n$ má na místě ji prvek, který má matice AB na místě ij , tj. prvek $\sum_{s=1}^m a_{is}b_{sj}$. Matice B^T typu $k \times m$ má na místě js prvek b_{sj} , matice A^T typu $m \times n$ na místě si prvek a_{is} a matice $B^T A^T$ na místě ji prvek

$$\sum_{s=1}^m b_{sj}a_{is} = \sum_{s=1}^m a_{is}b_{sj} ,$$

tj. stejný prvek jako matice $(AB)^T$.

Nakonec dokážeme rovnost (v). Z rovnosti

$$A \cdot A^{-1} = A^{-1} \cdot A = E$$

vyplývá podle tvrzení (ii) rovnost

$$(A^{-1})^T \cdot A^T = A^T \cdot (A^{-1})^T = E^T = E .$$

Odtud $(A^T)^{-1} = (A^{-1})^T$. \square

Poznamenejme, že matice A a A^T se vzhledem k 4.20(iv) nazývají *navzájem transponované*.

V následujícím se budeme věnovat speciálním typům matic.

4.21. Definice. Nechť R je komutativní okruh. *Diagonální maticí* nad okruhem R budeme rozumět každou matici, která má mimo hlavní diagonálu samé nulové prvky.

Obdélníková matice $A = (a_{ij})$ typu $n \times m$ je tedy diagonální, jestliže pro každé $i = 1, \dots, n$ a $j = 1, \dots, m$, $i \neq j$, je $a_{ij} = 0$.

4.22. Příklady. Diagonálními maticemi nad oborem integrity \mathbb{Z} jsou např. matice

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}, \quad (3 \ 0 \ 0 \ 0) .$$

4.23. Definice. Nechť $A = (a_{ij})$ je čtvercová matice řádu n nad komutativním okruhem R . Řekneme, že matice A je

- (i) *skalární*, jestliže pro každé $i, j = 1, \dots, n$, $i \neq j$, je $a_{ij} = 0$ a $a_{ii} = c \in R$;
- (ii) *horní trojúhelníková*, jestliže pro každé $i, j = 1, \dots, n$, $i > j$, je $a_{ij} = 0$;
- (iii) *dolní trojúhelníková*, jestliže pro každé $i, j = 1, \dots, n$, $i < j$, je $a_{ij} = 0$;
- (iv) *symetrická*, jestliže pro každé $i, j = 1, \dots, n$ je $a_{ij} = a_{ji}$;
- (v) *antisymetrická*, jestliže pro každé $i, j = 1, \dots, n$ je $a_{ij} = -a_{ji}$.

Nechť $A = (a_{ij})$ je čtvercová matice řádu n nad tělesem \mathbb{C} komplexních čísel. Řekneme, že matice A je

(vi) *hermitovská*, jestliže pro každé $i, j = 1, \dots, n$ je $a_{ij} = \bar{a}_{ji}$.

Horní (dolní) trojúhelníková matice má pod (nad) hlavní diagonálou samé nuly.

Poznamenejme, že čtvercová matice A je symetrická, právě když je $A^T = A$; symetrická matice je „souměrná podle hlavní diagonály“. Matice A je antisymetrická právě tehdy, když je $A^T = -A$. Pro antisymetrickou matici musí být $a_{ii} = -a_{ii}$, tj. $2a_{ii} = 0$; antisymetrická matice nad tělesem, které nemá charakteristiku 2, má tedy na hlavní diagonále nuly.

Čtvercová matice A je hermitovská, právě když je $A^T = \bar{A}$; matice \bar{A} má na místě ij komplexně sdružené číslo k číslu, které je v matici A na místě ij . Hermitovská matice má na hlavní diagonále reálná čísla.

4.24. Příklady. Uvažujme matice

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 2 & 5 \\ 0 & 4 & -2 \\ 0 & 0 & 6 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 3 & -1 & 0 & 0 \\ 4 & 0 & 3 & 0 \\ 2 & -5 & -6 & 2 \end{pmatrix},$$

$$M = \begin{pmatrix} 3 & 2 & -5 \\ 2 & 2 & 4 \\ -5 & 4 & 3 \end{pmatrix}, \quad N = \begin{pmatrix} 0 & -2 & 1 \\ 2 & 0 & 2 \\ -1 & -2 & 0 \end{pmatrix}$$

nad oborem integrity \mathbb{Z} . Matice A je skalární, matice B horní trojúhelníková a matice C dolní trojúhelníková; matice M je symetrická, matice N antisymetrická.

Matice

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

nad tělesem \mathbb{Z}_2 je současně symetrická i antisymetrická, neboť v \mathbb{Z}_2 je $1 = -1$.

4.25. Definice. *Stopou* $\text{tr } A$ čtvercové matice $A = (a_{ij})$ řádu n rozumíme součet prvků na její hlavní diagonále, tj.

$$\text{tr } A = \sum_{i=1}^n a_{ii}.$$

Důkazy následujících tvrzení nepředstavují problém.

4.26. Věta. *Jsou-li A, B čtvercové matice téhož řádu nad komutativním okruhem R a $c \in R$, potom*

- (i) $\text{tr}(A + B) = \text{tr } A + \text{tr } B$,
- (ii) $\text{tr}(cA) = c \cdot \text{tr } A$,
- (iii) $\text{tr } A^T = \text{tr } A$.

Jsou-li $A = (a_{ij})$ a $B = (b_{ji})$ matice typu $p \times q$, $q \times p$, potom

$$(iv) \operatorname{tr}(AB) = \operatorname{tr}(BA) = \sum_{i=1}^p \sum_{j=1}^q a_{ij}b_{ji} . \quad \square$$

Vodorovnými a svislými čarami můžeme matici rozdělit na tzv. *bloky* neboli *dílčí matice*. Obecně je to možno provést mnoha způsoby, v konkrétním případě to vypadá např. takto:

$$\left(\begin{array}{c|cc} 1 & 2 & 3 \\ \hline 4 & 5 & 6 \\ \hline - & - & - \\ \hline 7 & 8 & 9 \end{array} \right), \quad \left(\begin{array}{ccc} 1 & 2 & 3 \\ - & - & - \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array} \right), \quad \left(\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 4 & 5 & 6 \\ \hline - & - & - \\ \hline 7 & 8 & 9 \end{array} \right).$$

Matice A , která je nějakým způsobem rozdělena na bloky, se obvykle nazývá *bloková*; takovou matici zapisujeme v tvaru

$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1m} \\ A_{21} & A_{22} & \dots & A_{2m} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nm} \end{pmatrix};$$

dílčí matice stojící ve stejném sloupci blokové matice A mají stejný počet sloupců, dílčí matice stojící ve stejném řádku blokové matice A mají stejný počet řádků.

Je-li $m = n$ a jsou-li matice $A_{11}, A_{22}, \dots, A_{nn}$ čtvercové (hovoříme o tzv. *hlavní diagonále* blokové matice), pak se matice A nazývá *čtvercová bloková matice řádu n* .

4.27. Definice. Nechť $A = (A_{ij})$ je čtvercová bloková matice řádu n nad komutativním okruhem R . Řekneme, že matice A je

- (i) *horní trojúhelníková*, jestliže pro každé $i, j = 1, \dots, n$, $i > j$, je $A_{ij} = O$;
- (ii) *dolní trojúhelníková*, jestliže pro každé $i, j = 1, \dots, n$, $i < j$, je $A_{ij} = O$;
- (iii) *diagonální*, jestliže pro každé $i, j = 1, \dots, n$, $i \neq j$, je $A_{ij} = O$.

Z jednotlivých matic můžeme sestavovat blokové matice. Jsou-li např. A, B, C čtvercové matice stejného řádu a E , resp. O jednotková, resp. nulová matice téhož řádu, můžeme utvořit matice

$$\begin{pmatrix} A & | & E \end{pmatrix}, \quad \begin{pmatrix} A & | & B \end{pmatrix},$$

$$\begin{pmatrix} A & B \\ O & C \end{pmatrix}, \quad \begin{pmatrix} A \\ - \\ E \end{pmatrix}, \quad \begin{pmatrix} A \\ - \\ B \end{pmatrix}.$$

4.28. Poznámka. Kromě výše definovaného násobení matic se v matematice užívá i tzv. Hadamardův součin a Kroneckerův součin.

Nechť $A = (a_{ij})$ a $B = (b_{ij})$ jsou matice typu $n \times m$ nad komutativním okruhem R . *Hadamardovým součinem* matic A, B budeme rozumět matici

$$A * B = (a_{ij}b_{ij})$$

typu $n \times m$. V tomto případě se matice násobí „po složkách“.

Tato operace je zřejmě asociativní a komutativní, je rovněž distributivní vzhledem ke sčítání. Množina $R^{n \times m}$ všech matic typu $n \times m$ nad okruhem R je komutativním okruhem. Má-li okruh R jednotkový prvek, má i okruh $R^{n \times m}$ jednotkový prvek; je jím matice, která má na všech nm místech jednotkový prvek okruhu R . Invertibilními maticemi tohoto okruhu (vzhledem k Hadamardově součinu) jsou zřejmě právě ty matice, které mají na všech svých místech nenulové prvky.

Nechť $A = (a_{ij})$ a je matice typu $n \times m$ a B matice typu $p \times q$ nad komutativním okruhem R . *Kroneckerovým součinem* matic A, B budeme rozumět blokovou matici

$$A \otimes B = (a_{ij}B)$$

typu $np \times mq$. Tuto matici můžeme chápat jako blokovou matici; sestává z nm bloků — jsou to a_{ij} -násobky matice B .

Snadno se ověří následující vlastnosti Kroneckerova součinu (A_1, A_2 jsou matice stejného typu, B_1, B_2 rovněž matice stejného typu):

- (i) $O \otimes A = A \otimes O = O$,
- (ii) $(A_1 + A_2) \otimes B = A_1 \otimes B + A_2 \otimes B$,
- (iii) $A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2$,
- (iv) $(A \otimes B)^T = A^T \otimes B^T$,
- (v) $(aA) \otimes (bB) = ab \cdot (A \otimes B)$.

Jsou-li matice A, B invertibilní, je

$$(vi) (A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

4.29. Příklady. Nechť

$$A = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 & -2 \\ 0 & 1 & -2 \\ 0 & 3 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}.$$

Potom

$$A * B = \begin{pmatrix} 3 & -1 & -4 \\ 0 & 1 & -4 \\ 0 & 3 & -3 \end{pmatrix}, \quad A \otimes C = \begin{pmatrix} 3 & -3 & 1 & -1 & 2 & -2 \\ 6 & 3 & 2 & 1 & 4 & 2 \\ 1 & -1 & 1 & -1 & 2 & -2 \\ 2 & 1 & 2 & 1 & 4 & 2 \\ 2 & -2 & 1 & -1 & 3 & -3 \\ 4 & 2 & 2 & 1 & 6 & 3 \end{pmatrix}.$$

Poznamenejme, že součiny $A * C$ a $B * C$ neexistují.

5. GRUPY

Grupa je algebraická struktura s jednou binární operací, která má jisté vlastnosti. Podle toho, zda tuto operaci chápeme aditivně nebo multiplikativně, tj. zda ji zapisujeme jako sčítání nebo násobení, má příslušná definice dvojí podobu. Z metodických důvodů uvedeme obě verze.

5.1a. Definice. Množina G s binární operací " + " (sčítání) se nazývá *grupa*, jestliže platí následující axiomy:

- (i) $\forall a, b, c \in G \quad (a + b) + c = a + (b + c)$,
- (iii) $\exists 0 \in G \quad \forall a \in G \quad a + 0 = 0 + a = a$,
- (iv) $\forall a \in G \quad \exists -a \in G \quad a + (-a) = (-a) + a = 0$.

Pokud ještě platí axióm

- (ii) $\forall a, b \in G \quad a + b = b + a$,

pak hovoříme o *komutativní grupě*, resp. *Abelově grupě*.

5.1b. Definice. Množina G s binární operací " \cdot " (násobení) se nazývá *grupa*, jestliže platí následující axiomy:

- (v) $\forall a, b, c \in G \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- (vi) $\exists 1 \in G \quad \forall a \in G \quad a \cdot 1 = 1 \cdot a = a$,
- (vii) $\forall a \in G \quad \exists a^{-1} \in G \quad a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Pokud ještě platí axióm

- (x) $\forall a, b \in G \quad a \cdot b = b \cdot a$,

pak hovoříme o *komutativní grupě*, resp. *Abelově grupě*.

Poznamenejme, že jsme v definicích 5.1a a 5.1b užili pro axiomy grupy stejné číslování jako pro odpovídající axiomy tělesa, resp. okruhu v definicích 2.1, resp. 3.1.

V aditivním případě hovoříme o *nulovém* a *opačném* prvku (viz (iii), (iv)), v multiplikativním případě o *jednotkovém* a *inverzním* prvku (viz (vi), (vii)). Aditivní zápis se používá zejména pro komutativní grupy.

5.2. Poznámka. Pokud bychom náš výklad úvodních partií obecné algebry začali definicí grupy, mohli bychom definice okruhu a tělesa podat stručněji.

Okruhem je množina se dvěma binárními operacemi, sčítáním a násobením, která je vzhledem ke sčítání komutativní grupou, násobení je asociativní a je se sčítáním svázáno distributivními zákony.

Tělesem je okruh, jehož množina nenulových prvků je grupou vzhledem k násobení; je-li tato grupa komutativní, jde o komutativní těleso.

5.3. Příklady.

(i) Nechť T je (komutativní) těleso. Množina T je vzhledem ke sčítání komutativní grupou. Množina $T \setminus \{0\}$ je vzhledem k násobení (komutativní) grupou. Hovoříme tedy o aditivní grupě racionálních, resp. reálných, resp. komplexních čísel, resp.

kvaternionů, o multiplikatívni grupě nenulových racionálních, resp. nenulových reálných, resp. nenulových komplexních čísel, resp. o nekomutativní multiplikatívni grupě nenulových kvaternionů. Rovněž můžeme hovořit o aditivní grupě \mathbb{Z}_p , resp. o multiplikatívni grupě $\mathbb{Z}_p \setminus \{0\}$.

(ii) Multiplikatívni grupami jsou i množiny všech kladných racionálních, resp. kladných reálných čísel.

(iii) Multiplikatívni grupou je rovněž množina všech komplexních čísel, které mají jednotkovou absolutní hodnotu.

(iv) Multiplikatívni grupou je i dvouprvková množina $\{1, -1\}$.

(v) Nechť R je okruh. Množina R je vzhledem ke sčítání komutativní grupou. Hovoříme tedy o aditivní grupě celých čísel, resp. Gaussových celých čísel, resp. polynomů z $T[x]$, resp. reálných funkcí na intervalu (a, b) , resp. o aditivní grupě okruhu \mathbb{Z}_n apod.

(vi) Ani množina \mathbb{N} všech přirozených čísel, ani množina $\mathbb{N} \cup \{0\}$ všech celých nezáporných čísel vzhledem ke sčítání není grupou.

(vii) Množina $R^{m \times n}$ všech matic typu $m \times n$ nad okruhem R tvoří spolu s operací sčítání komutativní grupu.

(viii) Množina všech čtvercových invertibilních matic řádu n nad tělesem T (viz 4.12, 4.14) tvoří vzhledem k násobení grupu. Tato grupa se nazývá *obecná lineární grupa* a značí se zpravidla $GL(T, n)$ nebo $GL(n)$.

5.4. Příklad. Uvažujme pravidelný n -úhelník ($n \geq 3$) a všechny jeho *symetrie*, tj. „pohyby“, kterými tento n -úhelník přechází sám v sebe. Jde o n rotací kolem středu uvažovaného n -úhelníku o úhel

$$0 \cdot \frac{360^\circ}{n}, \quad 1 \cdot \frac{360^\circ}{n}, \quad 2 \cdot \frac{360^\circ}{n}, \quad \dots, \quad (n-1) \cdot \frac{360^\circ}{n}$$

a n osových souměrností; je-li n sudé, procházejí osy $\frac{n}{2}$ osových souměrností protějšími vrcholy n -úhelníku a osy $\frac{n}{2}$ osových souměrností středy protějších stran, je-li n liché, prochází osa každé osové souměrnosti jedním vrcholem n -úhelníku a středem jeho protější strany.

Vzhledem k tomu, že složení symetrií je symetrie, operace skládání symetrií je asociativní, identické zobrazení (tj. rotace o úhel 0°) je symetrie a ke každé symetrii existuje symetrie inverzní, je množina všech symetrií n -úhelníku grupou vzhledem ke skládání. Je to tzv. *dihedrální grupa*, má $2n$ prvků.

V nejjednodušším případě, kdy jde o symetrie rovnostranného trojúhelníku, jde o grupu, která má 6 prvků. Označíme-li vrcholy uvažovaného trojúhelníku čísla 1, 2, 3, můžeme jednotlivé symetrie reprezentovat „tabulkami“, ve kterých jsou v horním řádku vrcholy 1, 2, 3 a ve spodním řádku jejich obrazy při dané symetrii. Rotace o 0° , 120° , 240° jsou tedy zaznamenány tabulkami

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

a symetrie, jejichž osy procházejí vrcholem 1, resp. 2, resp. 3, jsou zaznamenány tabulkami

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Snadno se přesvědčíme, že tato grupa není komutativní.

5.5. Definice. Nechť G a H jsou multiplikativní grupy. Zobrazení f grupy G do grupy H se nazývá *homomorfismus*, jestliže

$$\forall a, b \in G \quad f(a \cdot b) = f(a) \cdot f(b).$$

Jestliže je zobrazení f injektivní, resp. surjektivní, resp. bijektivní, hovoříme o *monomorfismu*, resp. *epimorfismu*, resp. *izomorfismu*. Homomorfismus grupy G do téže grupy G se nazývá *endomorfismus* grupy G ; je-li navíc bijektivní, pak hovoříme o *automorfismu* grupy G . Množinu všech endomorfismů, resp. automorfismů grupy G značíme $\text{End } G$, resp. $\text{Aut } G$.

Zobrazení, které každému prvku grupy G přiřadí jednotkový prvek grupy H , je homomorfismus, který se nazývá *triviální*. Zobrazení, které každému prvku grupy G přiřadí týž prvek g , je automorfismus grupy G ; nazývá se *identický automorfismus* grupy G a značí se obvykle 1_G .

Jestliže f je homomorfismus grupy G_1 do grupy G_2 a g homomorfismus grupy G_2 do grupy G_3 , potom je složené zobrazení gf homomorfismus grupy G_1 do grupy G_3 ; pro každé dva prvky a, b grupy G_1 je totiž

$$(gf)(ab) = g(f(ab)) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b)) = (gf)(a) \cdot (gf)(b).$$

Jsou-li f a g monomorfismy, resp. epimorfismy, resp. izomorfismy (endomorfismy, resp. automorfismy), je gf rovněž monomorfismus, resp. epimorfismus, resp. izomorfismus (endomorfismus, resp. automorfismus). Skládání homomorfismů je asociativní, neboť je asociativní skládání zobrazení.

Pro každý endomorfismus f grupy G je zřejmé

$$f \cdot 1_G = 1_G \cdot f = f.$$

Jestliže je f izomorfismus grupy G na grupu H , potom inverzní zobrazení f^{-1} je izomorfismus grupy H na grupu G . Zřejmě je f^{-1} bijekce; stačí tedy dokázat, že pro každé dva prvky $a, b \in H$ je $f^{-1}(ab) = f^{-1}(a) \cdot f^{-1}(b)$. Označme c, d prvky grupy G , pro které je $f(c) = a$ a $f(d) = b$; prvky c, d existují a jsou určeny jednoznačně, neboť f je bijekce. Nyní je

$$f^{-1}(ab) = f^{-1}(f(c) \cdot f(d)) = f^{-1}(f(cd)) = cd = f^{-1}(a) \cdot f^{-1}(b).$$

5.6. Poznámka. Pro aditivní grupy G, H je homomorfismem grupy G do grupy H každé zobrazení, pro které je

$$\forall a, b \in G \quad f(a + b) = f(a) + f(b) .$$

Všechny výše zavedené pojmy zůstanou nezměněny; např. *triviální homomorfismus* neboli *nulový homomorfismus* zobrazuje všechny prvky grupy G na nulový prvek grupy H . Výše uvedený důkaz tvrzení, že složení homomorfismů je homomorfismus, vypadá v aditivním případě takto:

$$(gf)(a+b) = g(f(a+b)) = g(f(a)+f(b)) = g(f(a))+g(f(b)) = (gf)(a)+(gf)(b) .$$

Podobným způsobem se modifikuje důkaz rovnosti

$$f \cdot 1_G = 1_G \cdot f = f ,$$

resp. důkaz faktu, že inverzní zobrazení k izomorfismu je izomorfismus.

Poznamenejme, že jestliže je grupa G multiplikativní a grupa H aditivní, pak zobrazení f grupy G do grupy H se nazývá homomorfismus, jestliže

$$\forall a, b \in G \quad f(ab) = f(a) + f(b) .$$

5.7. Věta. *Množina $\text{Aut } G$ všech automorfismů grupy G spolu se skládáním automorfismů je grupa.*

Důkaz. Viděli jsme, že skládání automorfismů grupy G je asociativní binární operací na množině $\text{Aut } G$. Identický automorfismus 1_G grupy G je jednotkovým prvkem vzhledem ke skládání automorfismů. Ke každému automorfismu f grupy G existuje automorfismus f^{-1} , pro který je

$$f \cdot f^{-1} = f^{-1} \cdot f = 1_G .$$

Množina $\text{Aut } G$ je tedy grupa. \square

Jestliže je G komutativní grupa, pak grupovou operaci píšeme zpravidla aditivně. V tomto případě můžeme vedle skládání endomorfismů grupy G definovat i jejich sčítání. Jestliže f a g jsou endomorfismy komutativní grupy G , definujeme zobrazení $f + g$ grupy G do grupy G rovností

$$(f + g)(a) = f(a) + g(a) .$$

Zobrazení $f + g$ je endomorfismus grupy G , neboť pro každé dva prvky a, b grupy G je

$$\begin{aligned} (f + g)(a + b) &= f(a + b) + g(a + b) = f(a) + f(b) + g(a) + g(b) = \\ &= f(a) + g(a) + f(b) + g(b) = (f + g)(a) + (f + g)(b) . \end{aligned}$$

Povšimněme si, že jsme při třetí rovnosti opravdu využili komutativitu sčítání prvků grupy G ; pro nekomutativní grupy (psané multiplikativně) nelze obdobnou operaci násobení endomorfismů zavést. Sčítání endomorfismů aditivně psané komutativní grupy G je tedy binární operací na množině $\text{End } G$.

5.8. Věta. *Množina $\text{End } G$ všech endomorfismů aditivně psané komutativní grupy G spolu se sčítáním a skládáním endomorfismů je okruh s jednotkovým prvkem.*

Důkaz. Již jsme si uvědomili, že skládání endomorfismů grupy G je asociativní binární operace na množině $\text{End } G$, která má jednotkový prvek 1_G . Dále jsme ukázali, že sčítání endomorfismů je binární operace na množině $\text{End } G$. Z platnosti asociativního a komutativního zákona pro operaci " + " v grupě G vyplývá platnost asociativního a komutativního zákona pro sčítání endomorfismů. Nulový endomorfismus grupy G je nulovým prvkem vzhledem ke sčítání endomorfismů. Jestliže f je endomorfismus grupy G , potom zobrazení přiřazující každému prvku $a \in G$ opačný prvek k prvku $f(a)$ (tj. prvek $-f(a) \in G$) je zřejmě endomorfismus grupy G , který je opačným prvkem k endomorfismu f při sčítání endomorfismů. Pro každé tři endomorfismy f, g, h grupy G platí rovnosti

$$f(g+h) = fg + fh, \quad (f+g)h = fh + gh.$$

Pro každé $a \in G$ je totiž

$$\begin{aligned} (f(g+h))(a) &= f((g+h)(a)) = f(g(a) + h(a)) = f(g(a)) + f(h(a)) = \\ &= (fg)(a) + (fh)(a) = (fg + fh)(a); \end{aligned}$$

stejně se dokáže druhá rovnost. Množina $\text{End } G$ je tedy okruh s jednotkovým prvkem. \square

Na jednoduchých příkladech je možno ukázat, že součet dvou automorfismů komutativní grupy G nemusí být automorfismem grupy G . Sčítání automorfismů tedy není binární operací na množině $\text{Aut } G$.

5.9. Příklady.

(i) Zobrazení, které každému číslu $a \in \mathbb{Z}$ přiřazuje číslo $-a \in \mathbb{Z}$, je automorfismem grupy \mathbb{Z} . Tento automorfismus je opačným prvkem k identickému automorfismu $1_{\mathbb{Z}}$ grupy \mathbb{Z} . Součet těchto dvou automorfismů je nulovým endomorfismem grupy \mathbb{Z} . Grupa $\text{Aut } \mathbb{Z}$ je dvouprvková, $\text{Aut } \mathbb{Z} = \{1_{\mathbb{Z}}, -1_{\mathbb{Z}}\}$.

Zobrazení φ_n , které každému číslu $a \in \mathbb{Z}$ přiřazuje číslo $na \in \mathbb{Z}$, kde $n \in \mathbb{Z}$ je pevně zvolené číslo, je endomorfismem grupy \mathbb{Z} . Není obtížné ukázat, že jiné endomorfismy grupy \mathbb{Z} neexistují, tj. $\text{End } \mathbb{Z} = \{\varphi_n; n \in \mathbb{Z}\}$.

Pro každé $n, m \in \mathbb{Z}$ je

$$\varphi_n + \varphi_m = \varphi_{n+m}, \quad \varphi_n \varphi_m = \varphi_{nm},$$

dále je

$$\varphi_1 = 1_{\mathbb{Z}}, \quad \varphi_{-1} = -1_{\mathbb{Z}}, \quad \varphi_0 = 0.$$

(ii) Zobrazení, které každé matici $A \in R^{n \times n}$ přiřazuje její stopu $\text{tr } A$, je epimorfismem aditivní grupy $R^{n \times n}$ na aditivní grupu R (viz 4.26(i)).

(iii) Zobrazení, které každé matici $A \in R^{m \times n}$ přiřazuje matici A^T , je izomorfismus aditivní grupy $R^{m \times n}$ na aditivní grupu $R^{n \times m}$ (viz 4.20(i)).

(iv) Zobrazení, které každému polynomu $f \in \mathbb{R}[x]$ přiřazuje jeho derivaci f' , je endomorfismus aditivní grupy $\mathbb{R}[x]$; tento endomorfismus je epimorfismem, ale není monomorfismem.

(v) Zobrazení, které každému Gaussovu celému číslu $a + bi \in \mathbb{Z}[i]$ přiřazuje číslo a (resp. b , resp. $a + b$), je epimorfismem aditivní grupy $\mathbb{Z}[i]$ na aditivní grupu \mathbb{Z} .

(vi) Zobrazení, které každé čtvercové matici $A \in R^{n \times n}$ přiřazuje symetrickou matici $\frac{1}{2}(A + A^T)$, je endomorfismem aditivní grupy $R^{n \times n}$.

(vii) *Logaritmus* (při libovolném základu z) je izomorfismem multiplikatívni grupy kladných reálných čísel na aditivní grupu všech reálných čísel; pro každá dvě čísla $a, b \in (0, \infty)$ je totiž

$$\log_z ab = \log_z a + \log_z b .$$

(viii) Zobrazení, které přiřazuje každému komplexnímu číslu jeho druhou (resp. n -tou) mocninu, je endomorfismem multiplikatívni grupy všech komplexních čísel. Zúžení tohoto zobrazení je endomorfismus multiplikatívni grupy komplexních čísel jednotkové absolutní hodnoty.

5.10. Definice. Nechť G je multiplikatívni grupa. Podmnožina G' grupy G se nazývá *podgrupa* grupy G , má-li tyto vlastnosti:

- (i) $1 \in G'$,
- (ii) jestliže $a, b \in G'$, potom $ab \in G'$ a $a^{-1} \in G'$.

Přeformulujme ještě definici podgrupy do aditivní řeči.

Nechť G je aditivní grupa. Podmnožina G' grupy G se nazývá *podgrupa* grupy G , má-li tyto vlastnosti:

- (i) $0 \in G'$,
- (ii) jestliže $a, b \in G'$, potom $a + b \in G'$ a $-a \in G'$.

Rozvážíme-li příklady, které již byly v předchozím textu uvedeny (2.3 a 2.9, 2.5 a 2.8, 3.4 a 3.6, 4.11, 5.3, 5.4), snadno získáme řadu příkladů podgrup.

6. PERMUTACE

6.1. Definice. Necht M je konečná množina. *Permutací* množiny M nazveme každé vzájemně jednoznačné zobrazení (bijekci) množiny M na množinu M .

Při vyšetřování permutací je zřejmě lhostejné, jak označíme prvky množiny M . V celém dalším výkladu budeme proto bez újmy na obecnosti předpokládat, že je $M = \{1, 2, \dots, n\}$, kde n je nějaké přirozené číslo.

Permutaci P množiny M zapisujeme obvykle schématem

$$P = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix},$$

kde pro každé $i = 1, 2, \dots, n$ je $P(i) = a_i$, tj. obrazy a_1, a_2, \dots, a_n čísel $1, 2, \dots, n$ jsou zapsány pod těmito čísly. Přitom je

$$\{a_1, a_2, \dots, a_n\} = \{1, 2, \dots, n\},$$

tj. a_1, a_2, \dots, a_n je jen jiné *pořadí* čísel $1, 2, \dots, n$. V některých případech nepožadujeme, aby byla čísla v horním řádku uspořádána podle velikosti. Je tedy např.

$$\begin{pmatrix} 5 & 1 & 3 & 4 & 2 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}.$$

Permutace množiny M skládáme jako zobrazení; *složením permutací* P a Q (v tomto pořadí) rozumíme složené zobrazení QP , které každému číslu $i \in M$ přiřadí číslo $Q(P(i))$. Složení dvou permutací množiny M je opět nějaká permutace množiny M , neboť složení dvou bijekcí je opět bijekce. Jsou-li např.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \quad \text{a} \quad Q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$$

permutace množiny $M = \{1, 2, 3, 4, 5\}$, je

$$QP = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix} \quad \text{a} \quad PQ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}.$$

Skládání permutací tedy není komutativní. Přesto se může stát, že pro nějaké permutace P, Q množiny M platí rovnost $PQ = QP$; v tomto případě říkáme, že permutace P, Q jsou *záměnné*, resp. *komutující*.

6.2. Věta. *Množina všech permutací n -prvkové množiny M spolu s operací skládání tvoří grupu. Tato grupa má $n!$ prvků.*

Důkaz. Skládání permutací je podle předešlého binární operací na množině všech permutací množiny M . Tato operace je asociativní, neboť již skládání zobrazení je asociativní. Identické zobrazení 1_M množiny M na množinu M je tzv. *identická permutace*, která je jednotkovým prvkem při skládání permutací množiny M . Ke každé permutaci

$$P = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

množiny M existuje permutace P^{-1} taková, že $P \cdot P^{-1} = P^{-1} \cdot P = 1_M$. Permutace P^{-1} se nazývá *inverzní permutace* k permutaci P ; zřejmě je

$$P^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Množina všech permutací množiny M spolu s operací skládání permutací je tedy grupa. Indukcí snadno dokážeme, že n -prvková množina má právě $n!$ různých permutací. \square

6.3. Definice. Grupa všech permutací n -prvkové množiny se nazývá *symetrická grupa stupně n* . Značí se obvykle \mathbb{S}_n .

6.4. Definice. Nechť P je permutace množiny M . *Inverzí* permutace P budeme rozumět každou dvouprvkovou podmnožinu $\{i, j\}$ množiny M , kde

$$i < j \quad \text{a} \quad P(i) > P(j).$$

*Znaménko*⁸ $\text{sgn } P$ permutace P definujeme rovností

$$\text{sgn } P = (-1)^{\text{in } P},$$

kde $\text{in } P$ je počet všech inverzí permutace P . Permutace P se nazývá *sudá*, resp. *lichá*, jestliže je $\text{sgn } P = 1$, resp. $\text{sgn } P = -1$.

Permutace je tedy sudá, resp. lichá, má-li sudý, resp. lichý počet inverzí. Identická permutace 1_M nemá žádnou inverzi a je proto sudá.

6.5. Příklady.

(i) Symetrická grupa stupně 1 je jednoprvková, symetrická grupa stupně 2 je dvouprvková:

$$\mathbb{S}_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}, \quad \mathbb{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

⁸ Těž *signum*.

Symetrická grupa stupně 3 má šest prvků:

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Skládání těchto permutací je zachyceno v *multiplikační tabulce* grupy \mathbb{S}_3 (např. v průsečíku řádku začínajícího P_3 a sloupce začínajícího P_5 stojí $P_3 \cdot P_5 = P_6$):

.	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_3	P_1	P_6	P_4	P_5
P_3	P_3	P_1	P_2	P_5	P_6	P_4
P_4	P_4	P_5	P_6	P_1	P_2	P_3
P_5	P_5	P_6	P_4	P_3	P_1	P_2
P_6	P_6	P_4	P_5	P_2	P_3	P_1

Permutace P_1 je identická, nemá žádnou inverzi. Permutace P_2 má inverze $\{1, 3\}$, $\{2, 3\}$, permutace P_3 inverze $\{1, 2\}$, $\{1, 3\}$, permutace P_4 inverzi $\{2, 3\}$, permutace P_5 inverze $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, permutace P_6 inverzi $\{1, 2\}$. Permutace P_1, P_2, P_3 jsou sudé, permutace P_4, P_5, P_6 jsou liché.

Symetrická grupa \mathbb{S}_4 má 24 prvků, symetrická grupa \mathbb{S}_5 má 120 prvků.

(ii) Permutace

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$$

má inverze $\{1, 2\}$, $\{1, 5\}$, $\{3, 5\}$, $\{4, 5\}$ a je tedy sudá.

$$P^{-1} = \begin{pmatrix} 3 & 1 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}.$$

Permutace P^{-1} má inverze $\{1, 3\}$, $\{2, 3\}$, $\{2, 4\}$, $\{2, 5\}$ a je tedy rovněž sudá.

6.6. Věta. Jsou-li P, Q permutace množiny M , potom je

$$\operatorname{sgn} PQ = \operatorname{sgn} P \cdot \operatorname{sgn} Q.$$

Důkaz. Množinu K všech dvouprvkových podmnožin množiny M vyjádříme jako disjunkttní sjednocení čtyř množin,

$$K = K_1 \cup K_2 \cup K_3 \cup K_4,$$

kde

$$\begin{aligned} K_1 &= \{ \{i, j\}; i < j, Q(i) < Q(j), PQ(i) < PQ(j) \}, \\ K_2 &= \{ \{i, j\}; i < j, Q(i) < Q(j), PQ(i) > PQ(j) \}, \\ K_3 &= \{ \{i, j\}; i < j, Q(i) > Q(j), PQ(i) < PQ(j) \}, \\ K_4 &= \{ \{i, j\}; i < j, Q(i) > Q(j), PQ(i) > PQ(j) \}. \end{aligned}$$

Je tedy $K_3 \cup K_4$ množinou všech inverzí permutace Q a množina $K_2 \cup K_4$ množinou všech inverzí permutace PQ . Vzhledem k tomu, že permutace Q zobrazuje vzájemně jednoznačně množinu K na množinu K , je počet inverzí permutace P roven počtu prvků množiny $K_2 \cup K_3$. Je tedy

$$\text{in } PQ = |K_2| + |K_4| = |K_2| + |K_3| + |K_3| + |K_4| - 2|K_3| = \text{in } P + \text{in } Q - 2|K_3|$$

a tedy

$$\text{sgn } PQ = (-1)^{\text{in } P + \text{in } Q - 2|K_3|} = (-1)^{\text{in } P} \cdot (-1)^{\text{in } Q} = \text{sgn } P \cdot \text{sgn } Q. \quad \square$$

Poznamenejme, že jsme v předchozí větě dokázali, že zobrazení sgn , které každé permutaci P grupy \mathbb{S}_n přiřazuje její znaménko $\text{sgn } P$, je homomorfismus grupy \mathbb{S}_n do multiplikativní grupy $\{1, -1\}$. Pro $n > 1$ jde zřejmě o homomorfismus na grupu $\{1, -1\}$, neboli epimorfismus.

6.7. Důsledek. *Pro permutace množiny M platí:*

- (i) *Složení dvou sudých permutací je sudá permutace.*
- (ii) *Složení dvou lichých permutací je sudá permutace.*
- (iii) *Složení sudé a liché permutace je lichá permutace.*
- (iv) *Pro každou permutaci P je $\text{sgn } P^{-1} = \text{sgn } P$.*

Důkaz. Všechna tvrzení vyplývají z předchozí věty; při důkazu čtvrtého se využije rovnost $P \cdot P^{-1} = 1_M$. \square

6.8. Důsledek. *Nechť $P \in \mathbb{S}_n$ je pevně zvolená permutace. Zobrazení, které každé permutaci $Q \in \mathbb{S}_n$ přiřazuje permutaci $PQ \in \mathbb{S}_n$ (resp. $QP \in \mathbb{S}_n$), je bijekce množiny \mathbb{S}_n na množinu \mathbb{S}_n . Jestliže je permutace P sudá, pak při této bijekci přechází sudá permutace v sudou a lichá v lichou. Jestliže je permutace P lichá, pak při této bijekci přechází sudá permutace v lichou a lichá v sudou.*

Důkaz. Z rovnosti $PQ_1 = PQ_2$ dostáváme rovnost $P^{-1}PQ_1 = P^{-1}PQ_2$ a tedy i rovnost $Q_1 = Q_2$; uvažované zobrazení je tedy injektivní.

Z rovnosti $P(P^{-1}Q) = Q$ vyplývá, že jde též o surjekci, neboť na permutaci Q se zobrazí permutace $P^{-1}Q$.

Zbytek tvrzení vyplývá z věty 6.6, resp. důsledku 6.7. \square

Poznamenejme, že zobrazení z důsledku 6.8 je tzv. *levá* (resp. *pravá*) *translace* grupy \mathbb{S}_n určená prvkem P .

6.9. Věta. Množina všech sudých permutací n -prvkové množiny je podgrupou symetrické grupy \mathbb{S}_n . Pro $n > 1$ má tato podgrupa $\frac{n!}{2}$ prvků.

Důkaz. Podle předchozího (viz 6.7) je skládání permutací binární operací na množině všech sudých permutací množiny M . Identická permutace je sudá a inverzní permutace k sudé permutaci je také sudá. Podle 6.8 je pro $n > 1$ sudých permutací stejný počet jako lichých, tj. $\frac{n!}{2}$. \square

Poznamenejme pro úplnost, že podgrupa všech sudých permutací n -prvkové množiny je jádrem homomorfismu sgn a je to tedy dokonce *normální podgrupa* grupy \mathbb{S}_n . Tento fakt vyplývá též ze skutečnosti, že jde o podgrupu *indexu 2*.

6.10. Definice. Grupa všech sudých permutací n -prvkové množiny se nazývá *alternující grupa stupně n* . Obvykle se značí \mathbb{A}_n .

6.11. Příklad. Permutace P_1, P_2, P_3 z příkladu 6.5(i) tvoří alternující grupu stupně 3. Její multiplikativní tabulka se snadno získá z multiplikativní tabulky grupy \mathbb{S}_3 .

.	P_1	P_2	P_3
P_1	P_1	P_2	P_3
P_2	P_2	P_3	P_1
P_3	P_3	P_1	P_2

6.12. Definice. Permutace Q množiny M se nazývá *cyklus*, jestliže existuje přirozené číslo $m \geq 1$ a prvky $x_1, \dots, x_m \in M$ takové, že

$$\begin{aligned} Q(x_i) &= x_{i+1} \quad \text{pro každé } i = 1, \dots, m-1, \\ Q(x_m) &= x_1, \\ Q(x) &= x \quad \text{pro každé } x \in M \setminus \{x_1, \dots, x_m\}. \end{aligned}$$

Píšeme $Q = (x_1, x_2, \dots, x_m)$, číslo m se nazývá *délka cyklu*. Cyklus délky 2 se nazývá *transpozice*, cyklus délky 3 *trojcyklus*. Cykly (x_1, \dots, x_m) a (y_1, \dots, y_k) se nazývají *nezávislé* (někdy též *disjunktní*), jestliže $\{x_1, \dots, x_m\} \cap \{y_1, \dots, y_k\} = \emptyset$.

Identická permutace množiny M je podle předchozí definice cyklus; klademe totiž $m = 1$ a za x_1 vezmeme libovolný prvek množiny M . Délka tohoto cyklu je 1. Tento pohled na identickou permutaci se nám později bude hodit.

6.13. Věta. Každé dva nezávislé cykly jsou záměnné.

Důkaz. Nechť $P = (x_1, \dots, x_m)$ a $Q = (y_1, \dots, y_k)$ jsou nezávislé cykly, které jsou prvky grupy \mathbb{S}_n . Vzhledem k tomu, že P zobrazuje identicky všechny prvky různé od prvků x_1, \dots, x_m a Q zobrazuje identicky všechny prvky různé od prvků y_1, \dots, y_k , je $PQ(z) = QP(z)$ pro každé $z \in M$, tj. permutace P a Q jsou záměnné. \square

6.14. Příklad. Permutace

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 4 & 3 & 6 & 2 & 8 & 9 \end{pmatrix} \quad \text{a} \quad Q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 3 & 9 & 5 & 1 & 7 & 8 & 6 \end{pmatrix}$$

jsou cykly. Zapisují se též v tvaru

$$P = (2, 5, 3, 7), \quad Q = (1, 4, 9, 6).$$

Jsou to cykly délky 4 a jsou nezávislé; je

$$PQ = QP = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 7 & 9 & 3 & 1 & 2 & 8 & 6 \end{pmatrix}.$$

Poznamenejme, že každý cyklus délky m můžeme zapsat m způsoby (tzv. *cyklickou záměnou*); např.

$$P = (2, 5, 3, 7) = (5, 3, 7, 2) = (3, 7, 2, 5) = (7, 2, 5, 3).$$

Je-li cyklus takto zapsán, musí být jasné (např. z kontextu), jakou množinu permutuje. V našem případě je $P, Q \in S_9$. Ověřte, že permutace P, Q jsou liché.

Nechť P je permutace množiny M . Mocniny permutace P definujeme přirozeným způsobem:

$$P^1 = P, \quad P^2 = P \cdot P, \quad P^3 = P \cdot P^2, \quad \dots, \quad P^{n+1} = P \cdot P^n, \quad \dots;$$

dále klademe $P^{-n} = (P^{-1})^n$ a $P^0 = 1_M$.

Nechť P je permutace množiny M a nechť a je libovolný prvek množiny M . Posloupnost $a, P(a), P^2(a), \dots$ je utvořena z prvků konečné množiny M a proto se v ní musí prvky opakovat. Nechť j je takové přirozené číslo, že prvky

$$a, P(a), \dots, P^{j-1}(a)$$

jsou navzájem různé a prvek $P^j(a)$ se už v uvažované posloupnosti vyskytuje. Je tedy $P^j(a) = P^k(a)$, kde $0 \leq k \leq j-1$. Jestliže je $k \neq 0$, potom z injektivit permutace P vyplývá rovnost $P^{j-1}(a) = P^{k-1}(a)$ a to je spor s volbou čísla j . Proto je $k = 0$, tj. $P^j(a) = a$, $P^{j+1}(a) = P(a)$ atd. Uvažovaná posloupnost $a, P(a), P^2(a), \dots$ je tedy utvořena opakováním konečné posloupnosti $a, P(a), \dots, P^{j-1}(a)$.

Na množině M definujeme relaci ρ : pro prvky $a, b \in M$ nechť je $a\rho b$ právě tehdy, když existuje přirozené číslo m takové, že $P^m(a) = b$ (tj. b leží v posloupnosti $a, P(a), P^2(a), \dots$). Z předchozího odstavce vyplývá, že relace ρ je reflexivní, symetrická a tranzitivní, tj. ρ je ekvivalence na množině M . Ekvivalenci ρ odpovídá

disjunktní rozklad množiny M na třídy ekvivalence. Ekvivalenční třída obsahující prvek a je tvořena právě všemi prvky $a, P(a), \dots, P^{j-1}(a)$, kde j je nejmenší přirozené číslo s vlastností $P^j(a) = a$.

Necheť M_1, \dots, M_k jsou právě všechny třídy ekvivalence ρ . Definujme nyní zobrazení $P_i, i = 1, \dots, k$, množiny M do množiny M takto:

$$\begin{aligned} P_i(x) &= P(x) & \text{pro } x \in M_i, \\ P_i(x) &= x & \text{pro } x \in M \setminus M_i. \end{aligned}$$

Zobrazení P_1, \dots, P_k jsou zřejmě navzájem nezávislé cykly. Nazývají se *cykly permutace* P . Snadno se nyní uváží, že permutace P je složením všech svých cyklů P_1, \dots, P_k (v libovolném pořadí). Dokázali jsme tedy důležité tvrzení, které je vyjádřeno v následující větě.

6.15. Věta. *Každá permutace je složením všech svých cyklů, a to v libovolném pořadí.* \square

Poznamenejme, že permutace P může být složena i z jiných cyklů než z cyklů permutace P . V tom případě však tyto cykly nejsou nezávislé.

6.16. Příklad. Mějme permutaci

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 2 & 1 & 9 & 3 & 10 & 8 & 6 & 4 & 7 \end{pmatrix}.$$

Tato permutace má čtyři cykly:

$$P_1 = (1, 5, 3), \quad P_2 = (2), \quad P_3 = (4, 9), \quad P_4 = (6, 10, 7, 8).$$

Je tedy

$$P = P_1 P_2 P_3 P_4 = P_3 P_1 P_4 P_2 = P_4 P_3 P_1 P_2 = \dots;$$

přitom je P_1 trojcyklus, P_2 identická permutace a P_3 transpozice. Permutace P může být složena i z jiných cyklů, které však již nebudou záměnné (nejsou to cykly permutace P); např.

$$P = (3, 5, 4, 9, 2, 1) \cdot (7, 8, 6, 10) \cdot (1, 3, 2, 9, 5).$$

Pomocí rozkladu permutace na nezávislé cykly je možno snadno vypočítat její libovolně velké mocniny. Permutace P má cykly délky 3, 1, 2, 4, nejmenší společný násobek těchto čísel je 12. Mocníme-li tedy postupně permutaci P , dostaneme identitu až při dvanácté mocnině. Odtud je např.

$$P^{1000} = P^{12 \cdot 83 + 4} = (P^{12})^{83} \cdot P^4 = P^4.$$

Ověřte, že permutace P je sudá.

Každá permutace n -prvkové množiny má alespoň jeden cyklus a nejvýše n cyklů, přičemž součet délek všech jejích cyklů je roven n . Identická permutace má právě n cyklů délky 1 (všechny jsou rovny identické permutaci), neidentické permutace mají cyklů méně. Permutace, které mají právě jediný cyklus, se nazývají *cyklické* (jejich cyklus má délku n).

Transpozice je tedy permutace, která má jeden cyklus délky 2 a ostatní cykly délky 1 (je jich $n - 2$ a jsou rovny identické permutaci). Trojcyklus je permutace, která má jeden cyklus délky 3 a ostatní cykly délky 1 (je jich $n - 3$ a jsou rovny identické permutaci).

6.17. Lemma. *Každá transpozice je lichá.*

Důkaz. Transpozice

$$(i, j) = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

má tyto inverze:

$$\{i, i + 1\}, \{i, i + 2\}, \dots, \{i, j - 1\}, \{i, j\}, \\ \{i + 1, j\}, \{i + 2, j\}, \dots, \{j - 1, j\}.$$

Těchto inverzí je $2(j - i) - 1$, takže transpozice (i, j) je lichá. \square

6.18. Věta. *Každou permutaci je možno složit z transpozic.*

Důkaz. Podle věty 6.15 je každá permutace složením všech svých cyklů. K provedení důkazu tedy stačí rozložit cykly (délky alespoň 3) na transpozice. Jestliže je $P = (a_1, a_2, \dots, a_r)$ nějaký cyklus ($r \geq 3$), potom je

$$P = (a_1, a_r) \cdot (a_1, a_{r-1}) \cdot \dots \cdot (a_1, a_2).$$

Identickou permutaci chápeme jako složení prázdné množiny transpozic (je-li množina M alespoň dvouprvková, je též $1_M = (i, j) \cdot (i, j)$ pro libovolná $i, j \in M$). \square

Jestliže je permutace P složením m transpozic, potom je podle věty 6.6 a lematu 6.17 $\text{sgn } P = (-1)^m$. Znaménko permutace P můžeme tedy také určovat pomocí rozkladu na transpozice. Přitom je třeba si uvědomit, že danou permutaci můžeme z transpozic složit různými způsoby a že ani počet užitých transpozic nezůstává stejný. Zachovává se však *parita* počtu užitých transpozic, tj. sudá permutace je vždy vyjádřena jako složení sudého počtu transpozic a lichá permutace jako složení lichého počtu transpozic.

6.19. Věta. *Jestliže má permutace $P \in \mathbb{S}_n$ právě k cyklů, je $\text{sgn } P = (-1)^{n-k}$.*

Důkaz. Předpokládejme, že r_1, r_2, \dots, r_k jsou délky cyklů permutace P . Víme, že je $r_1 + r_2 + \dots + r_k = n$. Provedme rozklad permutace P na transpozice stejným způsobem jako v důkazu věty 6.18. Počet transpozic tohoto rozkladu je zřejmě

$$(r_1 - 1) + (r_2 - 1) + \dots + (r_k - 1) = n - k;$$

podle předešlého je tedy $\text{sgn } P = (-1)^{n-k}$. \square

Uvědomme si, že při zjišťování znaménka permutace podle předchozí věty je třeba počítat i cykly délky 1.

6.20. Příklady.

(i) Permutace

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 1 & 7 & 9 & 8 & 2 & 6 & 3 \end{pmatrix}$$

se snadno rozloží na cykly,

$$P = (1, 5, 9, 3) \cdot (2, 4, 7) \cdot (6, 8) .$$

Odtud dostáváme rozklad permutace P na transpozice,

$$P = (1, 3) \cdot (1, 9) \cdot (1, 5) \cdot (2, 7) \cdot (2, 4) \cdot (6, 8) .$$

Užitím cyklické záměny („posunutí cyklů“) dostaneme jiný rozklad na transpozice,

$$P = (5, 9, 3, 1) \cdot (7, 2, 4) \cdot (6, 8) ,$$

$$P = (5, 1) \cdot (5, 3) \cdot (5, 9) \cdot (7, 4) \cdot (7, 2) \cdot (6, 8) .$$

Můžeme též psát

$$P = (5, 1) \cdot (5, 3) \cdot (5, 9) \cdot (7, 4) \cdot (7, 2) \cdot (3, 5) \cdot (6, 8) \cdot (5, 3)$$

apod. Permutace P je sudá, neboť má tři cykly ($\text{sgn } P = (-1)^{9-3}$). Znaménko můžeme určit i rozkladem na transpozice ($\text{sgn } P = (-1)^6$).

Dále je

$$P^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 9 & 2 & 1 & 8 & 4 & 6 & 5 \end{pmatrix} ,$$

$$P^{-1} = (1, 3, 9, 5) \cdot (2, 7, 4) \cdot (6, 8) ,$$

$$P^{-1} = (1, 5) \cdot (1, 9) \cdot (1, 3) \cdot (2, 4) \cdot (2, 7) \cdot (6, 8) .$$

(ii) Permutace

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 2 & 6 & 3 & 5 \end{pmatrix}$$

je cyklická,

$$P = (1, 4, 2, 7, 5, 6, 3) ,$$

$$P = (1, 3) \cdot (1, 6) \cdot (1, 5) \cdot (1, 7) \cdot (1, 2) \cdot (1, 4) .$$

Permutace

$$P^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 6 & 1 & 7 & 5 & 2 \end{pmatrix}$$

je také cyklická,

$$P^{-1} = (3, 6, 5, 7, 2, 4, 1) = (1, 3, 6, 5, 7, 2, 4) ,$$

$$P^{-1} = (3, 1) \cdot (3, 4) \cdot (3, 2) \cdot (3, 7) \cdot (3, 5) \cdot (3, 6) = (1, 4) \cdot (1, 2) \cdot (1, 7) \cdot (1, 5) \cdot (1, 6) \cdot (1, 3) .$$

Obě permutace jsou sudé.

(iii) Permutace

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 3 & 2 & 4 & 1 & 9 & 6 & 8 \end{pmatrix}$$

má dva cykly,

$$P = (1, 5, 4, 2, 7, 9, 8, 6) \cdot (3) ,$$

jeden z možných rozkladů na transpozice je

$$P = (1, 6) \cdot (1, 8) \cdot (1, 9) \cdot (1, 7) \cdot (1, 2) \cdot (1, 4) \cdot (1, 5) .$$

Permutace P je lichá ($\text{sgn } P = (-1)^{9-2}$; uvědomme si, že je třeba počítat i cyklus délky 1).

Na závěr uvedeme větu, kterou někdy v obecné algebře využíváme. Při důkazu procvičíme skládání permutací.

6.21. Věta. *Pro $n \geq 3$ je alternující grupa \mathbb{A}_n rovna množině všech permutací, které jsou složením trojcyklů.*

Důkaz. Každý trojcyklus je sudou permutací, neboť jde vyjádřit jako složení dvou transpozic (viz důkaz věty 6.18). Skládáním trojcyklů tedy dostáváme výhradně sudé permutace.

Nyní ukážeme, že každá sudá permutace je složením trojcyklů. Protože je

$$(i, r) \cdot (i, j) = (i, j, r) , \quad (r, s) \cdot (i, j) = (i, r, s) \cdot (s, i, j) ,$$

je každá sudá permutace (jako složení sudého počtu transpozic) složením trojcyklů. \square

II. VEKTOROVÉ PROSTORY

7. PROSTORY A PODPROSTORY

7.1. Úmluva. V dalším textu budeme slovem *těleso* rozumět vždy *komutativní těleso* (tj. *pole*). Nulový a jednotkový prvek tělesa budeme pro jednoduchost nazývat *nula* a *jednička* a opačný prvek k jednotkovému prvku *minus jednička*. Tyto prvky budeme značit symboly $0, 1, -1$.

7.2. Definice. Nechť T je těleso a V množina s binární operací sčítání, kterou budeme značit symbolem $+$. Nechť je dáno zobrazení kartézského součinu $T \times V$ do množiny V ; dvojici prvků $a \in T$ a $v \in V$ toto zobrazení přiřazuje prvek, který značíme $a \cdot v$ nebo jednodušeji av ; hovoříme o *násobení* prvků množiny V prvky tělesa T , které značíme symbolem \cdot . Nechť dále platí:

- (i) $\forall u, v, w \in V \quad (u + v) + w = u + (v + w)$,
- (ii) $\forall u, v \in V \quad u + v = v + u$,
- (iii) $\exists o \in V \quad \forall u \in V \quad u + o = u$,
- (iv) $\forall u \in V \quad \exists -u \in V \quad u + (-u) = o$,
- (v) $\forall u, v \in V \quad \forall a \in T \quad a \cdot (u + v) = a \cdot u + a \cdot v$,
- (vi) $\forall u \in V \quad \forall a, b \in T \quad (a + b) \cdot u = a \cdot u + b \cdot u$,
- (vii) $\forall u \in V \quad \forall a, b \in T \quad (a \cdot b) \cdot u = a \cdot (b \cdot u)$,
- (viii) $\forall u \in V \quad 1 \cdot u = u$.

Potom budeme říkat, že V je *vektorový prostor* (nebo *lineární prostor*) nad tělesem T . Prvkům množiny V budeme říkat *vektory*, prvkům tělesa T *skaláry*. Vektor označený symbolem o a popsáný axiómem (iii) se nazývá *nulový vektor* prostoru V , vektor označený symbolem $-u$ a popsáný axiómem (iv) se nazývá *opačný vektor* k vektoru u .

Jestliže je T těleso reálných, resp. komplexních čísel, pak hovoříme o *reálném*, resp. *komplexním* vektorovém prostoru.

Vektory značíme většinou písmeny z konce abecedy a skaláry písmeny ze začátku abecedy. Násobení vektorů skaláry zapisujeme vždy tak, že skaláry píšeme vlevo a vektory vpravo.

Povšimněme si, že ve výše uvedených osmi axiómech je stejným symbolem $+$ značena operace sčítání skalárů i operace sčítání vektorů. Rovněž tak symbol \cdot (který často vynecháváme) užíváme jak pro označení násobení skalárů (binární operace v tělese T), tak pro označení násobení vektorů skaláry (zde se „násobí“ prvky dvou různých množin).

Axiómy (i) a (ii) jsou asociativní a komutativní zákon pro sčítání vektorů. Axióm (iii) postuluje existenci nulového vektoru; z tohoto axiómu plyne, že každý vektorový prostor je neprázdný. Axióm (iv) je axióm existence opačných prvků. Axiómům (v) a (vi) se často říká distributivní zákony, i když ve skutečnosti nejde

o distributivitu (distributivita je vazbou dvou binárních operací na téže množině); axióm (v) svazuje sčítání vektorů a násobení vektorů skaláry, axióm (vi) svazuje sčítání skalárů a násobení vektorů skaláry. Axióm (vii) se často nazývá asociativní zákon, i když opět nejde o skutečnou asociativitu (vlastnost jedné binární operace na množině); tento axióm svazuje násobení skalárů a násobení vektorů skaláry.

Místo vektorový prostor V nad tělesem T budeme často říkat pouze vektorový prostor V nebo pouze prostor V . Jsou-li u, v vektory prostoru V , pak místo $u + (-v)$ budeme psát $u - v$. V následujícím odstavci shrneme některá jednoduchá početní pravidla, která vyplývají z definice 7.2 a z uvedených úmluv.

7.3. Věta. *Nechť V je vektorový prostor nad tělesem T . Potom platí:*

- (i) $\forall u \in V \quad 0 \cdot u = o$,
- (ii) $\forall u \in V \quad (-1) \cdot u = -u$,
- (iii) $\forall u \in V \quad \forall a \in T \quad (-a) \cdot u = -(a \cdot u)$,
- (iv) $\forall u \in V \quad -(-u) = u$,
- (v) $\forall u, v \in V \quad \forall a \in T \quad a \cdot (u - v) = a \cdot u - a \cdot v$,
- (vi) $\forall u \in V \quad \forall a, b \in T \quad (a - b) \cdot u = a \cdot u - b \cdot u$,
- (vii) $\forall a \in T \quad a \cdot o = o$.

Důkaz. V důkazu již nebudeme psát tečky představující násobení vektorů skaláry, které jsme zatím důsledně psali (např. ve tvrzeních (i)–(vii)).

Pro každý vektor $u \in V$ platí rovnost $(1 + 0)u = 1u$. Užitím axiómů (vi) a (viii) z ní dostaneme rovnost $u + 0u = u$. K oběma stranám přičteme vektor $-u$ (užijeme tedy axióm (iv)) a pomocí axiómů (i), (iv), (iii), (ii) dojdeme k rovnosti $0u = o$.

Pro každý vektor $u \in V$ platí podle tvrzení (i) rovnost $(1 + (-1))u = o$. Užijeme-li axiomy (vi) a (viii) dostaneme z ní rovnost $u + (-1)u = o$. Přičteme-li k oběma stranám vektor $-u$ (axióm (iv)), dostaneme užitím axiómů (i), (iv), (iii), (ii) rovnost $(-1)u = -u$.

Dále je $(-a)u = ((-1)a)u = (-1)(au) = -(au)$ a tedy $-(-u) = u$ atd. \square

Podobných početních pravidel bychom mohli zformulovat a dokázat celou řadu. Při jejich dokazování podstatně využíváme i početní pravidla platná v tělese T . Poznamenejme ještě, že pomocí matematické indukce snadno dokážeme následující tvrzení.

7.4. Věta. *Nechť V je vektorový prostor nad tělesem T . Jestliže $u_1, \dots, u_k \in V$ a $a_1, \dots, a_m \in T$, potom*

$$\sum_{i=1}^m a_i \cdot \sum_{j=1}^k u_j = \sum_{i=1}^m \sum_{j=1}^k a_i u_j . \quad \square$$

7.5. Poznámka. Definice vektorového prostoru se často formuluje stručněji s využitím pojmů komutativní grupa a akce monoidu na množině. První pojem známe z předchozího textu; již v definici 7.2 jsme si mohli všimnout, že vektorový prostor V je vzhledem ke sčítání vektorů komutativní grupou.

Nechť G je tzv. *monoid*, tj. množina s asociativní binární operací, která má jednotkový prvek 1 , a necht' X je množina. *Akcí monoidu G na množině X* rozumíme zobrazení kartézského součinu $G \times X$ do množiny X (obraz dvojice $(g, x) \in G \times X$ se značí gx , hovoří se o násobení prvků množiny X prvky monoidu G), které má následující vlastnosti:

- (i) $\forall x \in X \quad 1x = x$,
- (ii) $\forall x \in X \quad \forall a, b \in G \quad (ab)x = a(bx)$.

Definici vektorového prostoru nad tělesem T lze potom stručně podat takto.

Nechť T je těleso. Vektorovým prostorem nad tělesem T budeme rozumět každou aditivně psanou komutativní grupu V spolu s akcí tělesa T na množině V splňující následující dva axiomy:

- (i) $\forall u \in V \quad \forall a, b \in T \quad (a + b)u = au + bu$,
- (ii) $\forall u, v \in V \quad \forall a \in T \quad a(u + v) = au + av$.

7.6. Definice. Necht' V je vektorový prostor nad tělesem T . Jestliže je podmnožina W prostoru V vektorovým prostorem nad tělesem T vzhledem k těmúž sčítání vektorů a těmúž násobení vektorů skaláry (operace "+" a "." zúžíme na podmnožinu W), potom říkáme, že množina W je *podprostorem* prostoru V .

7.7. Věta. *Necht' V je vektorový prostor nad tělesem T . Podmnožina W prostoru V je podprostorem prostoru V právě tehdy, když platí:*

- (i) $W \neq \emptyset$,
- (ii) $\forall u, v \in W \quad u + v \in W$,
- (iii) $\forall u \in W \quad \forall a \in T \quad au \in W$.

Důkaz. Jestliže je W podprostorem prostoru V , potom zřejmě (i)–(iii) platí, neboť sčítání vektorů a násobení vektorů skaláry je v podprostoru W stejné jako v prostoru V .

Jestliže naopak pro podmnožinu W prostoru V platí (i)–(iii), pak je na této množině definována operace sčítání i operace násobení prvků množiny V prvky tělesa T a tyto operace fungují stejně, jako když prvky množiny W považujeme za prvky prostoru V . Pro tyto operace platí axiomy (i)–(ii) a (v)–(viii) z definice 7.2, neboť tyto axiomy platí pro všechny prvky prostoru V . Protože je podle (i) množina W neprázdná, existuje prvek $u \in W$; podle (iii) je potom $0u = o \in W$. Pro každý prvek $v \in W$ je dále podle (iii) $(-1)v = -v \in W$, tj. množina W obsahuje s každým vektorem v i vektor k němu opačný. Platí tedy i axiomy (iii) a (iv) z definice 7.2. \square

Každý vektorový prostor V je zřejmě podprostorem sám v sobě. Tento podprostor se nazývá *nevlastní*; všechny ostatní podprostory prostoru V se nazývají

vlastní. Jednoprvková množina obsahující nulový vektor $o \in V$ je rovněž podprostorem prostoru V . Tento podprostor se nazývá *triviální* nebo *nulový*, značí se symbolem O . Ostatní podprostory prostoru V se nazývají *netriviální* nebo *nenulové*.

Nulový vektor prostoru V je nulovým vektorem každého podprostoru prostoru V . Relace „býti podprostorem“ je reflexivní, antisymetrická a tranzitivní.

7.8. Příklady.

(i) Množina všech vázaných vektorů v rovině se společným počátkem v pevně zvoleném bodě S je spolu se sčítáním vektorů a násobením vektorů reálnými čísly reálným vektorovým prostorem. Vedeme-li bodem S přímkou, pak všechny vektory, které leží na této přímce a mají počátek v bodě S , tvoří podprostor uvažovaného vektorového prostoru.

Podobný příklad dostaneme, uvažujeme-li vázané vektory v prostoru, které mají společný počátek v pevně zvoleném bodě S . Podprostory tohoto vektorového prostoru budou tvořeny množinami všech vektorů, jejichž vrcholy leží na nějaké přímce, resp. na nějaké rovině procházející bodem S ; není obtížné usoudit, že kromě nulového a nevlastního podprostoru další podprostory neexistují.

(ii) Množina $\mathbb{R}^{m \times n}$ všech reálných matic typu $m \times n$ spolu se sčítáním matic a násobením matic reálnými čísly je reálným vektorovým prostorem. Podprostorem tohoto prostoru je například množina všech matic typu $m \times n$, které mají na pevně zvolených místech nuly. Existuje však řada zajímavějších podprostorů, zejména v případě, kdy $m = n$. Viz příklad (vi).

(iii) Každé těleso T je vektorovým prostorem samo nad sebou. Sčítání vektorů definujeme jako sčítání prvků tělesa T a násobení vektorů skaláry jako násobení prvků tělesa T prvky tělesa T . Těleso \mathbb{R} je tedy reálným vektorovým prostorem, těleso \mathbb{C} je komplexním vektorovým prostorem, těleso \mathbb{Q} je vektorovým prostorem nad \mathbb{Q} , každé těleso \mathbb{Z}_p je vektorovým prostorem nad tělesem \mathbb{Z}_p apod. Uvědomme si, že těleso T jako vektorový prostor nad T má jen nulový a nevlastní podprostor.

(iv) Každé těleso T je vektorovým prostorem nad libovolným svým podtělesem T' . Sčítání vektorů (prvků z T) i násobení vektorů (prvků z T) skalárem (prvkem z T') definujeme jako sčítání, resp. násobení prvků tělesa T . Těleso komplexních čísel \mathbb{C} můžeme tedy chápat i jako reálný vektorový prostor nebo jako vektorový prostor nad tělesem racionálních čísel. Těleso reálných čísel \mathbb{R} je též vektorovým prostorem nad tělesem racionálních čísel.

(v) Množina $T^{m \times n}$ všech matic typu $m \times n$ nad tělesem T je vektorovým prostorem nad tělesem T (srovnej s příkladem (ii)). Podobně je množina T^n všech n -tic prvků tělesa T vektorovým prostorem nad tělesem T . Jde vlastně o prostor $T^{1 \times n}$, neboť každou n -tici prvků tělesa T můžeme chápat jako matici typu $1 \times n$. Sčítání dvou n -tic a násobení n -tice skalárem je tedy definováno rovnostmi

$$\begin{aligned}(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n), \\ c \cdot (a_1, a_2, \dots, a_n) &= (ca_1, ca_2, \dots, ca_n); \end{aligned}$$

říkáme, že sčítání n -tic a násobení n -tice skalárem se provádí „po složkách“.

(vi) V prostoru $T^{n \times n}$ všech čtvercových matic řádu n nad tělesem T můžeme vyšetřovat řadu podprostorů. Jsou to např.

- množina všech horních trojúhelníkových matic,
- množina všech dolních trojúhelníkových matic,
- množina všech diagonálních matic,
- množina všech skalárních matic,
- množina všech symetrických matic,
- množina všech antisymetrických matic.

Poznamenejme, že množina všech hermitovských matic řádu n není podprostorem komplexního vektorového prostoru $\mathbb{C}^{n \times n}$. Násobek hermitovské matice komplexním číslem totiž nemusí být hermitovská matice; např.

$$i \cdot \begin{pmatrix} 1 & i \\ -i & 2 \end{pmatrix} = \begin{pmatrix} i & -1 \\ 1 & 2i \end{pmatrix} .$$

Součet hermitovských matic však hermitovskou maticí je, rovněž tak reálný násobek hermitovské matice. Množina všech hermitovských matic řádu n je tedy podprostorem reálného prostoru všech komplexních matic řádu n .

(vii) Množina $T^{\mathbb{N}}$ všech nekonečných posloupností prvků tělesa T je vektorovým prostorem nad tělesem T . Sčítání takovýchto posloupností i násobení posloupnosti skalárem se provádí „po složkách“:

$$\begin{aligned} (a_1, a_2, \dots) + (b_1, b_2, \dots) &= (a_1 + b_1, a_2 + b_2, \dots) , \\ c \cdot (a_1, a_2, \dots) &= (ca_1, ca_2, \dots) . \end{aligned}$$

(viii) V reálném prostoru $\mathbb{R}^{\mathbb{N}}$ všech nekonečných posloupností reálných čísel můžeme vyšetřovat řadu zajímavých podprostorů; jsou to např.:

- množina všech posloupností s nulami na prvních n místech (n je pevně zvolené přirozené číslo),
- množina všech posloupností, které mají $(n+1)$ -ním místem počínaje samé nuly,
- množina všech posloupností, které mají jen konečně mnoho nenulových členů,
- množina všech konvergentních posloupností,
- množina všech posloupností s limitou nula.

Poznamenejme, že množina všech posloupností s limitou $c \neq 0$ není podprostorem prostoru $\mathbb{R}^{\mathbb{N}}$; tato množina totiž není uzavřena ani na sčítání ani na násobení skalárem.

(ix) Nechť X je množina a W vektorový prostor nad tělesem T . Symbolem W^X označme množinu všech zobrazení množiny X do množiny W . Součet zobrazení $f, g \in W^X$ a násobek zobrazení $f \in W^X$ skalárem $a \in T$ definujeme takto: pro každé $x \in X$ je

$$(f + g)(x) = f(x) + g(x) , \quad (af)(x) = a \cdot f(x) .$$

S takto definovanými operacemi je W^X vektorovým prostorem nad tělesem T . Speciální volbou množiny X , resp. prostoru W dostaneme další příklady vektorových prostorů; některé z nich již známe:

- prostor T^n ($W = T, X = \{1, 2, \dots, n\}$) — viz příklad (v),
- prostor $T^{\mathbb{N}}$ ($W = T, X = \mathbb{N}$) — viz příklad (vii),
- prostor $T^{m \times n}$ ($W = T, X = \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}$) — viz příklad (v),
- prostor T^X ($W = T$) — jde o prostor všech zobrazení množiny X do tělesa T ,
- prostor \mathbb{R}^X ($W = \mathbb{R}$) — jde o prostor všech reálných funkcí na množině X .

V prostoru W^X budeme někdy uvažovat podprostor $K(W^X)$ tvořený všemi zobrazeními množiny X do prostoru W , která jsou *skoro všude rovna nule* (tzv. *zobrazení s konečným nosičem*):

$$K(W^X) = \{ f : X \rightarrow W; \exists X' \subseteq X, X' \text{ je konečná, } \forall x \in X \setminus X' \quad f(x) = 0 \}$$

Prostor $K(T^{\mathbb{N}})$ je tedy tvořen všemi posloupnostmi prvků tělesa T , které mají jen konečně mnoho nenulových členů. Je zřejmé, že $K(T^n) = T^n$ a $K(T^{m \times n}) = T^{m \times n}$; dále je $K(T^X) = T^X$ právě tehdy, když je množina X konečná.

(x) Položíme-li v příkladu (ix) za X otevřený interval (a, b) a za W těleso \mathbb{R} jako reálný prostor, dojdeme k prostoru $\mathbb{R}^{(a,b)}$ všech reálných funkcí definovaných na intervalu (a, b) . V tomto prostoru můžeme vyšetřovat řadu zajímavých podprostorů sestávajících z funkcí, které mají na intervalu (a, b) nějakou rozumnou vlastnost:

- množina všech funkcí, které jsou na intervalu (a, b) omezené,
- množina všech funkcí, které jsou na intervalu (a, b) spojité,
- množina všech funkcí, které mají na intervalu (a, b) spojité derivace až do řádu n (n je pevně zvolené přirozené číslo),
- množina všech funkcí, které mají na intervalu (a, b) spojité derivace všech řádů,
- množina všech polynomů,
- množina všech polynomů stupně nejvýše n (n je pevně zvolené přirozené číslo),
- množina všech funkcí, které jsou nenulové jen pro konečně mnoho čísel z intervalu (a, b) (jde o prostor $K(\mathbb{R}^{(a,b)})$).

Poznamenejme, že množina všech polynomů stupně právě n , kde n je pevně zvolené přirozené číslo, netvoří podprostor prostoru $\mathbb{R}^{(a,b)}$; tato množina není uzavřená ani vzhledem ke sčítání ani vzhledem k násobení skalárem.

Za množinu X jsme mohli vzít i uzavřený nebo polouzavřený interval. U některých podprostorů bychom však museli trochu upřesnit jejich definici (např. spojitost zprava a zleva v krajních bodech intervalu). Podobně bychom mohli vytvářet prostory komplexních funkcí reálné proměnné apod.

7.9. Lemma. *Průnik neprázdného souboru podprostorů vektorového prostoru V nad tělesem T je podprostorem prostoru V .*

Důkaz. Průnik uvažovaného souboru podprostorů označme písmenem W . Protože nulový vektor prostoru V leží v každém podprostoru prostoru V , leží i v průniku W uvažovaného souboru; množina W je tedy neprázdná. Jestliže vektory

x, y leží v množině W , leží i v každém podprostoru uvažovaného souboru; podle 7.7 leží tedy v každém podprostoru uvažovaného souboru i vektory $x + y$ a ax , kde $a \in T$. Tyto vektory tedy leží i v průniku W . Podle 7.7 je W podprostorem prostoru V . \square

Průnik souboru $\{V_\alpha\}_{\alpha \in \Lambda}$ podprostorů prostoru V značíme

$$\bigcap_{\alpha \in \Lambda} V_\alpha ;$$

je-li indexová množina konečná, píšeme např.

$$\bigcap_{i=1}^n V_i, \quad V_1 \cap V_2 \cap V_3, \quad V_1 \cap V_2 \quad \text{apod.}$$

7.10. Definice. Nechť V je vektorový prostor nad tělesem T a M podmnožina prostoru V . Průnik všech podprostorů prostoru V , které množinu M obsahují, nazveme *lineární obal* množiny M a označíme symbolem $[M]$. Lineární obal podmnožiny $\{v_1, v_2, \dots, v_k\}$ prostoru V budeme značit symbolem $[v_1, v_2, \dots, v_k]$.

Lineární obal podmnožiny M prostoru V je podle předchozího lemmatu podprostorem prostoru V . Je to nejmenší podprostor prostoru V obsahující množinu M , neboť je podle definice obsažen ve všech podprostorech, které množinu M obsahují.

Lineární obal podmnožiny M prostoru V se dá popsat přímo pomocí prvků množiny M . Nejprve však musíme zavést pojem lineární kombinace.

7.11. Definice. Nechť V je vektorový prostor nad tělesem T , v_1, \dots, v_k vektory prostoru V a a_1, \dots, a_k prvky tělesa T . Vektor

$$\sum_{i=1}^k a_i v_i$$

se nazývá *lineární kombinace* vektorů v_1, \dots, v_k s koeficienty a_1, \dots, a_k . Jestliže je množina vektorů prázdná (v tom případě můžeme psát $k = 0$), pak hovoříme o *prázdné* lineární kombinaci, kterou klademe rovnou nulovému vektoru. Jestliže je $k \geq 1$, pak v případě $a_1 = a_2 = \dots = a_k = 0$ hovoříme o *triviální* lineární kombinaci a v opačném případě, tj. je-li aspoň jeden z koeficientů a_1, \dots, a_k nenulový, o *netriviální* lineární kombinaci.

Prázdná lineární kombinace je tzv. *prázdný součet*, který se klade rovný nulovému prvku, tj. neutrálnímu prvku operace sčítání. Podobně se *prázdný součin* klade rovný jednotkovému prvku, tj. neutrálnímu prvku operace násobení (pokud ovšem jednotkový prvek existuje). Zcela ve stejném duchu můžeme za průnik prázdného souboru podprostorů prostoru V považovat prostor V ; je to totiž neutrální prvek vůči operaci průniku (pro každý podprostor W prostoru V je $W \cap V = W$).

7.12. Věta. *Nechť V je vektorový prostor nad tělesem T . Lineární obal $[M]$ podmnožiny M prostoru V je roven množině všech lineárních kombinací vektorů množiny M s koeficienty z tělesa T .*

Důkaz. Jestliže je množina M prázdná, pak tvrzení platí. Průnik všech podprostorů, které M obsahují, je triviální podprostor. Na druhé straně lze z prázdné množiny vytvořit jedinečně prázdnou lineární kombinaci, která je rovna nulovému vektoru.

Předpokládejme, že M je neprázdná, a označme písmenem W množinu všech lineárních kombinací vektorů množiny M s koeficienty z tělesa T . Množina W je zřejmě neprázdná; součet dvou lineárních kombinací vektorů množiny M i násobek takovéto lineární kombinace je zřejmě opět lineární kombinací vektorů množiny M , takže podle 7.7 je množina W podprostorem prostoru V . Tento podprostor zřejmě obsahuje množinu M , neboť každý vektor $v \in M$ lze vyjádřit jako lineární kombinaci $v = 1 \cdot v$. Podle definice lineárního obalu je tedy $[M] \subseteq W$.

Lineární obal $[M]$ podmnožiny M je podprostorem prostoru V , který obsahuje všechny vektory množiny M . Podle 7.7 tedy obsahuje i všechny jejich násobky, součty těchto násobků, tj. i všechny lineární kombinace vektorů množiny M s koeficienty z tělesa T ; tedy $W \subseteq [M]$. \square

7.13. Příklady.

(i) Lineárním obalem podmnožiny $M = \{(1, 2, 3), (1, -1, 1)\}$ prostoru \mathbb{R}^3 je množina všech lineárních kombinací

$$a \cdot (1, 2, 3) + b \cdot (1, -1, 1), \quad \text{kde } a, b \in \mathbb{R}.$$

Je tedy $[M] = \{(a + b, 2a - b, 3a + b); a, b \in \mathbb{R}\}$.

(ii) Uvažujme prostor všech vázaných vektorů v prostoru, které mají společný počátek v pevně zvoleném bodě. Nechť u, v jsou dva nenulové vektory tohoto prostoru. Jestliže vektory u, v leží na jedné přímce, je tato přímka jejich lineárním obalem. Neleží-li na jedné přímce, je jejich lineárním obalem rovina, kterou určují; každý vektor této roviny lze totiž vyjádřit jako lineární kombinaci $au + bv$ a žádný jiný vektor takto vyjádřit nelze.

(iii) Lineárním obalem podmnožiny $\{1, x, x^2, x^3, \dots\}$ prostoru všech reálných funkcí spojitých na intervalu $(-\infty, \infty)$ je množina všech lineárních kombinací funkcí $1, x, x^2, x^3, \dots$, tj. podprostor všech polynomů $a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$, kde $n \geq 0, a_0, a_1, \dots, a_n \in \mathbb{R}$.

Nechť V je vektorový prostor nad tělesem T . Jestliže $M = \{v_1, \dots, v_k\}$ je podmnožina prostoru V , pak podle věty 7.12 je podprostor $[M]$ možno vyjádřit v tvaru

$$[M] = \left\{ \sum_{i=1}^k a_i v_i; a_1, \dots, a_k \in T \right\}.$$

Jestliže je množina $M = \{v_\alpha; \alpha \in \Lambda\}$ nekonečná, pak její lineární obal $[M]$ vyjádříme pomocí tzv. *formálně nekonečného součtu* v tvaru

$$[M] = \left\{ \sum_{\alpha \in \Lambda} a_\alpha v_\alpha; \forall \alpha \in \Lambda \quad a_\alpha \in T \right\}.$$

Vždy však předpokládáme, že pro skoro všechna $\alpha \in \Lambda$, tj. až na konečný počet výjimek, je $a_\alpha = 0$. Výraz $\sum_{\alpha \in \Lambda} a_\alpha v_\alpha$ tedy ve skutečnosti představuje lineární kombinaci popsanou v definici 7.11. Můžeme též psát

$$[M] = \left\{ \sum_{v \in M} a_v v; \forall v \in M \quad a_v \in T \right\};$$

přitom opět předpokládáme, že pro skoro všechny vektory $v \in M$ je ve výrazu $\sum_{v \in M} a_v v$ koeficient a_v roven nule. Toto označení, které využívá formálně nekonečné součty, se nám v některých důkazech bude hodit.

V následujícím odstavci shrneme několik vlastností, které vyplývají z definice 7.10 a věty 7.12.

7.14. Poznámka. Pro podmnožiny M, N vektorového prostoru platí:

- (i) $M \subseteq [M]$.
- (ii) Jestliže $M \subseteq N$, potom $[M] \subseteq [N]$.
- (iii) $[[M]] = [M]$.
- (iv) $[\emptyset] = O$.
- (v) Jestliže $M \subseteq N \subseteq [M]$, potom $[N] = [M]$.
- (vi) Inkluze $[M] \subseteq [N]$ platí právě tehdy, když je $M \subseteq [N]$.
- (vii) Rovnost $[M] = [N]$ platí právě tehdy, když je $M \subseteq [N]$ a $N \subseteq [M]$.
- (viii) Nechť $v_1, v_2, \dots, v_k \in V$, $a_1, a_2, \dots, a_k \in T$, $a_1 \neq 0$. Potom

$$\begin{aligned} [v_1, v_2, \dots, v_k] &= [a_1 v_1, v_2, \dots, v_k], \\ [v_1, v_2, \dots, v_k] &= [v_1, v_2 + a_2 v_1, \dots, v_k + a_k v_1]. \quad \square \end{aligned}$$

První tři vlastnosti charakterizují tzv. *uzávěrový operátor* na množině V , tj. zobrazení, které každé podmnožině M přiřazuje její uzávěr $[M]$. Z věty 7.12 vyplývá, že jde o tzv. *algebraický uzávěrový operátor*; to znamená, že každý vektor z uzávěru $[M]$ leží v uzávěru nějaké konečné podmnožiny množiny M (každý vektor je totiž podle 7.12 lineární kombinací konečně mnoha vektorů množiny M).

Tvrzení (vi) a (vii) se pomocí věty 7.12 dají slovně vyjádřit takto:

- Inkluze $[M] \subseteq [N]$ platí právě tehdy, když je každý vektor množiny M lineární kombinací vektorů množiny N .
- Rovnost $[M] = [N]$ platí právě tehdy, když je každý vektor množiny M lineární kombinací vektorů množiny N a každý vektor množiny N lineární kombinací vektorů množiny M . (Odtud ihned vyplývá tvrzení (viii).)

Tvrzení (viii) se v praxi využívá při přechodu od jedné množiny vektorů k jiné množině vektorů, při němž se nemění lineární obal (viz dále příklad 7.17).

7.15. Definice. Nechť V je vektorový prostor nad tělesem T a M podmnožina prostoru V . Jestliže lineárním obalem podmnožiny M je celý prostor V , pak říkáme, že M je *množinou generátorů* prostoru V , resp. že množina M *generuje* prostor V .

Prostor V se nazývá *konečně generovaný*, existuje-li konečná množina, která ho generuje; v opačném případě se prostor V nazývá *nekonečně generovaný*.

Jestliže je M množina generátorů prostoru V , pak každá podmnožina prostoru V , která M obsahuje, je také množinou generátorů prostoru V . Každý vektorový prostor má zřejmě množinu generátorů; např. množina V generuje prostor V .

7.16. Příklady. Vektorový prostor T^n nad tělesem T je konečně generovaný, neboť každá n -tice $(a_1, a_2, \dots, a_n) \in T^n$ je lineární kombinací vektorů

$$u_1 = (1, 0, 0, \dots, 0), \quad u_2 = (0, 1, 0, \dots, 0), \quad \dots, \quad u_n = (0, 0, 0, \dots, 1);$$

pro každé $i = 1, \dots, n$ je u_i n -ticí, která má na i -tém místě jedničku a na ostatních místech nuly, tj.

$$(a_1, a_2, \dots, a_n) = \sum_{i=1}^n a_i u_i.$$

Podobně usoudíme, že i prostor $T^{m \times n}$ je konečně generovaný. Těleso T jako vektorový prostor nad T i vektorový prostor komplexních čísel nad tělesem reálných čísel jsou konečně generované prostory. Konečně generované jsou rovněž prostory vázaných vektorů (se společným počátkem v daném bodě) v rovině či v prostoru.

Nekonečně generované prostory jsou např. $T^{\mathbb{N}}$, $K(T^{\mathbb{N}})$, prostor všech reálných funkcí definovaných na intervalu (a, b) i podprostory tohoto prostoru tvořené po řadě funkcemi omezenými, spojitými, se spojitými derivacemi, polynomy apod. V žádném z těchto prostorů neexistuje konečná množina generátorů. Tuto skutečnost hlouběji pochopíme v následujícím paragrafu o lineární nezávislosti.

7.17. Příklad. Uvažujme podprostor

$$W = [(2, 3, 1, 4), (1, 1, 2, 3), (3, 2, 1, 2), (4, 2, 1, 4)]$$

vektorového prostoru \mathbb{Z}_5^4 . Tento podprostor se nezmění (viz 7.14(viii)), když přetvoříme jeho množinu generátorů takto: ke druhému, třetímu a čtvrtému vektoru přičteme po řadě dvojnásobek prvního, první a trojnásobek prvního vektoru. Tedy

$$W = [(2, 3, 1, 4), (0, 2, 4, 1), (0, 0, 2, 1), (0, 1, 4, 1)].$$

Nyní přičteme dvojnásobek druhého vektoru ke čtvrtému:

$$W = [(2, 3, 1, 4), (0, 2, 4, 1), (0, 0, 2, 1), (0, 0, 2, 3)]$$

Čtyřnásobek třetího vektoru přičteme ke čtvrtému:

$$W = [(2, 3, 1, 4), (0, 2, 4, 1), (0, 0, 2, 1), (0, 0, 0, 2)]$$

Nyní je zřejmé, že $W = \mathbb{Z}_5^4$, neboť lineární kombinace posledních čtyř vektorů vytvářejí celý prostor \mathbb{Z}_5^4 ; každou čtveřici (a_1, a_2, a_3, a_4) totiž snadno vyjádříme jako lineární kombinaci uvedených vektorů:

$$(a_1, a_2, a_3, a_4) = x_1 \cdot (2, 3, 1, 4) + x_2 \cdot (0, 2, 4, 1) + x_3 \cdot (0, 0, 2, 1) + x_4 \cdot (0, 0, 0, 2)$$

Odtud

$$\begin{aligned} a_1 &= 2x_1, \\ a_2 &= 3x_1 + 2x_2, \\ a_3 &= x_1 + 4x_2 + 2x_3, \\ a_4 &= 4x_1 + x_2 + x_3 + 2x_4. \end{aligned}$$

Snadno se vypočte, že

$$x_1 = 3a_1, \quad x_2 = 3a_1 + 3a_2, \quad x_3 = 4a_2 + 3a_3, \quad x_4 = 4a_2 + a_3 + 3a_4.$$

Ukázali jsme (viz 7.9), že průnik souboru podprostorů vektorového prostoru je opět podprostorem tohoto prostoru. Sjednocení souboru podprostorů však obecně podprostorem není. Jako příklad stačí uvést sjednocení dvou různoběžných přímek v rovině, kterou chápeme jako vektorový prostor vázaných vektorů se společným počátkem v průsečíku zmíněných přímek. Jiným jednoduchým příkladem je sjednocení podprostorů symetrických a antisymetrických matic prostoru reálných matic druhého řádu. Sjednocení souboru podprostorů je sice uzavřeno na násobení vektorů skaláry, není však uzavřeno na sčítání vektorů.

Množinové operaci sjednocení odpovídá v teorii vektorových prostorů svým významem operace součtu (spojení) dvou nebo více podprostorů.

7.18. Definice. *Součtem (spojením) souboru podprostorů vektorového prostoru budeme rozumět lineární obal množinového sjednocení podprostorů tohoto souboru.*

Součet souboru $\{V_\alpha; \alpha \in \Lambda\}$ podprostorů prostoru V značíme

$$\sum_{\alpha \in \Lambda} V_\alpha;$$

je-li indexová množina konečná, píšeme např.

$$\sum_{i=1}^n V_i, \quad V_1 + V_2 + V_3, \quad V_1 + V_2 \quad \text{apod.}$$

Definici součtu souboru podprostorů $\{V_\alpha; \alpha \in \Lambda\}$ můžeme tedy symbolicky zapsat rovností

$$\sum_{\alpha \in \Lambda} V_\alpha = \left[\bigcup_{\alpha \in \Lambda} V_\alpha \right].$$

Součtem prázdného souboru podprostorů je triviální podprostor (jde o lineární obal prázdné množiny). Z předchozích výsledků (7.12 a 7.7) vyplývá, že součet souboru podprostorů je roven množině všech konečných součtů vektorů ze sjednocení podprostorů tohoto souboru. Je tedy

$$\begin{aligned} V_1 + V_2 &= \{v_1 + v_2; v_1 \in V_1, v_2 \in V_2\}, \\ \sum_{i=1}^n V_i &= \left\{ \sum_{i=1}^n v_i; v_1 \in V_1, \dots, v_n \in V_n \right\}, \\ \sum_{\alpha \in \Lambda} V_\alpha &= \left\{ \sum_{\alpha \in \Lambda} v_\alpha; \forall \alpha \in \Lambda \quad v_\alpha \in V_\alpha \right\}; \end{aligned}$$

připomeňme znovu, že ve formálním součtu $\sum_{\alpha \in \Lambda} v_\alpha$ jsou skoro všechny vektory v_α rovny nulovému vektoru.

Zatímco průnik souboru podprostorů prostoru V je největším podprostorem prostoru V , který je obsažen ve všech podprostorech daného souboru, tak součet tohoto souboru je nejmenším podprostorem prostoru V , který všechny podprostory daného souboru obsahuje.

Množina všech podprostorů vektorového prostoru s operacemi průniku a součtu je *úplný svaz*. Je totiž částečně uspořádána inkluzí; *infimem*, resp. *supremem* daného souboru podprostorů je průnik, resp. součet tohoto souboru.

7.19. Příklad.

(i) Nechť V je vektorový prostor všech vázaných vektorů v prostoru, které mají společný počátek v pevně zvoleném bodě S . Součtem dvou různoběžných přímek procházejících bodem S – jako podprostorů prostoru V – je rovina těmito přímkami proložená. Součtem přímky p a roviny ϱ , které obě procházejí bodem S , je celý prostor V , pokud ovšem přímka p neleží v rovině ϱ ; v opačném případě je jejich součtem rovina ϱ . Součtem dvou různých rovin procházejících bodem S je celý prostor V .

(ii) Součtem prostorů

$$W_1 = [(1, 2, 3), (0, 1, 1)], \quad W_2 = [(1, 0, 0), (1, 1, 1)]$$

prostoru \mathbb{R}^3 je prostor

$$W_1 + W_2 = [(1, 2, 3), (0, 1, 1), (1, 0, 0), (1, 1, 1)] = \mathbb{R}^3.$$

(iii) Nechť V_i , $i = 1, 2, \dots$, je podprostor prostoru $T^{\mathbb{N}}$ tvořený všemi posloupnostmi prvků tělesa T , které mají nuly na všech místech kromě i -tého. Součtem podprostorů V_1, V_2, \dots je podprostor $K(T^{\mathbb{N}})$; tj. $K(T^{\mathbb{N}}) = \sum_{i=1}^{\infty} V_i$.

7.20. Definice. Nechť V je vektorový prostor nad tělesem T a W jeho podprostor. *Lineární množinou* určenou vektorem $v \in V$ a podprostorem W budeme rozumět množinu $v + W = \{v + w; w \in W\}$.

Lineární množinu $v + W$ si můžeme představit jako „podprostor W posunutý o vektor v “ (viz příklad 7.22).

7.21. Lemma. *Nechť V je vektorový prostor nad tělesem T , W jeho podprostor a $v_1, v_2 \in V$. Potom platí:*

- (i) *Pro každý vektor $v \in V$ je $v \in v + W$.*
- (ii) *Jestliže $v_1 \in v_2 + W$, potom $v_1 + W = v_2 + W$.*
- (iii) *Lineární množiny $v_1 + W$, $v_2 + W$ se buď rovnají nebo jsou disjunktní.*
- (iv) *Rovnost $v_1 + W = v_2 + W$ nastane právě tehdy, když $v_1 - v_2 \in W$.*
- (v) *Lineární množina $v + W$ je určena libovolným svým prokem (a podprostorem W).*
- (vi) *Prostor V je disjunktním sjednocením lineárních množin určených podprostorem W .*

Důkaz.

(i) Zřejmě je $v = v + 0$, takže $v \in v + W$.

(ii) Jestliže $v_1 \in v_2 + W$, potom $v_1 = v_2 + w_0$, kde $w_0 \in W$. Pro každý vektor $w \in W$ je nyní

$$v_1 + w = v_2 + w_0 + w \in v_2 + W \quad \text{a} \quad v_2 + w = v_1 - w_0 + w \in v_1 + W,$$

takže $v_1 + W = v_2 + W$.

(iii) Mají-li lineární množiny $v_1 + W$ a $v_2 + W$ společný prvek v_3 , pak je podle tvrzení (ii) $v_1 + W = v_3 + W = v_2 + W$.

(iv) Jestliže $v_1 - v_2 = w_0 \in W$, pak mají lineární množiny $v_1 + W, v_2 + W$ společný vektor $v_1 = v_2 + w_0$ a jsou podle tvrzení (iii) totožné. Jsou-li naopak totožné, je zřejmě $v_1 = v_2 + w_0 \in v_2 + W$, $w_0 \in W$, tj. $v_1 - v_2 = w_0 \in W$.

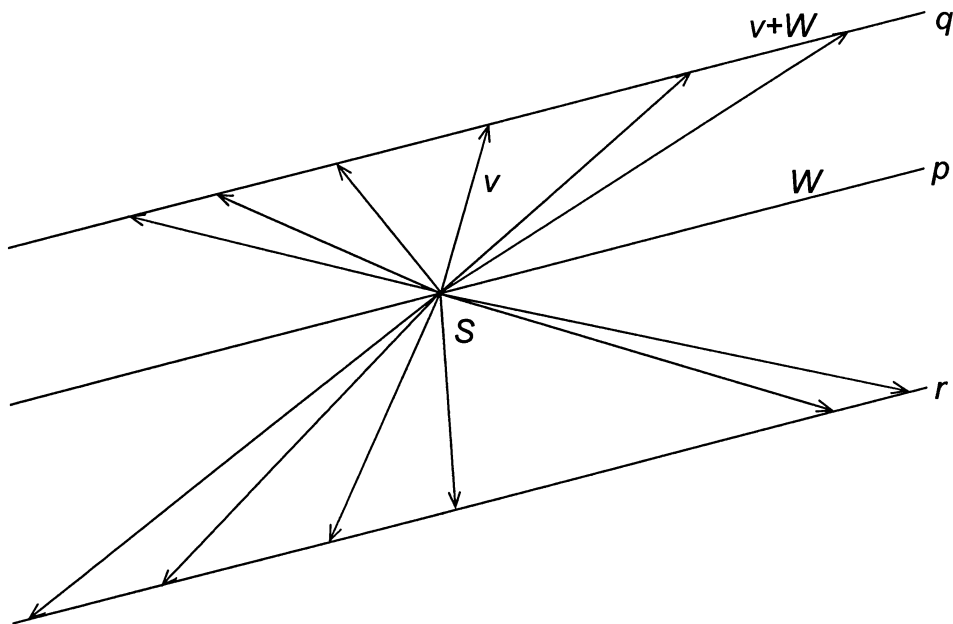
(v) Toto tvrzení ihned vyplývá z 7.21(ii).

(vi) Tvrzení vyplývá z 7.21(i) a (iii). \square

7.22. Příklad. Nechť V je vektorový prostor všech vázaných vektorů v rovině, které mají společný počátek v pevně zvoleném bodě S ; nechť W je podprostor tvořený všemi vektory prostoru V , které leží na pevně zvolené přímce p procházející bodem S .

Pro každý vektor $v \in V$ je lineární množina $v + W$ tvořena všemi vektory, jejichž vrcholy leží na přímce q , která je rovnoběžná s přímkou p a prochází vrcholem vektoru v . Celý prostor V je disjunktním sjednocením všech lineárních množin určených podprostorem W — všech přímek, které jsou rovnoběžné s přímkou p ;

každá takováto přímka r je chápána jako množina všech vektorů, jejichž počátek je v bodě S a vrchol na přímce r .



Podobný příklad dostaneme, budeme-li uvažovat vektorový prostor V všech vázaných vektorů v prostoru, které mají společný počátek v daném bodě S , a podprostor W tvořený všemi vektory, které leží na dané přímce (resp. rovině) tímto bodem procházející.

Nechť W je podprostorem vektorového prostoru V nad tělesem T . Symbolem V/W označme množinu všech lineárních množin prostoru V určených podprostorem W ; znovu připomeňme, že dva různé vektory $v_1, v_2 \in V$ mohou určovat touž lineární množinu (to nastane právě když je $v_1 - v_2 \in W$ — viz 7.21(iv)).

Nyní budeme definovat sčítání lineárních množin a násobení lineárních množin skaláry. Pro $v_1, v_2 \in V$ definujeme

$$(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$$

a pro $v \in V$ a $a \in T$

$$a \cdot (v + W) = av + W .$$

Vzhledem k tomu, že definice těchto operací závisí na označení lineárních množin (na volbě vektorů $v_1, v_2, v \in V$), které není jednoznačné, musíme prověřit jejich korektnost.

Jestliže $v_1 + W = v'_1 + W$ a $v_2 + W = v'_2 + W$, potom je podle 7.21(iv) $v_1 - v'_1 \in W$ a $v_2 - v'_2 \in W$. Protože je W podprostor, je též $v_1 - v'_1 + v_2 - v'_2 \in W$; podle 7.21(iv) je tedy $(v_1 + v_2) + W = (v'_1 + v'_2) + W$ a korektnost definice sčítání je prověřena.

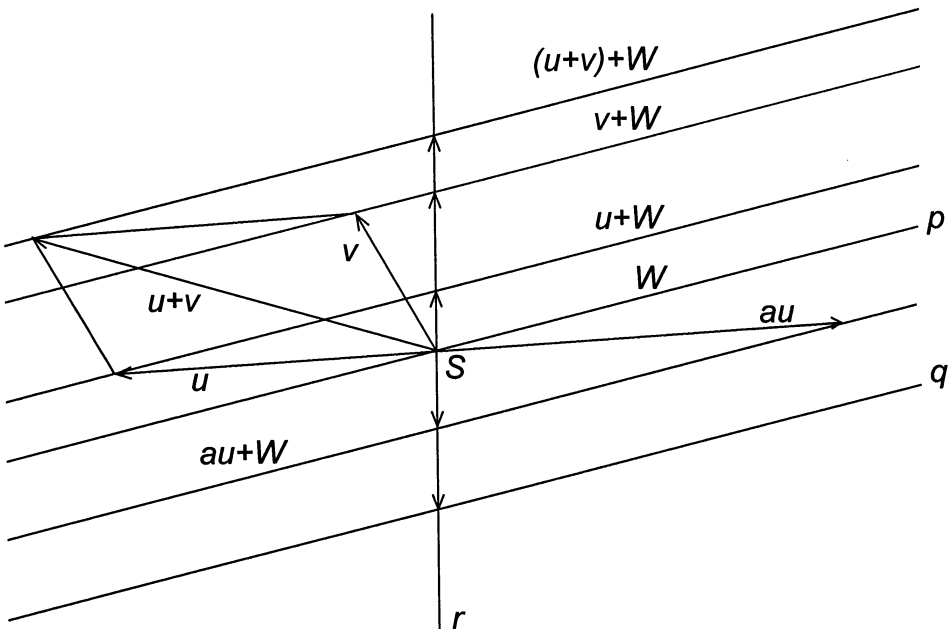
Jestliže je $v + W = v' + W$, potom je podle 7.21(iv) $v - v' \in W$. Protože je W podprostor, je též $a(v - v') \in W$; podle 7.21(iv) je tedy $av + W = av' + W$ a tím je prověřena i korektnost definice násobení skalářem.

Snadno se uváží, že pro tyto operace platí všechny axiomy z definice vektorového prostoru; je to bezprostředním důsledkem platnosti těchto axiomů pro operace původního vektorového prostoru V .

7.23. Definice. Nechť W je podprostorem vektorového prostoru V nad tělesem T . Vektorový prostor V/W všech lineárních množin prostoru V určených podprostorem W se nazývá *faktorový prostor* prostoru V podle podprostoru W .

Nulovým vektorem faktorového prostoru V/W je lineární množina $o + W = W$. Jestliže je W triviální podprostor, jsou lineární množiny jednoprvkové a faktorový prostor V/W se prakticky neliší od prostoru V . Jestliže je $W = V$, potom je faktorový prostor V/W triviální.

7.24. Příklady.



(i) Uvažujme prostor V a jeho podprostor W z příkladu 7.22. Faktorový prostor V/W si můžeme představit jako množinu všech přímek, které jsou s danou přímkou p rovnoběžné. Sčítání těchto přímek a násobení takovéto přímky skalárem se provádí pomocí sčítání vektorů a násobení vektoru skalárem; stačí zvolit ke každé přímce jeden vektor, který má na ní vrchol (viz obrázek).

Vedme bodem S přímkou r , která je různá od přímky p . Každá rovnoběžka q s přímkou p je určena svým průsečíkem s přímkou r . Lineární množinu q , tj. vektor prostoru V/W , si tedy můžeme představit jako vektor spojující bod S s průsečíkem přímek q a r . Faktorový prostor V/W si pak můžeme představit jako množinu vektorů přímky r se společným počátkem v bodě S .

(ii) Nechť V je prostor všech polynomů s reálnými koeficienty na intervalu $(-\infty, \infty)$ a W prostor všech polynomů bez absolutního členu. Dva polynomy leží v téže lineární množině určené podprostorem W právě tehdy, když jejich rozdíl leží ve W (viz 7.21(iv)), tj. právě tehdy, když mají stejný absolutní člen. Součtem dvou lineárních množin $f+W$ a $g+W$ je lineární množina $(f+g)+W$ všech polynomů, jejichž absolutní člen je součtem absolutních členů polynomů f a g . Podobně pro násobek.

7.25. Definice. Nechť V je vektorový prostor nad tělesem T . Na množině V nechť je dána binární operace \cdot násobení vektorů. Jestliže je množina V vzhledem ke sčítání a násobení vektorů asociativním okruhem a jestliže pro každé $x, y \in V$ a $a \in T$ je

$$(ax)y = a(xy) = x(ay) ,$$

potom se množina V nazývá *lineární algebra* nad tělesem T . Jestliže T je těleso reálných, resp. komplexních čísel, pak hovoříme o *reálné*, resp. *komplexní* lineární algebře. V závislosti na vlastnostech binární operace násobení vektorů hovoříme o *komutativní* lineární algebře, o algebře *s jednotkovým prvkem* apod.

Podalgebrou algebry V budeme rozumět každou její podmnožinu, která je algebrou nad tělesem T vzhledem ke stejnému sčítání a násobení vektorů a stejnému násobení vektorů skaláry z tělesa T (opět jde o zúžení operací z množiny V na nějakou její podmnožinu).

Podobně jako v 7.7 se dokáže, že podmnožina W algebry V je podalgebrou právě tehdy, když platí:

- (i) $W \neq \emptyset$,
- (ii) $\forall u, v \in W \quad u + v \in W$,
- (iii) $\forall u, v \in W \quad uv \in W$,
- (iv) $\forall u \in W \quad \forall a \in T \quad au \in W$.

Poznamenejme ještě, že stejným symbolem \cdot (který často vynecháváme) značíme binární operaci násobení skalárů, binární operaci násobení vektorů a násobení vektorů skaláry.

7.26. Příklady.

(i) Množina $T^{n \times n}$ čtvercových matic řádu n nad tělesem T je lineární algebrou nad tělesem T . Operace sčítání a násobení matic a násobení matice skalárem totiž mají všechny vlastnosti požadované v definici 7.25. Tato algebra má jednotkový prvek (jednotková matice) a je pro $n > 1$ nekomutativní.

(ii) Každé těleso T je lineární algebrou samo nad sebou. Je komutativní a má jednotkový prvek.

(iii) Každé těleso je lineární algebrou nad libovolným svým podtělesem. Je komutativní a má jednotkový prvek. Např. těleso \mathbb{C} je reálnou lineární algebrou, její podalgebrou je algebra reálných čísel.

(iv) Nekomutativní těleso kvaternionů je reálnou lineární algebrou; tato algebra má jednotkový prvek. Podalgebrou této nekomutativní algebry je komutativní reálná algebra komplexních čísel.

8. LINEÁRNÍ ZÁVISLOST A NEZÁVISLOST

8.1. Definice. Nechť V je vektorový prostor nad tělesem T . Nechť M je podmnožina prostoru V a S soubor vektorů prostoru V .

Podmnožina M se nazývá *lineárně závislá*, jestliže nějaký vektor množiny M je možno vyjádřit jako lineární kombinaci ostatních vektorů této množiny. V opačném případě se množina M nazývá *lineárně nezávislá*.

Jestliže se v souboru S alespoň jeden vektor vyskytuje vícekrát, říkáme, že je soubor S *lineárně závislý*. Jestliže se v souboru S žádný vektor neopakuje, je tento soubor podmnožinou prostoru V a je lineárně závislý nebo nezávislý podle předchozí definice.

Podmnožina M prostoru V je tedy lineárně nezávislá, jestliže žádný její vektor není lineární kombinací ostatních vektorů této množiny.

Prázdná množina je podle definice 8.1 lineárně nezávislá. Pokud množina M obsahuje nulový vektor, je lineárně závislá. Jestliže totiž množina M obsahuje kromě nulového vektoru ještě nějaký vektor v , potom je $0 = 0 \cdot v$; nulový vektor však můžeme rovněž vyjádřit jako prázdnou lineární kombinaci (i v případě, kdy je $M = \{0\}$).

Jednoprvková množina $\{v\}$, kde v je nenulový vektor, je lineárně nezávislá. Dvouprvková množina $\{v_1, v_2\}$ je lineárně závislá, jestliže je některý z vektorů v_1, v_2 násobkem druhého.

Každá podmnožina lineárně nezávislé množiny je lineárně nezávislá. Každá „nadmnožina“ lineárně závislé množiny je lineárně závislá.

Hovoříme-li o lineární závislosti či nezávislosti vektorů v_1, \dots, v_k , míníme tím lineární závislost či nezávislost souboru $\{v_1, \dots, v_k\}$.

8.2. Příklady.

(i) Množina

$$\{(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, 0, \dots, 1)\}$$

vektorového prostoru T^n je lineárně nezávislá, neboť žádný její vektor není možno vyjádřit jako lineární kombinaci vektorů ostatních.

(ii) Vektory

$$(2, 1, 1, 1), (1, 2, 1, 1), (1, 1, 2, 1), (1, 1, 1, 2)$$

vektorového prostoru \mathbb{Z}_5^4 jsou lineárně závislé. Každý z nich je totiž součtem čtyřnásobků ostatních vektorů.

(iii) Vektory $(1+i, 2i, -i)$, $(2, 2+2i, -1-i)$ komplexního prostoru \mathbb{C}^3 jsou lineárně závislé, neboť druhý vektor je $(1-i)$ -násobkem prvního. Jako vektory reálného prostoru \mathbb{C}^3 jsou ovšem lineárně nezávislé.

(iv) Vektory $\sin x$, $\cos x$ vektorového prostoru všech funkcí definovaných na intervalu $\langle 0, \pi \rangle$ jsou lineárně nezávislé. Na množině $\{k\pi; k = 0, 1, 2, \dots\}$ jsou však tyto funkce lineárně závislé, neboť na této množině je $\sin x = 0$.

8.3. Věta. *Nechť M je podmnožina vektorového prostoru V nad tělesem T . Následující tvrzení jsou ekvivalentní.*

- (i) *Množina M je lineárně závislá.*
- (ii) *Nulový vektor je možno vyjádřit jako netriviální lineární kombinaci navzájem různých vektorů množiny M .*
- (iii) *Existuje vlastní podmnožina N množiny M , pro kterou je $[N] = [M]$.*

Důkaz.

(i) \Rightarrow (ii) Je-li M lineárně závislá, je některý její vektor lineární kombinací vektorů ostatních, např.

$$v = \sum_{i=1}^k a_i v_i, \text{ kde } v, v_1, \dots, v_k \in M.$$

Zřejmě je možno předpokládat, že vektory $v, v_1, \dots, v_k \in M$ jsou navzájem různé. Potom je však

$$0 = \sum_{i=1}^k a_i v_i - 1 \cdot v,$$

tj. nulový vektor je netriviální lineární kombinací navzájem různých vektorů množiny M .

(ii) \Rightarrow (i) Jestliže je nulový vektor netriviální lineární kombinací navzájem různých vektorů množiny M , tj.

$$0 = \sum_{i=1}^k a_i v_i,$$

kde např. $a_1 \neq 0$, potom je

$$v_1 = \sum_{i=2}^k \left(-\frac{a_i}{a_1}\right) \cdot v_i,$$

tj. M je lineárně závislá podle definice 8.1.

(iii) \Rightarrow (i) Jestliže je $N \subset M$ a $[N] = [M]$, pak se vektor $v \in M \setminus N$ dá vyjádřit jako lineární kombinace vektorů množiny N , tj. množina M je lineárně závislá.

(i) \Rightarrow (iii) Jestliže je množina M lineárně závislá, tj. některý vektor $v \in M$ je vyjádřen jako lineární kombinace ostatních vektorů množiny M , potom je

$$[M \setminus \{v\}] = [M];$$

do každé lineární kombinace vektorů množiny M dosadíme za vektor v jeho vyjádření a dostaneme lineární kombinaci vektorů množiny $M \setminus \{v\}$. \square

8.4. Důsledek. *Nechť M je podmnožina vektorového prostoru V nad tělesem T . Následující tvrzení jsou ekvivalentní.*

- (i) *Množina M je lineárně nezávislá.*
- (ii) *Nulový vektor není možno vyjádřit jako netriviální lineární kombinaci navzájem různých vektorů množiny M .*
- (iii) *Pro každou vlastní podmnožinu N množiny M je $[N] \subset [M]$. \square*

Na základě věty 8.3, resp. důsledku 8.4 se v praktických příkladech lineární závislost a nezávislost zjišťuje.

8.5. Příklady.

(i) Zjistíme, zda vektory $(1, 2, 3)$, $(2, 5, 6)$, $(4, 2, 5)$ reálného vektorového prostoru \mathbb{R}^3 jsou lineárně závislé nebo nezávislé.

Utvořme obecnou lineární kombinaci těchto tří vektorů a předpokládejme, že se rovná nulovému vektoru:

$$a \cdot (1, 2, 3) + b \cdot (2, 5, 6) + c \cdot (4, 2, 5) = (0, 0, 0)$$

Odtud

$$\begin{aligned} a + 2b + 4c &= 0, \\ 2a + 5b + 2c &= 0, \\ 3a + 6b + 5c &= 0. \end{aligned}$$

Vyjádríme-li z první rovnice a , pak po dosazení do zbývajících dvou rovnic zjistíme, že $a = b = c = 0$. Uvažovaná lineární kombinace je triviální a dané vektory jsou lineárně nezávislé.

(ii) Nechť u, v, w jsou lineárně nezávislé vektory prostoru V nad tělesem T . Zjistíme, zda množina $M = \{u + v, u + w, v + w\}$ je lineárně závislá nebo nezávislá.

Utvořme obecnou lineární kombinaci vektorů množiny M a předpokládejme, že je rovna nulovému vektoru:

$$a \cdot (u + v) + b \cdot (u + w) + c \cdot (v + w) = o$$

Odtud

$$(a + b) \cdot u + (a + c) \cdot v + (b + c) \cdot w = o.$$

Protože jsou vektory u, v, w lineárně nezávislé, je nutně

$$\begin{aligned} a + b &= 0, \\ a + c &= 0, \\ b + c &= 0. \end{aligned}$$

Odečteme-li třetí rovnici od součtu prvních dvou, vyjde $2a = 0$. Je-li $\text{char } T \neq 2$, pak je $a = b = c = 0$ a množina M je lineárně nezávislá. Je-li $\text{char } T = 2$, můžeme položit $a = b = c = 1$, tj. množina M je lineárně závislá (součet uvažovaných tří vektorů je roven nulovému vektoru).

(iii) Zjistíme, zda vektory $2x^2 + 3x + 1$, $x^2 + x + 1$, $x^2 + 3x - 1$ vektorového prostoru všech reálných spojitých funkcí jsou lineárně závislé nebo nezávislé.

Utvoříme obecnou lineární kombinaci těchto vektorů a budeme zkoumat, kdy je rovna nulovému vektoru:

$$a \cdot (2x^2 + 3x + 1) + b \cdot (x^2 + x + 1) + c \cdot (x^2 + 3x - 1) = 0$$

Odtud

$$(2a + b + c) \cdot x^2 + (3a + b + 3c) \cdot x + (a + b - c) = 0 .$$

Má-li tato rovnost platit identicky, musí být

$$2a + b + c = 0 ,$$

$$3a + b + 3c = 0 ,$$

$$a + b - c = 0 .$$

Vypočteme z poslední rovnice a , dosadíme do prvních dvou rovnic a dojdeme k jediné rovnici $3c - b = 0$. Snadno zjistíme, že rovnici vyhovují např. hodnoty $a = -2$, $b = 3$, $c = 1$. Uvažovaná lineární kombinace tedy nemusí být triviální, takže dané tři vektory jsou lineárně závislé.

8.6. Lemma. *Nechť M je lineárně nezávislá podmnožina vektorového prostoru V a v vektor tohoto prostoru. Jestliže množina $M \cup \{v\}$ je lineárně závislá, potom je $v \in [M]$.*

Důkaz. Protože je množina $M \cup \{v\}$ lineárně závislá, existuje netriviální lineární kombinace navzájem různých vektorů množiny $M \cup \{v\}$, která je rovna nulovému vektoru. Je tedy

$$av + \sum_{i=1}^k a_i v_i = 0 , \quad \text{kde } v_1, \dots, v_k \in M .$$

Protože je množina M lineárně nezávislá, je $a \neq 0$. Tedy

$$v = \sum_{i=1}^k \left(-\frac{a_i}{a}\right) \cdot v_i ,$$

tj. $v \in [M]$. \square

8.7. Lemma. *Podmnožina M vektorového prostoru V je lineárně nezávislá právě tehdy, když je každá její konečná podmnožina lineárně nezávislá.*

Důkaz. Je-li množina M lineárně nezávislá, pak je zřejmě každá její podmnožina (konečná i nekonečná) lineárně nezávislá.

Jestliže je naopak množina M lineárně závislá, je nějaký její vektor lineární kombinací ostatních jejích vektorů, např.

$$v = \sum_{i=1}^k a_i v_i ,$$

kde v, v_1, \dots, v_k jsou navzájem různé vektory množiny M . Konečná podmnožina $\{v, v_1, \dots, v_k\}$ množiny M je potom lineárně závislá. \square

Předchozí lemma říká, že lineární nezávislost je tzv. *vlastnost konečného charakteru*, tj. vlastnost, kterou má množina právě tehdy, když ji má každá její konečná podmnožina. Vlastnosti konečného charakteru umožňují užití Zornova lemmatu (viz následující lemma a druhá část důkazu věty 8.11).

8.8. Lemma. *Sjednocení řetězce lineárně nezávislých podmnožin vektorového prostoru V je opět lineárně nezávislá podmnožina prostoru V .*

Důkaz. Necht $\{M_\alpha\}_{\alpha \in \Lambda}$ je (spočetný nebo nespočetný) řetězec lineárně nezávislých podmnožin vektorového prostoru V , tj. pro každé $\alpha, \alpha' \in \Lambda$ je buď $M_\alpha \subseteq M_{\alpha'}$ nebo $M_{\alpha'} \subseteq M_\alpha$. Necht M je sjednocení tohoto řetězce, tj.

$$M = \bigcup_{\alpha \in \Lambda} M_\alpha .$$

Předpokládejme, že $K = \{x_1, \dots, x_k\}$ je libovolně zvolená konečná podmnožina množiny M . Každý prvek $x_i \in K$ je obsažen v nějaké podmnožině M_{α_i} , celá množina K je tedy obsažena v největší z těchto podmnožin (ta existuje, neboť jde o řetězec). Protože je tato množina podle předpokladu lineárně nezávislá, je i její podmnožina K lineárně nezávislá. Podle lemmatu 8.7 je množina M lineárně nezávislá. \square

8.9. Definice. *Bází vektorového prostoru budeme rozumět každou jeho lineárně nezávislou množinu generátorů.*

8.10. Příklady.

(i) Prázdná množina je bází triviálního prostoru. Je lineárně nezávislá a generuje triviální prostor, neboť nulový vektor je prázdnou lineární kombinací (lineární kombinací prázdné množiny vektorů).

(ii) Každá jednoprvková množina $\{a\}$, kde a je nenulový prvek tělesa T , je bází prostoru T . Jiné báze tohoto prostoru neexistují.

(iii) Ve vektorovém prostoru všech vázaných vektorů roviny (resp. prostoru), které mají společný počátek v pevně zvoleném bodě S , je bází každá dvojice (resp. trojice) vektorů, které neleží v téže přímce (resp. rovině).

(iv) Bází prostoru \mathbb{C} nad tělesem \mathbb{R} (vektorový prostor komplexních čísel nad tělesem reálných čísel) je např. dvouprvková množina $\{1, i\}$. Dalšími bázemi jsou např. $\{2, 3 + 81i\}$, $\{1 + i, 1 - i\}$, $\{9 + 3i, 1 - 8i\}$ apod.

(v) Bází prostoru T^n je např. množina

$$\{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)\}.$$

Tato báze se nazývá *kanonická* nebo *standardní*.

(vi) Bází prostoru $T^{m \times n}$ je např. množina mn matic

$$\{E_{ij}\}_{i=1, \dots, m, j=1, \dots, n},$$

kde každá matice E_{ij} má na místě ij jedničku a na ostatních místech nuly. Také této bázi se někdy říká *kanonická*.

(vii) Nekonečná spočetná množina

$$\{(1, 0, 0, \dots), (0, 1, 0, \dots), (0, 0, 1, \dots), \dots\}$$

není bází vektorového prostoru $T^{\mathbb{N}}$ všech nekonečných posloupností prvků tělesa T ; je sice lineárně nezávislá, ale generuje pouze podprostor $K(T^{\mathbb{N}})$ prostoru $T^{\mathbb{N}}$, který obsahuje právě všechny posloupnosti mající jen konečný počet nenulových prvků.

(viii) Jednou z bází prostoru $T[x]$ všech polynomů nad tělesem T je nekonečná, ale spočetná množina $\{1, x, x^2, \dots\}$.

(ix) Nespočetná množina

$$\{f_c\}_{c \in (a, b)}$$

reálných funkcí definovaných na intervalu (a, b) , kde pro každé $c \in (a, b)$ je

$$f_c(c) = 1 \quad \text{a} \quad f_c(x) = 0 \quad \text{pro každé} \quad x \in (a, b), \quad x \neq c,$$

je bází prostoru $K(\mathbb{R}^{(a, b)})$ všech funkcí definovaných na intervalu (a, b) , které mají na tomto intervalu konečný nosič (viz příklad 7.8(ix)–(x)).

8.11. Věta. *Každá lineárně nezávislá podmnožina vektorového prostoru je částí nějaké báze tohoto prostoru.*

Důkaz.

(i) Předpokládejme nejprve, že V je konečně generovaný vektorový prostor; nechť $\{v_1, \dots, v_k\}$ je nějaká jeho množina generátorů a M lineárně nezávislá podmnožina. Položme

$$M_1 = \begin{cases} M, & \text{jestliže} \quad v_1 \in [M], \\ M \cup \{v_1\}, & \text{jestliže} \quad v_1 \notin [M]. \end{cases}$$

Podle lemmatu 8.6 je množina M_1 lineárně nezávislá; navíc je $v_1 \in [M_1]$. Položme dále

$$M_2 = \begin{cases} M_1, & \text{jestliže } v_2 \in [M_1], \\ M_1 \cup \{v_2\}, & \text{jestliže } v_2 \notin [M_1]. \end{cases}$$

Podle lemmatu 8.6 je množina M_2 lineárně nezávislá; navíc je $v_1, v_2 \in [M_2]$. Po k krocích dojdeme k lineárně nezávislé množině M_k , jejíž lineární obal $[M_k]$ obsahuje množinu generátorů $\{v_1, \dots, v_k\}$ prostoru V . Množina M_k proto generuje prostor V a je tedy bází prostoru V , která obsahuje množinu M .

(ii) Předpokládejme nyní, že V je prostor, který není konečně generovaný, nechť M je jeho lineárně nezávislá podmnožina. Uvažujme množinu \mathfrak{A} všech lineárně nezávislých podmnožin prostoru V , které obsahují množinu M . Množina \mathfrak{A} je neprázdná ($M \in \mathfrak{A}$), je částečně uspořádaná inkluzí a podle lemmatu 8.8 je induktivní. Podle Zornova lemmatu existuje v množině \mathfrak{A} maximální prvek N . Ukážeme, že množina N generuje prostor V . Nechť $v \in V$ je libovolný vektor, který neleží v množině N . Z maximality množiny N vyplývá, že množina $N \cup \{v\}$ je lineárně závislá. Podle lemmatu 8.6 je tedy $v \in [N]$. Pro každý vektor $v \in V$ je tedy $v \in [N]$, tj. množina N generuje prostor V . Množina N je proto bází prostoru V , která obsahuje lineárně nezávislou množinu M . \square

Z důsledku 8.4(iii) vyplývá, že báze prostoru V je minimální množinou generátorů tohoto prostoru. Na druhé straně je každá báze prostoru V maximální lineárně nezávislou množinou (viz lemma 8.6, resp. důkaz věty 8.11).

Jako důsledek předchozí věty můžeme vyslovit toto důležité zjištění:

8.12. Věta. *Každý vektorový prostor má bázi.*

Důkaz. Protože v každém vektorovém prostoru existuje lineárně nezávislá podmnožina (např. prázdná množina), existuje podle předchozí věty i báze tohoto prostoru. \square

8.13. Věta. *Nechť V je vektorový prostor nad tělesem T . Podmnožina M prostoru V je bází prostoru V právě tehdy, když ke každému vektoru $x \in V$ existuje právě jediný soubor $\{a_v\}_{v \in M}$ obsahující pouze konečně mnoho nenulových prvků, pro který je*

$$x = \sum_{v \in M} a_v v .$$

Důkaz. Nechť M je báze prostoru V . Protože je M množinou generátorů prostoru V , je každý vektor $x \in V$ lineární kombinací vektorů báze M . Tuto lineární kombinaci můžeme zapsat v tvaru

$$x = \sum_{v \in M} a_v v ,$$

kde je jen konečně mnoho koeficientů a_v nenulových (viz poznámka před 7.14). Jestliže je $x = \sum_{v \in M} b_v v$ druhá taková lineární kombinace, potom je

$$0 = \sum_{v \in M} (a_v - b_v) v$$

a z lineární nezávislosti množiny M plyne rovnost $a_v = b_v$ pro každé $v \in M$.

Jestliže je naopak splněna podmínka uvedená ve větě, je zřejmě M množinou generátorů prostoru V . Kdyby byla množina M lineárně závislá, byl by nějaký její vektor lineární kombinací ostatních vektorů množiny M a to by bylo ve sporu s jednoznačností vyjádření, kterou jsme předpokládali. Množina M je tedy bází prostoru V . \square

Na základě předchozí věty můžeme nyní definovat souřadnice vektoru.

8.14. Definice. Nechť M je báze vektorového prostoru V nad tělesem T . *Souborem souřadnic* vektoru $x \in V$ vzhledem k bázi M budeme rozumět jednoznačně určený soubor $\{a_v\}_{v \in M}$ (obsahující jen konečně mnoho nenulových prvků), pro který je

$$x = \sum_{v \in M} a_v v .$$

Soubor souřadnic vektoru x vzhledem k bázi M značíme symbolem $\langle x \rangle_M$, tj. $\langle x \rangle_M = \{a_v\}_{v \in M}$.

Soubor souřadnic $\{a_v\}_{v \in M}$ je indexován prvky báze M . Pokud je báze M konečná, pak vektory báze zpravidla číslujeme a stejnými indexy číslujeme i příslušné souřadnice. Je-li $M = \{v_1, \dots, v_n\}$ a $x = \sum_{i=1}^n a_i v_i$, píšeme $\langle x \rangle_M = (a_1, \dots, a_n)$ a hovoříme o první až n -té souřadnici vektoru x . Obdobně postupujeme i v případě, kdy je báze M nekonečná. Je-li $M = \{v_\alpha\}_{\alpha \in \Lambda}$ a

$$x = \sum_{\alpha \in \Lambda} a_\alpha v_\alpha ,$$

píšeme $\langle x \rangle_M = \{a_\alpha\}_{\alpha \in \Lambda}$.

Jestliže je $M = \{v_1, \dots, v_n\}$, pak přiřazení souřadnic (a_1, \dots, a_n) vektoru $x \in V$ je vzájemně jednoznačné zobrazení prostoru V na prostor T^n . V obecném případě, tj. ať je báze M jakákoliv, je přiřazení souřadnic $\{a_v\}_{v \in M}$ vektoru $x \in V$ vzájemně jednoznačné zobrazení prostoru V na prostor $K(T^M)$ (viz příklad 7.8(ix)). Hledat souřadnice vektoru vzhledem k různým bázím a stanovit jejich vztah se naučíme později.

Pro další rozvinutí teorie (zavedení pojmu dimenze vektorového prostoru) budeme potřebovat následující lemma.

Tvrzení (ii) vyplývá ihned z tvrzení (i). Předpokládejme, že vektory v_1, \dots, v_n prostoru V jsou lineárně nezávislé a že prostor V má m -prvkovou množinu generátorů, kde $m < n$. Potom jsou lineárně nezávislé vektory v_1, \dots, v_{m+1} lineárními kombinacemi m vektorů prostoru V a to je spor s tvrzením (i). \square

Z lemmatu 8.15 bezprostředně vyplývá, že každé dvě báze konečně generovaného prostoru mají stejný počet prvků (viz dále). Obdobné tvrzení však platí i pro nekonečně generované prostory; při důkazu tohoto tvrzení je však nutno užít základní fakta o počítání s kardinálními čísly. Tvrzení o invariantnosti počtu prvků, resp. mohutnosti báze tedy může být zformulováno zcela obecně.

8.16. Věta. *Každé dvě báze vektorového prostoru mají stejnou mohutnost.*

Důkaz. Předpokládejme, že V je konečně generovaný vektorový prostor nad tělesem T . Nechť M, N jsou dvě báze prostoru V , které mají po řadě m, n prvků. Podle tvrzení (ii) lemmatu 8.15 nemůže být ani $m < n$, ani $n < m$. Báze M a N tedy mají stejný počet prvků.

Poznamenejme ještě pro úplnost, že v konečně generovaném prostoru V konečná báze existuje podle věty 8.11, resp. 8.12; z tvrzení (ii) lemmatu 8.15 rovněž vyplývá, že konečně generovaný prostor nemůže mít žádnou nekonečnou bázi.

Předpokládejme, že prostor V není konečně generovaný; nechť M, N jsou dvě jeho báze. Každý vektor $v \in M$ je lineární kombinací vektorů konečné podmnožiny N_v báze N . Protože je M množinou generátorů prostoru V , je i množina $\bigcup_{v \in M} N_v$ množinou generátorů prostoru V . Protože je N báze prostoru V , je $N = \bigcup_{v \in M} N_v$ (viz důsledek 8.4). Nyní je

$$|N| \leq \sum_{v \in M} |N_v| \leq \aleph_0 \cdot |M| = |M| .$$

Obdobným způsobem dokážeme nerovnost $|M| \leq |N|$; můžeme se však též odvolat na symetrii situace. Báze M a N tedy mají stejnou mohutnost. \square

8.17. Poznámka. První část důkazu věty 8.16 se často provádí podle tzv. **Steinitzovy věty o výměně**:

Jestliže M je m -prvková množina generátorů prostoru V a N n -prvková lineárně nezávislá podmnožina prostoru V , pak existuje n -prvková podmnožina M' množiny M taková, že $(M \setminus M') \cup N$ generuje prostor V .

Nějakých n vektorů množiny M se tedy „zamění“ za n -prvkovou množinu N a vlastnost generovat prostor V se přitom zachová.

Steinitzova věta o výměně však obrací pozornost nežádoucím směrem, totiž na „výměnu“ podmnožiny M' za množinu N . Za touto výměnou je skryta důležitá nerovnost $n \leq m$ (srovnej s tvrzením (ii) lemmatu 8.15), ze které vyplývá rovnost počtu prvků dvou bází konečně generovaného prostoru.

Důkaz Steinitzovy věty se provádí indukcí. Pro $n = 0$ není co dokazovat.

Předpokládejme, že tvrzení platí pro $n - 1$. Nechť $N = \{y_1, \dots, y_n\}$. Podle indukčního předpokladu existuje taková $(n - 1)$ -prvková podmnožina K množiny M , že množina $M_1 = (M \setminus K) \cup \{y_1, \dots, y_{n-1}\}$ generuje prostor V . Vektor y_n je proto lineární kombinací vektorů této množiny; protože je množina N lineárně nezávislá, musí být v této lineární kombinaci alespoň u jednoho vektoru u z množiny $M \setminus K$ nenulový koeficient. Tento vektor u jde potom vyjádřit jako lineární kombinace vektorů množiny $M_2 = (M \setminus K \cup \{u\}) \cup N$. Protože je každý vektor prostoru V lineární kombinací vektorů množiny M_1 , je též lineární kombinací vektorů množiny M_2 (do lineární kombinace vektorů množiny M_1 dosadíme za vektor u).

Věta 8.16 říká, že každé dvě báze konečně generovaného prostoru mají stejný počet prvků a že každé dvě báze nekonečně generovaného prostoru mají stejnou mohutnost. Na základě tohoto zjištění můžeme zavést pojem dimenze vektorového prostoru.

8.18. Definice. *Dimenzí* $\dim V$ vektorového prostoru V budeme rozumět mohutnost jeho libovolné báze.

Vektorový prostor dimenze n budeme též nazývat *n -dimenzionálním prostorem*. Viděli jsme, že v takovémto prostoru existuje n lineárně nezávislých vektorů a že každá podmnožina prostoru V , která má více než n prvků, je lineárně závislá. Poznamenejme ještě, že každých n lineárně nezávislých vektorů n -dimenzionálního prostoru tvoří bázi tohoto prostoru.

Dimenzí lineární množiny (viz 7.20) často rozumíme dimenzi podprostoru, který ji určuje, tj. $\dim(u + W) = \dim W$.

8.19. Příklady.

- (i) Triviální prostor má dimenzi 0.
- (ii) Dimenze tělesa T jako vektorového prostoru nad T je 1.
- (iii) Dimenze prostoru všech vázaných vektorů v rovině (resp. prostoru), které mají společný počátek v pevně zvoleném bodě, je 2 (resp. 3).
- (iv) Dimenze reálného vektorového prostoru všech komplexních čísel (tj. \mathbb{C} nad \mathbb{R}) je 2.
- (v) Dimenze prostoru T^n je n . Uvědomme si, že je-li těleso T konečné, je i prostor T^n konečný; např. prostor \mathbb{Z}_5^4 má $5^4 = 625$ prvků. Prostor \mathbb{R}^n se často nazývá *n -dimenzionální aritmetický prostor*.
- (vi) Dimenze prostoru $T^{n \times m}$ všech matic typu $n \times m$ nad tělesem T je nm . Je-li těleso T konečné, je i prostor $T^{n \times m}$ konečný.

Prostor $T^{n \times n}$ všech čtvercových matic řádu n má tedy dimenzi n^2 . V prostoru $T^{n \times n}$ jsme uvažovali řadu podprostorů. Podprostor všech skalárních matic má dimenzi 1, podprostor všech diagonálních matic dimenzi n , podprostor všech horních (dolních) trojúhelníkových matic dimenzi $\frac{1}{2}n(n + 1)$, stejnou dimenzi má podprostor všech symetrických matic. Pokud není charakteristika tělesa T rovna 2, má

podprostor všech antisymetrických matic dimenzi $\frac{1}{2}n(n-1)$; je-li $\text{char } T = 2$, pak dimenze podprostoru všech antisymetrických matic je $\frac{1}{2}n(n+1)$.

(vii) Dimenze prostoru $K(T^{\mathbb{N}})$ všech nekonečných posloupností prvků tělesa T , které mají jen konečně mnoho nenulových členů, je \aleph_0 .

(viii) Dimenze prostoru $T[x]$ všech polynomů s koeficienty z tělesa T je \aleph_0 . Dimenze podprostoru tvořeného všemi polynomy stupně nejvýše n je $n+1$.

(ix) Dimenze prostoru všech reálných funkcí definovaných na intervalu (a, b) je nespočetná. Nespočetná je rovněž dimenze podprostoru všech funkcí, které mají konečný nosič (viz příklad 8.10(ix)).

(x) Na množině \mathbb{R}^+ všech kladných reálných čísel definujme binární operaci "⊕" rovností

$$u \oplus v = u \cdot v$$

a násobení "⊖" prvků množiny \mathbb{R}^+ reálnými čísly rovností

$$a \ominus u = u^a .$$

Množina \mathbb{R}^+ je s těmito operacemi reálným vektorovým prostorem. Nulovým vektorem tohoto prostoru je číslo 1, bázi je každá jednoprvková množina $\{u\}$, kde $1 \neq u \in \mathbb{R}^+$, $\dim \mathbb{R}^+ = 1$.

Dimenzi lineárního obalu konečně mnoha vektorů zjišťujeme pomocí tvrzení 7.14(viii). Množinu generátorů postupně přetváříme, až získáme bázi uvažovaného lineárního obalu.

8.20. Příklad. Uvažujme podprostor

$$W = [(3, 4, 1, 2), (2, 0, 1, 2), (1, 3, 2, 4), (4, 0, 2, 4)]$$

vektorového prostoru \mathbb{Z}_5^4 . Přičteme-li první vektor ke druhému, trojnásobek prvního ke třetímu a dvojnásobek ke čtvrtému, získáme podle 7.14(viii) rovnost

$$W = [(3, 4, 1, 2), (0, 4, 2, 4), (0, 0, 0, 0), (0, 3, 4, 3)] .$$

Nyní přičteme trojnásobek druhého vektoru ke čtvrtému:

$$W = [(3, 4, 1, 2), (0, 4, 2, 4), (0, 0, 0, 0), (0, 0, 0, 0)] = [(3, 4, 1, 2), (0, 4, 2, 4)]$$

Tedy $\dim W = 2$.

8.21. Věta. *Necht V je vektorový prostor nad tělesem T . Potom platí:*

- (i) *Je-li M lineárně nezávislá podmnožina prostoru V , je $|M| \leq \dim V$.*
- (ii) *Je-li W podprostor prostoru V , je $\dim W \leq \dim V$.*

Důkaz. Každou lineárně nezávislou podmnožinu M prostoru V (resp. bázi M podprostoru W) můžeme rozšířit na bázi prostoru V (viz 8.11); odtud vyplývají obě tvrzení. \square

8.22. Věta. *Pro vektorový prostor V nad tělesem T jsou následující tvrzení ekvivalentní:*

- (i) *Prostor V má konečnou dimenzi.*
- (ii) *Pro každý vlastní podprostor W prostoru V je $\dim W < \dim V$.*

Důkaz. Předpokládejme, že má prostor V konečnou dimenzi a že W je jeho vlastní podprostor. Jestliže nějakou bázi $\{w_1, \dots, w_m\}$ podprostoru W rozšíříme na bázi prostoru V , pak k vektorům w_1, \dots, w_m nutně přibude alespoň jeden vektor (viz např. důkaz věty 8.11). Tedy $\dim W < \dim V$.

Předpokládejme, že má prostor V nekonečnou dimenzi. Jestliže z nějaké báze prostoru V vynecháme jeden vektor, dostaneme bázi vlastního podprostoru W , která má stejnou mohutnost jako báze prostoru V , takže $\dim W = \dim V$. \square

8.23. Příklad. Uvažujme prostor $\mathbb{R}[x]$ všech polynomů jedné neurčité s reálnými koeficienty; tento prostor má dimenzi \aleph_0 . Následující podprostory tohoto prostoru jsou vlastní a mají zřejmě stejnou dimenzi jako prostor $\mathbb{R}[x]$:

- podprostor všech polynomů, které nemají absolutní člen; jeho bázi je množina $\{x, x^2, x^3, \dots\}$,
- podprostor všech polynomů, které nemají lineární člen; jeho bázi je množina $\{1, x^2, x^3, \dots\}$,
- podprostor všech polynomů, které nemají členy s mocninami menšími než 10; jeho bázi je množina $\{x^{10}, x^{11}, x^{12}, \dots\}$,
- podprostor všech polynomů, které mají jen členy se sudými mocninami neurčité x ; jeho bázi je množina $\{1, x^2, x^4, \dots\}$ atd.

8.24. Věta o dimenzích spojení a průniku. *Nechť U, V jsou podprostory nějakého vektorového prostoru nad tělesem T . Potom je*

$$\dim(U + V) + \dim(U \cap V) = \dim U + \dim V .$$

Důkaz. Budeme předpokládat, že oba podprostory U, V jsou konečně generované. V obecném případě sice tvrzení věty také platí (a dokáže se obdobně), ale věta nemá praktický význam; ze tří dimenzí uvedených v rovnosti nelze vždy určit čtvrtou.

Nechť $\{w_1, \dots, w_k\}$ je báze podprostoru $U \cap V$. Tuto bázi rozšíříme (viz 8.11) jednak na bázi

$$A = \{w_1, \dots, w_k, u_1, \dots, u_n\}$$

prostoru U a jednak na bázi

$$B = \{w_1, \dots, w_k, v_1, \dots, v_m\}$$

prostoru V . Je tedy $\dim U \cap V = k$, $\dim U = k + n$ a $\dim V = k + m$.

Nyní dokážeme, že množina

$$C = \{w_1, \dots, w_k, u_1, \dots, u_n, v_1, \dots, v_m\}$$

je bázi podprostoru $U + V$. Víme, že každý vektor podprostoru $U + V$ je možno vyjádřit v tvaru $x + y$, kde $x \in U$ a $y \in V$. Zřejmě $x \in [A]$, $y \in [B]$ a tedy $x + y \in [C]$. Množina C proto generuje podprostor $U + V$.

Jestliže je

$$o = \sum_{r=1}^k a_r w_r + \sum_{i=1}^n b_i u_i + \sum_{j=1}^m c_j v_j ,$$

je též

$$\sum_{r=1}^k a_r w_r + \sum_{i=1}^n b_i u_i = - \sum_{j=1}^m c_j v_j . \quad (3)$$

Tento vektor leží v podprostoru U (viz levá strana rovnosti) i v podprostoru V (viz pravá strana rovnosti), takže leží v jejich průniku. Je ho tedy možno vyjádřit jako lineární kombinaci vektorů w_1, \dots, w_k , tj.

$$- \sum_{j=1}^m c_j v_j = \sum_{s=1}^k d_s w_s \quad \text{a odtud} \quad \sum_{j=1}^m c_j v_j + \sum_{s=1}^k d_s w_s = o .$$

Vzhledem k tomu, že je množina B lineárně nezávislá, jsou všechny koeficienty d_1, \dots, d_k a c_1, \dots, c_m rovny nule. Z rovnosti (3) dostáváme rovnost

$$\sum_{r=1}^k a_r w_r + \sum_{i=1}^n b_i u_i = o ;$$

z lineární nezávislosti množiny A vyplývá, že všechny koeficienty a_1, \dots, a_k a všechny koeficienty b_1, \dots, b_n jsou rovny nule. Množina C je tedy lineárně nezávislá, tj. je bázi podprostoru $U + V$. Proto je $\dim(U + V) = n + m + k$; tvrzení věty jsme dokázali. \square

8.25. Příklad. Uvažujme podprostory

$$V_1 = [(-3, 0, 2, 0)] , \quad V_2 = [(1, 0, 2, -3), (3, 2, 1, -5), (-1, 2, 1, -2)]$$

vektorového prostoru \mathbb{R}^4 . Zřejmě je $\dim V_1 = 1$. Množinu generátorů podprostoru V_2 upravíme podobně jako v příkladu 8.20:

$$V_2 = [(1, 0, 2, -3), (0, 2, -5, 4), (0, 2, 3, -5)] ,$$

$$V_2 = [(1, 0, 2, -3), (0, 2, -5, 4), (0, 0, 8, -9)] .$$

Je tedy $\dim V_2 = 3$. Součet $V_1 + V_2$ je generován sjednocením množin generátorů podprostorů V_1 a V_2 . Tuto množinu generátorů nyní upravíme:

$$V_1 + V_2 = [(1, 0, 2, -3), (0, 2, -5, 4), (0, 0, 8, -9), (-3, 0, 2, 0)] ,$$

$$V_1 + V_2 = [(1, 0, 2, -3), (0, 2, -5, 4), (0, 0, 8, -9), (0, 0, 8, -9)] ,$$

$$V_1 + V_2 = [(1, 0, 2, -3), (0, 2, -5, 4), (0, 0, 8, -9)] .$$

Je tedy $\dim(V_1 + V_2) = 3$ a

$$\dim(V_1 \cap V_2) = \dim V_1 + \dim V_2 - \dim(V_1 + V_2) = 1 + 3 - 3 = 1 .$$

Podprostor V_1 je obsažen v podprostoru V_2 .

S následující větou se setkáváme v algebře při studiu rozšíření těles.

8.26. Věta o stupních. *Nechť T_1 je podtěleso tělesa T_2 a T_2 podtěleso tělesa T_3 . Jestliže m je dimenze tělesa T_2 jako vektorového prostoru nad tělesem T_1 a n dimenze tělesa T_3 jako vektorového prostoru nad tělesem T_2 , potom je mn dimenze tělesa T_3 jako vektorového prostoru nad tělesem T_1 .*

Důkaz. Nechť $\{v_1, \dots, v_m\}$ je báze prostoru T_2 nad tělesem T_1 a $\{w_1, \dots, w_n\}$ báze prostoru T_3 nad tělesem T_2 . Dokážeme, že bázi prostoru T_3 nad tělesem T_1 je množina

$$M = \{v_i w_j ; i = 1, \dots, m, j = 1, \dots, n\} .$$

Každý vektor $w \in T_3$ se dá vyjádřit v tvaru

$$w = \sum_{j=1}^n a_j w_j , \quad \text{kde } a_1, \dots, a_n \in T_2 .$$

Koeficienty a_1, \dots, a_n se však dají vyjádřit jako lineární kombinace vektorů báze prostoru T_2 , tj. pro každé $j = 1, \dots, n$ je

$$a_j = \sum_{i=1}^m b_{ij} v_i , \quad \text{kde } b_{ij} \in T_1 \quad \text{pro } i = 1, \dots, m, j = 1, \dots, n .$$

Nyní je

$$w = \sum_{j=1}^n \sum_{i=1}^m b_{ij} v_i w_j ,$$

takže množina M generuje prostor T_3 nad tělesem T_1 .

Předpokládejme nyní, že je

$$\sum_{j=1}^n \sum_{i=1}^m b_{ij} v_i w_j = 0 .$$

Protože je $\{w_1, \dots, w_n\}$ báze prostoru T_3 nad tělesem T_2 , je pro každé $j = 1, \dots, n$

$$\sum_{i=1}^m b_{ij} v_i = 0 .$$

Protože je $\{v_1, \dots, v_m\}$ báze prostoru T_2 nad tělesem T_1 , je $b_{ij} = 0$ pro každé $j = 1, \dots, n$ a $i = 1, \dots, m$. Množina M je tedy lineárně nezávislá a je proto bází prostoru T_3 nad tělesem T_1 . \square

Obsahuje-li těleso T_2 těleso T_1 , hovoříme o *rozšíření* $T_1 \subseteq T_2$. *Stupněm* tohoto rozšíření rozumíme dimenzi tělesa T_2 jako vektorového prostoru nad tělesem T_1 . Věta o stupních tedy říká, že stupeň rozšíření $T_1 \subseteq T_3$ je roven součinu stupňů rozšíření $T_1 \subseteq T_2$ a $T_2 \subseteq T_3$. Z věty o stupních vyplývá např. následující tvrzení:

Jestliže je stupeň rozšíření $T_1 \subseteq T_2$ roven prvočíslu, pak neexistuje vlastní podtěleso tělesa T_2 , které by obsahovalo T_1 jako vlastní podtěleso (tj. neexistuje „meztěleso“).

Protože je dimenze reálného vektorového prostoru \mathbb{C} rovna 2, neexistuje vlastní podtěleso tělesa komplexních čísel, které by obsahovalo jako vlastní podtěleso těleso reálných čísel.

9. DIREKTNÍ SOUČET

9.1. Definice. Nechť V je vektorový prostor nad tělesem T a V_1, V_2 jeho dva podprostory. Řekneme, že prostor V je *direktním součtem* podprostorů V_1 a V_2 , jestliže

- (i) $V = V_1 + V_2$,
- (ii) $V_1 \cap V_2 = O$;

tuto skutečnost vyjadřujeme zápisem $V = V_1 \oplus V_2$. Často též hovoříme o *direktním rozkladu* prostoru V . Podprostory V_1, V_2 jsou *direktními sčítanci* prostoru V , podprostor V_1 je *direktním doplňkem* podprostoru V_2 v prostoru V (a podprostor V_2 je direktním doplňkem podprostoru V_1 v prostoru V).

9.2. Věta. *Vektorový prostor V je direktním součtem podprostorů V_1 a V_2 právě tehdy, když každý vektor $v \in V$ je možno právě jediným způsobem vyjádřit v tvaru $v = v_1 + v_2$, kde $v_1 \in V_1$ a $v_2 \in V_2$.*

Důkaz. Předpokládejme, že $V = V_1 \oplus V_2$. Protože $V = V_1 + V_2$, existují ke každému vektoru $v \in V$ vektory $v_1 \in V_1$ a $v_2 \in V_2$, pro které $v = v_1 + v_2$. Jestliže je ještě $v = v'_1 + v'_2$, kde $v'_1 \in V_1$ a $v'_2 \in V_2$, potom je $v_1 + v_2 = v'_1 + v'_2$ a vektor $v_1 - v'_1 = v'_2 - v_2$ leží v průniku $V_1 \cap V_2$. Tento průnik je však podle předpokladu triviální, takže $v_1 - v'_1 = o, v'_2 - v_2 = o$, tj. $v_1 = v'_1$ a $v_2 = v'_2$.

Předpokládejme naopak, že každý vektor $v \in V$ je možno právě jediným způsobem vyjádřit v tvaru $v = v_1 + v_2$, kde $v_1 \in V_1$ a $v_2 \in V_2$. Zřejmě je tedy $V = V_1 + V_2$. Jestliže $v \in V_1 \cap V_2$, potom můžeme psát $v = v + o = o + v$. Z předpokladu jednoznačnosti vyjádření vektoru v vyplývá rovnost $v = o$. \square

9.3. Příklady.

(i) Nechť V je vektorový prostor všech vázaných vektorů v rovině, jejichž počátky jsou v pevně zvoleném bodě S . Uvažujme dvě různé přímky p, q , které bodem S procházejí. Tyto přímky určují podprostory V_1, V_2 všech vektorů prostoru V , které na přímkách p, q leží. Prostor V je direktním součtem podprostorů V_1 a V_2 . Poznamenejme, že přímky p, q nemusí být na sebe kolmé.

Podobný příklad dostaneme, budeme-li uvažovat vektorový prostor V vázaných vektorů v prostoru se společným počátkem v pevně daném bodě S a podprostory V_1, V_2 určené rovinou ϱ a přímkou p , které procházejí bodem S ; přímka p však nesmí ležet v rovině ϱ .

V obou příkladech je zřejmé, že každý vektor $v \in V$ je možno právě jediným způsobem zapsat v tvaru $v = v_1 + v_2$, kde $v_1 \in V_1, v_2 \in V_2$ (viz věta 9.2), tj. $V = V_1 \oplus V_2$.

(ii) Uvažujme vektorový prostor $T^{n \times n}$ čtvercových matic řádu n nad tělesem T a předpokládejme, že $\text{char } T \neq 2$. Potom je prostor $T^{n \times n}$ direktním součtem svých podprostorů symetrických a antisymetrických matic:

$$T^{n \times n} = \mathbb{S}(T^{n \times n}) \oplus \mathbb{A}(T^{n \times n})$$

Jestliže je matice $A = (a_{ij})$ současně symetrická i antisymetrická, pak pro každé $i, j = 1, \dots, n$ je $a_{ij} = a_{ji}$ a $a_{ij} = -a_{ji}$ a tedy $2a_{ij} = 0$. Protože je $\text{char } T \neq 2$, je $a_{ij} = 0$ pro každé $i, j = 1, \dots, n$. Průnik podprostorů symetrických a antisymetrických matic je tedy nulový.

Na druhé straně je možno každou matici $A = (a_{ij})$ napsat jako součet symetrické a antisymetrické matice. Pro každé $i, j = 1, \dots, n$ položme

$$b_{ij} = \frac{1}{2}(a_{ij} + a_{ji}), \quad c_{ij} = \frac{1}{2}(a_{ij} - a_{ji})$$

(zde jsme opět využili předpokladu $\text{char } T \neq 2$ — prvek $\frac{1}{2}$ je inverzním prvkem k nenulovému prvku $1 + 1 = 2$). Matice $B = (b_{ij})$ je zřejmě symetrická, matice $C = (c_{ij})$ antisymetrická a je $A = B + C$. Tomuto rozkladu matice A někdy říkáme *rozklad na symetrickou a antisymetrickou část*.

Pro matice nad tělesem charakteristiky 2 uvedené tvrzení neplatí, neboť např. matice

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

nad tělesem \mathbb{Z}_2 je symetrická i antisymetrická.

Z věty o dimenzích spojení a průniku dvou podprostorů bezprostředně vyplývá následující výsledek.

9.4. Věta. *Jestliže je vektorový prostor V direktním součtem svých podprostorů V_1 a V_2 , pak je $\dim V = \dim V_1 + \dim V_2$. \square*

Direktním sčítancem prostoru V je podle definice 9.1 takový podprostor V_1 prostoru V , ke kterému existuje direktní doplněk, tj. podprostor V_2 prostoru V , pro který je $V = V_1 \oplus V_2$. Pojem direktního sčítance není v teorii vektorových prostorů důležitý (jako v jiných algebraických teoriích), jak vyplývá z následující věty.

9.5. Věta. *Každý podprostor vektorového prostoru je jeho direktním sčítancem.*

Důkaz. Nechť V_1 je podprostor vektorového prostoru V . Zvolme bázi M tohoto podprostoru a rozšířme ji na bázi N prostoru V . Podprostor V_2 generovaný množinou $N \setminus M$ je direktním doplňkem podprostoru V_1 v prostoru V . Ze základní vlastnosti báze (viz 8.13) totiž vyplývá, že každý vektor $v \in V$ je možno jediným způsobem zapsat v tvaru $v = v_1 + v_2$, kde $v_1 \in V_1$ a $v_2 \in V_2$. \square

9.6. Poznámka. V předchozích odstavcích jsme se zabývali situací, kdy vektorový prostor byl direktním součtem svých podprostorů. Pomocí direktního součtu však můžeme z daných vektorových prostorů též konstruovat vektorové prostory nové.

Nechť W_1 a W_2 jsou vektorové prostory nad tělesem T . Na kartézském součinu $V = W_1 \times W_2$ definujeme binární operaci sčítání a operaci násobení skalárem „po složkách“: jestliže $w_1, w'_1 \in W_1$, $w_2, w'_2 \in W_2$ a $a \in T$, pak

$$(w_1, w_2) + (w'_1, w'_2) = (w_1 + w'_1, w_2 + w'_2) ,$$

$$a \cdot (w_1, w_2) = (aw_1, aw_2) .$$

Uvědomme si, že operace sčítání dvojic a násobení dvojice skalárem jsou definovány pomocí operací definovaných v prostorech W_1 a W_2 . Snadno se ověří, že s operacemi právě definovanými je množina V vektorovým prostorem; všech osm axiomů z definice vektorového prostoru je splněno, např. nulovým vektorem v prostoru V je dvojice (o, o) složená z nulových vektorů prostorů W_1 a W_2 . Právě vytvořený vektorový prostor V se nazývá *vnější direktní součet* prostorů W_1 a W_2 . Tento prostor je však ve smyslu definice 9.1 direktním součtem svých podprostorů

$$V_1 = \{ (w_1, o) ; w_1 \in W_1 \} , \quad V_2 = \{ (o, w_2) ; w_2 \in W_2 \} ,$$

kteří se jen „nepodstatně liší“ od prostorů W_1, W_2 (později budeme říkat, že jsou *izomorfní*). Z tohoto důvodu budeme pro vnější direktní součet užívat stejného symbolu jako pro „vnitřní“ direktní součet zavedený v 9.1, tj. budeme psát

$$V = W_1 \oplus W_2 .$$

Ze stejného důvodu nebudeme mnohdy zdůrazňovat, zda jde o vnější nebo vnitřní direktní součet a budeme hovořit jen o direktním součtu.

Definici 9.1, ve které je zaveden pojem direktního součtu dvou podprostorů, nyní zobecníme a zavedeme direktní součet libovolného souboru podprostorů. Zobecníme i větu 9.2, která charakterizuje direktní součet ekvivalentní podmínkou. Zavedení pojmu direktního součtu souboru podprostorů dává nový pohled na strukturu vektorových prostorů (viz věta 9.9 a příklady 9.12).

9.7. Definice. Nechť V je vektorovým prostorem nad tělesem T a V_α , $\alpha \in \Lambda$, necht' jsou jeho podprostory. Řekneme, že vektorový prostor V je *direktním součtem* podprostorů V_α , $\alpha \in \Lambda$, jestliže

- (i) $V = \sum_{\alpha \in \Lambda} V_\alpha$,
- (ii) $\forall \beta \in \Lambda \quad V_\beta \cap \sum_{\substack{\alpha \in \Lambda \\ \alpha \neq \beta}} V_\alpha = O$;

tento fakt zapíšeme symbolicky v tvaru $V = \bigoplus_{\alpha \in \Lambda} V_\alpha$.

Z druhé vlastnosti zjevně vyplývá, že $V_\alpha \cap V_\beta = O$ pro každé $\alpha, \beta \in \Lambda$, $\alpha \neq \beta$.

9.8. Věta. *Vektorový prostor V je direktním součtem podprostorů V_α , $\alpha \in \Lambda$, právě tehdy, když každý vektor $v \in V$ je možno právě jediným způsobem vyjádřit v tvaru*

$$v = \sum_{\alpha \in \Lambda} v_\alpha ,$$

kde pro každé $\alpha \in \Lambda$ je $v_\alpha \in V_\alpha$ a pro skoro všechna $\alpha \in \Lambda$ je $v_\alpha = o$.

Důkaz. Nechť je prostor V direktním součtem podprostorů V_α , $\alpha \in \Lambda$. Podle první vlastnosti direktního součtu je každý vektor $v \in V$ možno vyjádřit v uvedeném tvaru. Jestliže

$$v = \sum_{\alpha \in \Lambda} v_\alpha = \sum_{\alpha \in \Lambda} v'_\alpha$$

jsou dvě vyjádření vektoru v uvažovaného typu (tj. pro každé $\alpha \in \Lambda$ je $v_\alpha, v'_\alpha \in V_\alpha$, pro skoro všechna $\alpha \in \Lambda$ je $v_\alpha = o$ a pro skoro všechna $\alpha \in \Lambda$ je $v'_\alpha = o$), potom je pro každé $\beta \in \Lambda$

$$v_\beta - v'_\beta = \sum_{\substack{\alpha \in \Lambda \\ \alpha \neq \beta}} (v'_\alpha - v_\alpha) \in V_\beta \cap \sum_{\substack{\alpha \in \Lambda \\ \alpha \neq \beta}} V_\alpha .$$

Z druhé vlastnosti direktního součtu vyplývá, že $v_\beta = v'_\beta$; tím je dokázána jednoznačnost uvažovaného vyjádření vektoru v .

Nechť je naopak každý vektor $v \in V$ možno vyjádřit jediným způsobem v uvažovaném tvaru. Prostor V je tedy součtem svých podprostorů V_α , $\alpha \in \Lambda$. Předpokládejme, že pro nějaké $\beta \in \Lambda$ je

$$o \neq v \in V_\beta \cap \sum_{\substack{\alpha \in \Lambda \\ \alpha \neq \beta}} V_\alpha .$$

Vektor v má však nyní dvě různá vyjádření,

$$v \in V_\beta \quad \text{a} \quad v = \sum_{\substack{\alpha \in \Lambda \\ \alpha \neq \beta}} v_\alpha \in \sum_{\substack{\alpha \in \Lambda \\ \alpha \neq \beta}} V_\alpha ,$$

a to je spor, který jsme potřebovali. \square

Důkaz předchozí věty probíhá stejně jako důkaz věty 9.2; je z něj dobře vidět, že podmínka (ii) z definice 9.7 odpovídá podmínce (ii) z definice 9.1.

Následující věta dává nový pohled na bázi vektorového prostoru.

9.9. Věta. *Nechť V je vektorový prostor nad tělesem T a necht' M je podmnožina prostoru V . Množina M je bázi prostoru V právě tehdy, když je*

$$V = \bigoplus_{v \in M} [v] .$$

Důkaz. Podle věty 8.13 je M bází prostoru V právě tehdy, když každý vektor $x \in V$ je možno právě jediným způsobem vyjádřit v tvaru $x = \sum_{v \in M} a_v v$, kde pro skoro všechny vektory $v \in M$ je $a_v = 0$. Podle předchozí věty je to však ekvivalentní s tím, že prostor V je direktním součtem podprostorů $[v]$, $v \in M$. \square

Získali jsme tedy nový pohled na vektorové prostory: každý vektorový prostor V je direktním součtem svých podprostorů dimenze 1; jejich počet (resp. mohutnost indexové množiny) je roven dimenzi prostoru V . Každý vektorový prostor dimenze δ je tedy direktním součtem δ jednodimenzionálních prostorů.

9.10. Věta. *Jestliže je vektorový prostor V direktním součtem svých podprostorů V_α , $\alpha \in \Lambda$, potom je*

$$\dim V = \sum_{\alpha \in \Lambda} \dim V_\alpha .$$

Důkaz. Pro každé $\alpha \in \Lambda$ nechť M_α je nějaká báze podprostoru V_α . Ukážeme, že sjednocení M těchto bází je báze prostoru V .

Protože každá množina M_α generuje prostor V_α a sjednocení všech podprostorů V_α generuje prostor V , je množina M množinou generátorů prostoru V . Každou lineární kombinaci vektorů množiny M můžeme vyjádřit jako součet $v_1 + \dots + v_k$, kde v_1, \dots, v_k jsou lineární kombinace vektorů z jednotlivých množin M_{α_i} , kde indexy $\alpha_1, \dots, \alpha_k$ jsou navzájem různé. Jestliže je nyní

$$v_1 + v_2 + \dots + v_k = o ,$$

je

$$v_k = -v_1 - v_2 - \dots - v_{k-1} \in V_{\alpha_k} \cap \sum_{\substack{\alpha \in \Lambda \\ \alpha \neq \alpha_k}} V_\alpha .$$

Podle druhé vlastnosti direktního součtu je $v_k = o$ a z lineární nezávislosti množiny M_{α_k} vyplývá, že lineární kombinace v_k je triviální. Stejně dokážeme, že i lineární kombinace v_1, \dots, v_{k-1} jsou triviální. Z této úvahy vyplývá, že i lineární kombinace $v_1 + \dots + v_k$ je triviální, tj. množina M je lineárně nezávislá a je proto bází prostoru V . Protože jsou množiny M_α po dvou disjunktní (viz poznámka za definicí 9.7), je

$$\dim V = |M| = \sum_{\alpha \in \Lambda} |M_\alpha| = \sum_{\alpha \in \Lambda} \dim V_\alpha . \quad \square$$

9.11. Poznámka. Podobným způsobem, jakým jsme v 9.6 vytvořili vnější direktní součet dvou prostorů, budeme nyní definovat vnější direktní součet libovolného souboru vektorových prostorů. Nechť W_α , $\alpha \in \Lambda$, jsou vektorové prostory nad týmž tělesem T . Na kartézském součinu

$$W = \prod_{\alpha \in \Lambda} W_\alpha = \{ (w_\alpha)_{\alpha \in \Lambda} ; \forall \alpha \in \Lambda \quad w_\alpha \in W_\alpha \}$$

definujeme operaci sčítání a operaci násobení skalárem „po složkách“:

$$(w_\alpha)_{\alpha \in \Lambda} + (w'_\alpha)_{\alpha \in \Lambda} = (w_\alpha + w'_\alpha)_{\alpha \in \Lambda} ,$$

$$a \cdot (w_\alpha)_{\alpha \in \Lambda} = (aw_\alpha)_{\alpha \in \Lambda} .$$

Uvědomme si, že operace sčítání i operace násobení skalárem je definovaná pomocí operací sčítání a operací násobení skalárem v jednotlivých prostorech W_α , $\alpha \in \Lambda$. Snadno se ověří, že s právě definovanými operacemi je množina W vektorovým prostorem; všech osm axiomů definice vektorového prostoru je splněno, např. nulovým vektorem prostoru W je prvek $(o)_{\alpha \in \Lambda}$ — α -tá složka tohoto souboru je nulový vektor prostoru W_α . Takto definovaný vektorový prostor W se nazývá *produkt* souboru vektorových prostorů W_α , $\alpha \in \Lambda$.

Uvažujme nyní podmnožinu V prostoru W tvořenou všemi vektory, které mají jen konečně mnoho nenulových složek. Symbolicky je možno podmnožinu V definovat takto:

$$V = \{ (w_\alpha)_{\alpha \in \Lambda} \in W ; \exists \Lambda' \subseteq \Lambda, \Lambda' \text{ je konečná, } \forall \alpha \in \Lambda \setminus \Lambda' \quad w_\alpha = o \} .$$

Podmnožina V prostoru W je zřejmě uzavřena vzhledem k operaci sčítání i vzhledem k operaci násobení skalárem a je tedy podprostorem prostoru W . Vektorový prostor V se nazývá *vnější direktní součet* souboru prostorů W_α , $\alpha \in \Lambda$. Tento prostor je však ve smyslu definice 9.7 direktním součtem svých podprostorů V_α , $\alpha \in \Lambda$, které se jen „nepodstatně liší“ od původních prostorů W_α , $\alpha \in \Lambda$ (podprostor V_α je tvořen všemi soubory $(w_\beta)_{\beta \in \Lambda}$, pro které je $w_\beta = o$ pro každé $\beta \in \Lambda$, $\beta \neq \alpha$). Z tohoto důvodu budeme pro vnější direktní součet užívat stejného symbolu jako pro vnitřní direktní součet zavedený v 9.7, tj. budeme psát

$$V = \bigoplus_{\alpha \in \Lambda} W_\alpha .$$

Ze stejného důvodu nebudeme zdůrazňovat, zda jde o vnější nebo vnitřní direktní součet a budeme hovořit jen o direktním součtu.

Poznamenejme, že pro konečnou množinu Λ je zřejmě $V = W$, tj. direktní součet a produkt splývají. Je-li množina Λ dvouprvková, jde o direktní součet dvou prostorů popsany v 9.1, resp. 9.6.

9.12. Příklady. Vektorový prostor $T^{\mathbb{N}}$ z příkladu 7.8(vii) je produktem nekonečného spočetného souboru exemplářů tělesa T (jako vektorového prostoru nad tělesem T); jeho podprostor $K(T^{\mathbb{N}})$ je direktním součtem tohoto souboru. Můžeme psát

$$T^{\mathbb{N}} = \prod_{i=1}^{\infty} V_i , \quad K(T^{\mathbb{N}}) = \bigoplus_{i=1}^{\infty} V_i ,$$

kde pro každé $i = 1, 2, \dots$ je $V_i = T$.

Podobně můžeme psát

$$T^X = \prod_{x \in X} V_x, \quad K(T^X) = \bigoplus_{x \in X} V_x,$$

kde pro každé $x \in X$ je $V_x = T$.

Vektorový prostor T^n je direktním součtem n exemplářů tělesa T , tj.

$$T^n = \bigoplus_{i=1}^n V_i,$$

kde pro každé $i = 1, 2, \dots, n$ je $V_i = T$.

10. HOMOMORFISMY

10.1. Definice. Necht V a W jsou vektorové prostory nad tělesem T . Zobrazení f prostoru V do prostoru W se nazývá *homomorfismus*, jestliže platí:

- (i) $\forall x, y \in V \quad f(x + y) = f(x) + f(y)$,
- (ii) $\forall x \in V \quad \forall a \in T \quad f(ax) = a \cdot f(x)$.

Jestliže f je homomorfismus prostoru V do prostoru W , potom se množina

$$\text{Ker } f = \{v \in V; f(v) = o\}$$

nazývá *jádro* homomorfismu f a množina

$$\text{Im } f = \{w \in W; \exists v \in V \quad f(v) = w\}$$

se nazývá *obraz* homomorfismu f .

Symbolem $\text{Hom}(V, W)$ budeme značit množinu všech homomorfismů prostoru V do prostoru W .

Místo termínu homomorfismus se často užívá i termín *lineární zobrazení*. Místo symbolu $\text{Im } f$ se píše též $f(V)$, neboť $\text{Im } f$ je vlastně obrazem prostoru V při homomorfismu f (termíny *jádro* a *obraz* homomorfismu nejsou z jazykového hlediska ideální). Jádro $\text{Ker } f$ homomorfismu f je *úplným vzorem* nulového vektoru prostoru W .

Uvědomme si, že vlastnost „býti homomorfismem“ znamená záměnnost zobrazování se sčítáním vektorů a s násobením vektorů skaláry. Tuto skutečnost můžeme vyslovit také takto: Zobrazení f prostoru V do prostoru W je homomorfismem, právě když jsou splněny tyto dvě podmínky:

- (i) Jestliže libovolné dva vektory $x, y \in V$ sečteme a součet pak zobrazíme pomocí f , dospějeme k témuž výsledku, jako když vektory x, y nejprve zobrazíme pomocí f a získané obrazy sečteme.
- (ii) Jestliže libovolný vektor $x \in V$ vynásobíme skalárem $a \in T$ a získaný násobek zobrazíme pomocí f , dospějeme k témuž výsledku, jako když vektor x pomocí f zobrazíme a získaný obraz vynásobíme skalárem a .

10.2. Příklady.

- (i) Zobrazení f prostoru \mathbb{R}^2 do prostoru \mathbb{R}^3 , které vektoru $x = (x_1, x_2) \in \mathbb{R}^2$ přiřazuje vektor $f(x) = (2x_1 + x_2, x_1 - 3x_2, -2x_1 - x_2) \in \mathbb{R}^3$, je homomorfismus. Jestliže je totiž $y = (y_1, y_2) \in \mathbb{R}^2$ a $a \in \mathbb{R}$, potom je

$$x + y = (x_1 + y_1, x_2 + y_2), \quad ax = (ax_1, ax_2),$$

$$f(y) = (2y_1 + y_2, y_1 - 3y_2, -2y_1 - y_2),$$

$$f(x+y) = (2(x_1+y_1) + (x_2+y_2), (x_1+y_1) - 3(x_2+y_2), -2(x_1+y_1) - (x_2+y_2)) ,$$

$$f(ax) = (2ax_1 + ax_2, ax_1 - 3ax_2, -2ax_1 - ax_2) ,$$

takže $f(x+y) = f(x) + f(y)$ a $f(ax) = a \cdot f(x)$.

Jádro $\text{Ker } f$ homomorfismu f je tvořeno všemi vektory $x = (x_1, x_2) \in \mathbb{R}^2$, pro které je

$$\begin{aligned} 2x_1 + x_2 &= 0 , \\ x_1 - 3x_2 &= 0 , \\ -2x_1 - x_2 &= 0 , \end{aligned}$$

tj. všemi řešeními této soustavy rovnic. Snadno se vypočte, že $\text{Ker } f$ obsahuje jen nulový vektor.

Obraz $\text{Im } f$ homomorfismu f je tvořen všemi vektory $y = (y_1, y_2, y_3) \in \mathbb{R}^3$, pro které existuje vektor $x = (x_1, x_2) \in \mathbb{R}^2$ vyhovující rovnicím

$$\begin{aligned} 2x_1 + x_2 &= y_1 , \\ x_1 - 3x_2 &= y_2 , \\ -2x_1 - x_2 &= y_3 , \end{aligned}$$

tj. všemi vektory (y_1, y_2, y_3) , pro které je tato soustava rovnic řešitelná. Snadno se ukáže, že když je $y_3 = -y_1$, pak je možno ze zadaných čísel y_1, y_2 vypočítat neznámé x_1, x_2 . Tedy $\text{Im } f = \{(y_1, y_2, y_3); y_3 = -y_1\} = [(1, 0, -1), (0, 1, 0)]$.

(ii) Zobrazení prostoru \mathbb{R}^3 do prostoru \mathbb{R}^2 , která vektoru (x_1, x_2, x_3) přiřazují po řadě vektor $(0, 1)$, $(x_1 + 3x_2, x_3 - 2)$, $(x_1^2, x_2 + x_3^2)$, $(x_2 - \sqrt{x_3}, x_1)$, $(x_1 \cdot x_2, x_3)$, (x_1, e^{x_2}) nejsou homomorfismy.

(iii) Nechť V je vektorový prostor všech vázaných vektorů prostoru, které mají společný počátek v pevně zvoleném bodě S .

Nechť je dána přímka p , která prochází bodem S . Otočení prostoru V kolem přímky p o pevný úhel α přirozeným způsobem určuje homomorfismus prostoru V do prostoru V . Jádro tohoto homomorfismu je triviální, obrazem je celý prostor V .

Nechť je dána rovina ϱ , která prochází bodem S . Přiřadíme-li každému vektoru prostoru V jeho kolmou projekci na rovinu ϱ , dostaneme homomorfismus prostoru V do prostoru V . Jádrem je množina všech vektorů prostoru V , které jsou kolmé k rovině ϱ (leží na kolmé přímce k rovině ϱ procházející bodem S). Obrazem je rovina ϱ .

(iv) Nechť V je vektorový prostor všech funkcí, které jsou spojitě na uzavřeném intervalu $\langle 0, 1 \rangle$. Zobrazení, které každé funkci $v \in V$ přiřazuje funkci w ,

$$w(x) = \int_0^x v(t) dt , \quad x \in \langle 0, 1 \rangle ,$$

je homomorfismus prostoru V do prostoru V .

(v) Nechť V je vektorový prostor všech reálných funkcí definovaných na intervalu $(-\infty, \infty)$. Funkce v se nazývá *sudá*, resp. *lichá*, jestliže pro každé reálné číslo x platí $v(-x) = v(x)$, resp. $v(-x) = -v(x)$; tedy např. funkce \sin je lichá a funkce \cos je sudá. Snadno se ověří, že zobrazení f , které každé funkci $v \in V$ přiřazuje funkci w , $w(x) = \frac{1}{2}(v(x) + v(-x))$, je homomorfismus V do V a že $\text{Ker } f$ je množina všech lichých funkcí a $\text{Im } f$ je množina všech sudých funkcí. Zobrazení g , které každé funkci $v \in V$ přiřazuje funkci w , $w(x) = \frac{1}{2}(v(x) - v(-x))$, je rovněž homomorfismus V do V ; $\text{Ker } g$ je množina všech sudých funkcí a $\text{Im } g$ množina všech lichých funkcí.

10.3. Příklady.

(i) Nechť V a W jsou vektorové prostory. Zobrazení, které každému vektoru prostoru V přiřadí nulový vektor prostoru W , je homomorfismus. Nazývá se *nulový* a značí se obvykle symbolem 0 . Jeho jádrem je celý prostor V , jeho obrazem je nulový podprostor prostoru W .

(ii) Nechť U je podprostor prostoru V . Zobrazení, které každému vektoru $u \in U$ přiřadí též vektor u chápaný jako vektor prostoru V , je homomorfismus. Nazývá se *vnoření* podprostoru U do prostoru V . Jeho jádrem je nulový podprostor prostoru U a obrazem podprostor U prostoru V . Jestliže je podprostor U nulový, jde o nulový homomorfismus. Jestliže je $U = V$, dostáváme identické zobrazení prostoru V na prostor V ; v tomto případě hovoříme o tzv. *identickém automorfismu* prostoru V , který značíme 1_V (viz dále definice 10.9).

(iii) Nechť U je podprostor prostoru V . Zobrazení, které každému vektoru $v \in V$ přiřadí vektor $v + U$ faktorového prostoru V/U , je homomorfismus. Nazývá se *přirozený* (nebo též *kanonický*) homomorfismus prostoru V na faktorový prostor V/U . Jádrem tohoto homomorfismu je podprostor U , obrazem je prostor V/U . Jestliže je podprostor U nulový, dostáváme vlastně identický automorfismus prostoru V . Jestliže je $U = V$, dostáváme nulový homomorfismus prostoru V na nulový prostor.

V následující větě shrneme základní vlastnosti homomorfismů.

10.4. Věta. *Nechť f je homomorfismus prostoru V do prostoru W . Potom platí:*

- (i) *Homomorfismus f zobrazuje nulový vektor prostoru V na nulový vektor prostoru W .*
- (ii) *Homomorfismus f zobrazuje opačný vektor k vektoru $v \in V$ na opačný vektor k vektoru $f(v)$.*
- (iii) *Homomorfismus f zobrazuje lineární kombinaci vektorů prostoru V na stejnou lineární kombinaci obrazů těchto vektorů. Přesněji: je-li $v_1, \dots, v_k \in V$ a $a_1, \dots, a_k \in T$, potom*

$$f\left(\sum_{i=1}^k a_i v_i\right) = \sum_{i=1}^k a_i f(v_i) .$$

- (iv) *Obraz podprostoru prostoru V je podprostorem prostoru W .*
- (v) *$\text{Im } f$ je podprostorem prostoru W .*
- (vi) *Obraz množiny generátorů prostoru V je množinou generátorů prostoru $\text{Im } f$.*
- (vii) *Úplný vzor podprostoru prostoru W je podprostorem prostoru V .*
- (viii) *$\text{Ker } f$ je podprostorem prostoru V .*
- (ix) *Úplný vzor vektoru $w \in \text{Im } f$ je lineární množinou $v + \text{Ker } f$, kde $v \in V$ je libovolný vektor, pro který $f(v) = w$.*

Důkaz. Pro libovolně zvolený vektor $v \in V$ je

$$f(0) = f(0 \cdot v) = 0 \cdot f(v) = 0$$

a

$$f(-v) = f((-1) \cdot v) = (-1) \cdot f(v) = -f(v) ,$$

tj. tvrzení (i) a (ii) jsou dokázána.

Tvrzení (iii) se snadno dokáže z definice 10.1 pomocí matematické indukce.

Nechť V' je podprostor prostoru V . Zřejmě je $f(V')$ neprázdnou podmnožinou prostoru W , neboť podle tvrzení (i) obsahuje nulový vektor prostoru W . Jestliže $w_1, w_2 \in f(V')$, pak existují $v_1, v_2 \in V'$, pro které $f(v_1) = w_1$ a $f(v_2) = w_2$. Podle definice homomorfismu je

$$f(v_1 + v_2) = f(v_1) + f(v_2) = w_1 + w_2 ,$$

a protože $v_1 + v_2 \in V'$ (neboť V' je podprostor), je $w_1 + w_2 \in f(V')$. Jestliže $w \in f(V')$, pak existuje vektor $v \in V'$, pro který $f(v) = w$. Podle definice homomorfismu je pro každé $a \in T$

$$f(av) = a \cdot f(v) = aw ,$$

a protože $av \in V'$ (neboť V' je podprostor), je $aw \in f(V')$. Množina $f(V')$ je tedy neprázdná, uzavřená vzhledem ke sčítání vektorů a vzhledem k násobení vektorů skaláry a je proto podprostorem prostoru W . Tvrzení (iv) je tedy dokázáno; tvrzení (v) je důsledkem tvrzení (iv), neboť $\text{Im } f$ je obrazem prostoru V .

Nechť M je množinou generátorů prostoru V a necht' $w \in \text{Im } f$ je libovolně zvolený vektor. Pak existuje vektor $v \in V$, pro který je $f(v) = w$. Vektor v je lineární kombinací vektorů množiny M ; pišme:

$$v = \sum_{i=1}^k a_i x_i , \quad \text{kde } x_1, \dots, x_k \in M, \quad a_1, \dots, a_k \in T .$$

Podle tvrzení (iii) je

$$w = f(v) = \sum_{i=1}^k a_i f(x_i) ,$$

tj. vektor w je lineární kombinací vektorů $f(x_1), \dots, f(x_k) \in f(M)$. Množina $f(M)$ tedy generuje podprostor $\text{Im } f$.

Nechť W' je podprostorem prostoru W a V' je jeho úplný vzor, tj. množina všech vektorů $v \in V$, pro které $f(v) \in W'$. Množina V' je neprázdná, neboť obsahuje nulový vektor (viz (i)). Nechť $v_1, v_2 \in V'$, tj. $f(v_1), f(v_2) \in W'$. Podle definice homomorfismu je $f(v_1 + v_2) = f(v_1) + f(v_2)$. Protože $f(v_1) + f(v_2) \in W'$ (neboť W' je podprostor), je $v_1 + v_2 \in V'$. Nechť $v \in V'$, tj. $f(v) \in W'$, a $a \in T$. Podle definice homomorfismu je $f(av) = a \cdot f(v)$. Protože je $a \cdot f(v) \in W'$ (neboť W' je podprostor), je $av \in V'$. Množina V' je tedy neprázdná, uzavřená vzhledem ke sčítání vektorů a násobení vektorů skaláry, tj. V' je podprostorem prostoru V . Tvrzení (vii) je dokázáno; tvrzení (viii) je důsledkem tvrzení (vii), neboť $\text{Ker } f$ je úplným vzorem nulového podprostoru prostoru W .

Nechť $w \in \text{Im } f$. Zvolme libovolný vektor $v \in V$, pro který je $f(v) = w$. Jestliže je $u \in \text{Ker } f$, pak je

$$f(v + u) = f(v) + f(u) = w + o = w ;$$

lineární množina $v + \text{Ker } f$ je tedy obsažena v úplném vzoru vektoru w . Jestliže $f(x) = w$ pro nějaký vektor $x \in V$, pak

$$f(x - v) = f(x) - f(v) = w - w = o ,$$

takže je $x - v = y \in \text{Ker } f$ a tedy $x = v + y \in v + \text{Ker } f$. Úplným vzorem vektoru $w \in \text{Im } f$ je tedy lineární množina $v + \text{Ker } f$. \square

10.5. Příklad. Zobrazení d , které každému polynomu s reálnými koeficienty přiřazuje jeho derivaci, je homomorfismus prostoru $\mathbb{R}[x]$ do prostoru $\mathbb{R}[x]$. Jádrem tohoto homomorfismu tvoří všechny konstantní polynomy; můžeme psát $\text{Ker } d = [1]$. Zřejmě je $\text{Im } d = \mathbb{R}[x]$. Obrazem podprostoru tvořeného právě všemi polynomy stupně nejvýše n je podprostor právě všech polynomů stupně nejvýše $n - 1$. Úplným vzorem podprostoru všech polynomů stupně nejvýše n je podprostor všech polynomů stupně nejvýše $n + 1$. Úplným vzorem polynomu

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

je lineární množina

$$\frac{a_n}{n+1} x^{n+1} + \frac{a_{n-1}}{n} x^n + \dots + a_0 x + [1] ;$$

polynomy této množiny se liší pouze absolutním členem.

10.6. Věta. *Jestliže f je homomorfismus prostoru U do prostoru V a g homomorfismus prostoru V do prostoru W , potom složené zobrazení gf je homomorfismus prostoru U do prostoru W .*

Důkaz. Necht $u_1, u_2 \in U$. Protože f i g jsou homomorfismy, je

$$\begin{aligned}(gf)(u_1 + u_2) &= g(f(u_1 + u_2)) = g(f(u_1) + f(u_2)) = \\ &= g(f(u_1)) + g(f(u_2)) = (gf)(u_1) + (gf)(u_2) .\end{aligned}$$

Necht $u \in U$ a $a \in T$. Protože jsou f a g homomorfismy, je

$$(gf)(au) = g(f(au)) = g(a \cdot f(u)) = a \cdot (g(f(u))) = a \cdot (gf)(u) .$$

Ukázali jsme tedy, že složené zobrazení gf je homomorfismus prostoru U do prostoru W . \square

Jestliže je tedy $f \in \text{Hom}(U, V)$ a $g \in \text{Hom}(V, W)$, pak je $gf \in \text{Hom}(U, W)$; stručně říkáme, že složení homomorfismů je homomorfismus.

Protože pro skládání homomorfismů platí asociativní zákon (ten platí obecněji pro skládání zobrazení), není nutné užívat při zápisech složených homomorfismů závorek.

10.7. Věta. *Necht V je vektorový prostor nad tělesem T a M je podmnožina prostoru V . Množina M je bází prostoru V právě tehdy, když libovolné zobrazení množiny M do libovolně zvoleného prostoru W nad tělesem T je možno právě jediným způsobem rozšířit na homomorfismus.*

Důkaz. (i) Předpokládejme, že M je báze prostoru V . Necht g je nějaké zobrazení báze M do nějakého vektorového prostoru W . Definujme zobrazení f prostoru V do prostoru W takto: libovolně zvolený vektor $v \in V$ se dá jediným způsobem zapsat jako lineární kombinace vektorů báze M ; pišme

$$v = \sum_{x \in M} b_x x , \quad \text{kde } b_x \in T \quad \text{pro každé } x \in M .$$

Obraz tohoto vektoru v při zobrazení f definujme rovností

$$f(v) = \sum_{x \in M} b_x g(x) .$$

Má-li být zobrazení f homomorfismem rozšiřujícím zobrazení g , pak jiným způsobem f definovat nemůžeme (viz 10.4(iii)). Odtud vyplývá jednoznačnost; nyní dokažme, že f je homomorfismus.

Jestliže je ještě $v' \in V$,

$$v' = \sum_{x \in M} b'_x x , \quad \text{kde } b'_x \in T \quad \text{pro každé } x \in M ,$$

a $a \in T$, pak je

$$v + v' = \sum_{x \in M} (b_x + b'_x) x , \quad av = \sum_{x \in M} (ab_x) x$$

a podle definice zobrazení f je

$$f(v + v') = \sum_{x \in M} (b_x + b'_x)g(x) = \sum_{x \in M} b_x g(x) + \sum_{x \in M} b'_x g(x) = f(v) + f(v') ,$$

$$f(av) = \sum_{x \in M} (ab_x)g(x) = a \cdot \sum_{x \in M} b_x g(x) = a \cdot f(v) .$$

Zobrazení f je tedy homomorfismus.

(ii) Předpokládejme naopak, že libovolné zobrazení množiny M do libovolně zvoleného prostoru W je možno jediným způsobem rozšířit na homomorfismus. Jestliže je množina M lineárně závislá, pak je nějaký vektor $v \in M$ možno vyjádřit jako lineární kombinaci ostatních vektorů množiny M , tj.

$$v = \sum_{i=1}^k a_i v_i , \quad \text{kde } v, v_1, \dots, v_k \in M , \quad a_1, \dots, a_k \in T$$

(uvažované vektory jsou navzájem různé a skaláry vesměs nenulové). Zobrazení g množiny M do libovolně zvoleného nenulového vektorového prostoru W , které vektorům v_1, \dots, v_k přiřadí nulový vektor a vektoru v vektor nenulový, nejde rozšířit na homomorfismus f , neboť by pak muselo platit

$$o \neq f(v) = \sum_{i=1}^k a_i f(v_i) = o .$$

Z tohoto sporu vyplývá, že množina M je lineárně nezávislá.

Předpokládejme tedy, že množina M je lineárně nezávislá, ale není množinou generátorů prostoru V . Rozšířme ji na bázi N prostoru V . Zobrazení g množiny M do prostoru V jde zřejmě více způsoby rozšířit na zobrazení množiny N do prostoru V (neboť M je vlastní podmnožinou množiny N) a tedy i více způsoby na homomorfismus prostoru V do prostoru V (podle již dokázané implikace – první část důkazu). Z tohoto sporu vyplývá, že množina M je bázi prostoru V . \square

10.8. Důsledek. *Nechť V a W jsou vektorové prostory nad tělesem T . Každý homomorfismus prostoru V do prostoru W je určen obrazy vektorů libovolně zvolené báze prostoru V .* \square

Chceme-li tedy definovat homomorfismus prostoru V do prostoru W , stačí zvolit nějakou bázi prostoru V a vektorům této báze přiřadit nějaké vektory prostoru W . Tento způsob definování homomorfismů budeme často používat.

Podle předchozího důsledku může být např. každý homomorfismus g podprostoru U prostoru V do prostoru W rozšířen na homomorfismus f prostoru V do prostoru W . Stačí zvolit nějakou bázi M podprostoru U , rozšířit ji na bázi N prostoru V , na vektorech báze M definovat homomorfismus f stejně jako g a na vektorech z $N \setminus M$ libovolně.

10.9. Definice. Surjektivní homomorfismus se nazývá *epimorfismus*, injektivní homomorfismus se nazývá *monomorfismus*, bijektivní homomorfismus se nazývá *izomorfismus*.

Jestliže existuje izomorfismus prostoru V na prostor W , říkáme, že prostory V a W jsou *izomorfní* a tento fakt zapisujeme symbolem $V \cong W$.

Homomorfismus prostoru V do téhož prostoru V se nazývá *endomorfismus* prostoru V nebo též *lineární operátor* na prostoru V . Bijektivní endomorfismus prostoru V (tj. izomorfismus V na V) se nazývá *automorfismus* prostoru V .

Množinu všech endomorfismů prostoru V značíme $\text{End } V$, množinu všech automorfismů prostoru V značíme $\text{Aut } V$.

Zřejmě je $\text{Aut } V \subseteq \text{End } V = \text{Hom}(V, V)$.

10.10. Příklady.

(i) Zobrazení \log prostoru \mathbb{R}^+ (viz 8.19(x)) do prostoru \mathbb{R} , které každému kladnému reálnému číslu x přiřazuje číslo $\log_z x$, je izomorfismus prostoru \mathbb{R}^+ na prostor \mathbb{R} , neboť jde o bijekci a pro libovolně zvolená čísla $x, y \in \mathbb{R}^+$, $a \in \mathbb{R}$ platí

$$\log_z xy = \log_z x + \log_z y, \quad \log_z x^a = a \log_z x.$$

Prostory \mathbb{R}^+ a \mathbb{R} jsou tedy izomorfní. Poznamenejme, že nezáleží na tom, jaký základ z logaritmu uvažujeme.

(ii) Zobrazení f prostoru \mathbb{R}^3 do prostoru \mathbb{R}^2 , které vektoru (x, y, z) přiřazuje vektor $(x + y, 2y - z)$, je epimorfismus.

(iii) Zobrazení f prostoru \mathbb{R}^3 do prostoru \mathbb{R}^4 , které vektoru (x, y, z) přiřazuje vektor $(x, x + y, x + y + z, x - y + 2z)$, je monomorfismus.

(iv) Vnoření podprostoru U do prostoru V , které jsme definovali v 10.3(ii), je zřejmě monomorfismus. Přirozený homomorfismus prostoru V na faktorový prostor V/U , který jsme definovali v 10.3(iii), je zřejmě epimorfismus. Identický automorfismus 1_V prostoru V definovaný v 10.3(ii) je bijekce; termín zavedený v 10.3(ii) je tedy ve shodě s definicí 10.9.

(v) Nechť V je prostor dimenze m nad tělesem T a $M = \{v_1, \dots, v_m\}$ jeho báze. Přiřadíme-li každému vektoru $x \in V$ jeho souřadnice vzhledem k bázi M , dostaneme izomorfismus f prostoru V na prostor T^m . Viděli jsme už, že toto zobrazení je bijekce (viz 8.13, 8.14 a dále); ukažme, že jde vskutku o izomorfismus.

Jestliže je

$$x = \sum_{i=1}^m a_i v_i, \quad y = \sum_{i=1}^m b_i v_i \quad \text{a} \quad c \in T,$$

potom je

$$x + y = \sum_{i=1}^m (a_i + b_i) v_i, \quad cx = \sum_{i=1}^m ca_i v_i.$$

Je tedy

$$f(x) = (a_1, \dots, a_m), \quad f(y) = (b_1, \dots, b_m),$$

$$f(x+y) = (a_1 + b_1, \dots, a_m + b_m), \quad f(cx) = (ca_1, \dots, ca_m),$$

takže platí rovnosti

$$f(x+y) = f(x) + f(y) \quad \text{a} \quad f(cx) = cf(x).$$

Zobrazení f je tedy izomorfismus prostoru V na prostor T^m .

Jestliže má prostor V nekonečnou dimenzi α , pak postupujeme obdobně; změni se jen označení. Vektoru $x \in V$ přiřadíme jeho souřadnice $(a_v)_{v \in M}$ vzhledem k pevně zvolené bázi M . Dostáváme bijekci f prostoru V na prostor $K(T^M)$, tj. na direktní součet α exemplářů tělesa T (viz příklad 9.12). Je-li

$$x = \sum_{v \in M} a_v v, \quad y = \sum_{v \in M} b_v v \quad \text{a} \quad c \in T,$$

je

$$x+y = \sum_{v \in M} (a_v + b_v)v \quad \text{a} \quad cx = \sum_{v \in M} ca_v v.$$

Tedy

$$f(x) = (a_v)_{v \in M}, \quad f(y) = (b_v)_{v \in M},$$

$$f(x+y) = (a_v + b_v)_{v \in M}, \quad f(cx) = (ca_v)_{v \in M},$$

takže f je izomorfismus.

(vi) Zobrazení f prostoru všech polynomů stupně nejvýše n nad tělesem T (n je pevně zvoleno) do prostoru T^{n+1} , které každému polynomu $a_0 + a_1x + \dots + a_nx^n$ přiřazuje $(n+1)$ -tici (a_0, a_1, \dots, a_n) jeho koeficientů, je izomorfismus. Jde vlastně o izomorfismus z příkladu (v), který každému polynomu přiřazuje $(n+1)$ -tici jeho souřadnic vzhledem k bázi $\{1, x, x^2, \dots, x^n\}$.

Podobně můžeme hovořit o izomorfismu prostoru $T[x]$ všech polynomů nad tělesem T na prostor $K(T^{\mathbb{N}})$ posloupností prvků tělesa T , které mají jen konečně mnoho nenulových prvků; tento izomorfismus přiřazuje každému polynomu $a_0 + a_1x + \dots + a_nx^n$ posloupnost $(a_0, a_1, \dots, a_n, 0, 0, \dots)$. Uvědomme si, že jde o souřadnice uvažovaného polynomu vzhledem k bázi $\{1, x, x^2, \dots\}$ prostoru $T[x]$.

(vii) Nechť V je vektorový prostor všech funkcí v , které mají na intervalu $\langle 0, 1 \rangle$ spojitou druhou derivaci a pro které je $v(0) = v'(0) = 0$. Nechť p, q jsou pevně zvolené funkce, které jsou spojitě na intervalu $\langle 0, 1 \rangle$. Přiřadíme-li každé funkci $v \in V$ funkci

$$v'' + pv' + qv,$$

dostáváme izomorfismus prostoru V na prostor všech spojitých funkcí na intervalu $\langle 0, 1 \rangle$. Uvažované zobrazení je zřejmě homomorfismus; navíc z teorie diferenciálních rovnic plyne, že pro každou funkci y , která je spojitá na intervalu $\langle 0, 1 \rangle$, má diferenciální rovnice

$$y = x'' + px' + qx$$

právě jediné řešení $x \in V$. Jde tedy o izomorfismus.

10.11. Příklad. Následující věta o homomorfismu nemá v teorii vektorových prostorů ten význam jako věta o homomorfismu v teorii grup či jiných algebraických struktur. Uvádíme ji kvůli procvičení pojmů a jako průpravu pro obecnou algebru.

Věta o homomorfismu *Nechť f je homomorfismus prostoru V do prostoru W ; označme ν přirozený homomorfismus prostoru V na faktorový prostor $V/\text{Ker } f$ a ι vnoření podprostoru $\text{Im } f$ do prostoru W . Potom existuje právě jediný izomorfismus κ prostoru $V/\text{Ker } f$ na prostor $\text{Im } f$, pro který platí $f = \iota\kappa\nu$.*

Důkaz. Definujme zobrazení κ prostoru $V/\text{Ker } f$ do prostoru $\text{Im } f$ takto: pro každý prvek $v + \text{Ker } f \in V/\text{Ker } f$ položíme $\kappa(v + \text{Ker } f) = f(v)$.

Jestliže je $v_1 + \text{Ker } f = v_2 + \text{Ker } f$, potom je $v_1 - v_2 \in \text{Ker } f$ (viz 7.21(iv)) a

$$0 = f(v_1 - v_2) = f(v_1) - f(v_2) ;$$

definice zobrazení κ tedy nezávisí na volbě reprezentanta lineární množiny $v + \text{Ker } f$ a je proto korektní. Dále je

$$\begin{aligned} \kappa((v_1 + \text{Ker } f) + (v_2 + \text{Ker } f)) &= \kappa((v_1 + v_2) + \text{Ker } f) = \\ &= f(v_1 + v_2) = f(v_1) + f(v_2) = \kappa(v_1 + \text{Ker } f) + \kappa(v_2 + \text{Ker } f) , \\ \kappa(a(v + \text{Ker } f)) &= \kappa(av + \text{Ker } f) = f(av) = a \cdot f(v) = a \cdot \kappa(v + \text{Ker } f) ; \end{aligned}$$

zobrazení κ je tedy homomorfismus. Zřejmě je $\kappa(v + \text{Ker } f) = 0$, právě když je $f(v) = 0$, tj. $v \in \text{Ker } f$ neboli $v + \text{Ker } f = \text{Ker } f$. Jádrem homomorfismu κ je tedy triviální, tj. κ je monomorfismus. Surjektivita zobrazení κ je zřejmá, takže κ je izomorfismus.

Pro každý vektor $v \in V$ je

$$\iota\kappa\nu(v) = \iota\kappa(v + \text{Ker } f) = \iota(f(v)) = f(v) ,$$

takže rovnost $\iota\kappa\nu = f$ platí. Zároveň odtud vyplývá, že zobrazení κ jsme jiným způsobem definovat nemohli. \square

Věta o homomorfismu se často stručně zapisuje v tvaru

$$V/\text{Ker } f \cong \text{Im } f .$$

10.12. Věta. *Nechť f je homomorfismus prostoru U do prostoru V a g homomorfismus prostoru V do prostoru W . Potom platí:*

- (i) *Jsou-li f a g monomorfismy (epimorfismy, izomorfismy), je gf také monomorfismus (epimorfismus, izomorfismus).*
- (ii) *Jestliže je gf monomorfismus, je f monomorfismus.*
- (iii) *Jestliže je gf epimorfismus, je g epimorfismus.*
- (iv) *Jestliže je gf izomorfismus, je f monomorfismus a g epimorfismus.*

Důkaz. Tvrzení (i) platí, neboť složení homomorfismů je homomorfismus a složení injekcí (surjekcí) je injekce (surjekce).

Jestliže zobrazení f není injektivní, není injektivní ani zobrazení gf . Jestliže zobrazení g není surjektivní, není surjektivní ani zobrazení gf . Platí tedy tvrzení (ii) a (iii); tvrzení (iv) je jejich důsledkem. \square

10.13. Věta. *Jestliže je f izomorfismus prostoru V na prostor W , potom je zobrazení f^{-1} izomorfismus prostoru W na prostor V .*

Důkaz. Inverzní zobrazení f^{-1} prostoru W na prostor V existuje, neboť f je bijekce; zobrazení f^{-1} je rovněž bijekce. Dokážeme, že f^{-1} je homomorfismus. Nechť $w_1, w_2 \in W$; existují tedy vektory $v_1, v_2 \in V$, pro které $f(v_1) = w_1$ a $f(v_2) = w_2$. Nyní je

$$\begin{aligned} f^{-1}(w_1 + w_2) &= f^{-1}(f(v_1) + f(v_2)) = f^{-1}(f(v_1 + v_2)) = \\ &= v_1 + v_2 = f^{-1}(w_1) + f^{-1}(w_2). \end{aligned}$$

Nechť $w \in W$; existuje tedy vektor $v \in V$, pro který je $f(v) = w$. Pro každé $a \in T$ je

$$f^{-1}(aw) = f^{-1}(af(v)) = f^{-1}(f(av)) = av = a \cdot f^{-1}(w).$$

Zobrazení f^{-1} je tedy izomorfismus prostoru W na prostor V . \square

10.14. Věta o epimorfismu. *Pro homomorfismus f prostoru U do prostoru V jsou následující tvrzení ekvivalentní:*

- (i) *f je epimorfismus.*
- (ii) *Existuje homomorfismus g prostoru V do prostoru U , pro který $fg = 1_V$.*
- (iii) *Jsou-li h_1 a h_2 homomorfismy prostoru V do nějakého prostoru W , pro které $h_1f = h_2f$, potom $h_1 = h_2$.*

Důkaz. Dokážeme implikace $(i) \implies (ii) \implies (iii) \implies (i)$.

$(i) \implies (ii)$. Nechť f je epimorfismus. Zvolme bázi M prostoru V a definujme homomorfismus g prostoru V do prostoru U určením obrazů vektorů báze M (podle 10.7 — využívá se existence takto určeného homomorfismu): pro každý vektor $v \in M$ položme $g(v) = u$, kde $u \in U$ je nějaký vektor, pro který je $f(u) = v$ — takový vektor existuje, neboť f je podle předpokladu epimorfismus. Pro každý

vektor $v \in M$ je nyní $fg(v) = v$. Endomorfismus fg prostoru V tedy zobrazuje vektory báze M stejně jako identický automorfismus 1_V prostoru V . Podle věty 10.7 (nyní se využívá jednoznačnosti) je tedy $fg = 1_V$.

(ii) \implies (iii). Předpokládejme, že platí tvrzení (ii). Jsou-li h_1 a h_2 homomorfismy prostoru V do prostoru W , pro které je $h_1f = h_2f$, potom podle tvrzení (ii) je $h_1fg = h_2fg$, tj. $h_1 = h_2$.

(iii) \implies (i). Předpokládejme, že f není epimorfismus. Zvolme nějakou bázi M prostoru $\text{Im } f$ a rozšířme ji na bázi N prostoru V ; množina $N \setminus M$ je tedy neprázdná. Označme h_1 identický automorfismus prostoru V a h_2 endomorfismus prostoru V , který vektory množiny M zobrazí identicky a vektory množiny $N \setminus M$ zobrazí na nulový vektor. Nyní je $h_1f = f = h_2f$ a přitom je $h_1 \neq h_2$. Jestliže tedy platí tvrzení (iii), pak f musí být epimorfismus. \square

10.15. Věta o monomorfismu. *Pro homomorfismus f prostoru V do prostoru W jsou následující tvrzení ekvivalentní:*

- (i) f je monomorfismus.
- (ii) $\text{Ker } f = O$.
- (iii) *Obraz každé lineárně nezávislé podmnožiny prostoru V je lineárně nezávislá podmnožina prostoru W .*
- (iv) *Obraz každé báze prostoru V je báze prostoru $\text{Im } f$.*
- (v) *Existuje homomorfismus g prostoru W do prostoru V , pro který $gf = 1_V$.*
- (vi) *Jsou-li h_1 a h_2 homomorfismy nějakého prostoru U do prostoru V , pro které $fh_1 = fh_2$, potom $h_1 = h_2$.*

Důkaz. Dokážeme implikace (i) \implies (ii) \implies (i), (ii) \implies (iii) \implies (iv) \implies (ii), (i) \implies (v) \implies (vi) \implies (i).

(i) \implies (ii). Jestliže je f monomorfismus, je nutně $\text{Ker } f = O$, neboť $\text{Ker } f$ je úplný vzor nulového vektoru prostoru W .

(ii) \implies (i). Předpokládejme, že $\text{Ker } f = O$. Jestliže $v_1, v_2 \in V$ a $f(v_1) = f(v_2)$, potom je

$$f(v_1 - v_2) = f(v_1) - f(v_2) = o.$$

Je tedy $v_1 - v_2 \in \text{Ker } f = O$, odtud $v_1 = v_2$ a f je monomorfismus.

Je možno též uvažovat takto: Je-li $\text{Ker } f = O$, pak podle 10.4(ix) je úplný vzor každého vektoru $w \in \text{Im } f$ jednoprvkový, tj. f je monomorfismus.

(ii) \implies (iii). Nechť $\text{Ker } f = O$ a nechť M je lineárně nezávislá podmnožina prostoru V . Předpokládejme, že nějaká netriviální lineární kombinace navzájem různých vektorů $f(v_1), f(v_2), \dots, f(v_k)$ množiny $f(M)$ je rovna nulovému vektoru:

$$o = \sum_{i=1}^k a_i f(v_i).$$

Potom je

$$o = f\left(\sum_{i=1}^k a_i v_i\right), \quad \text{neboli} \quad \sum_{i=1}^k a_i v_i \in \text{Ker } f = O.$$

Protože je množina M lineárně nezávislá, jsou všechny koeficienty a_1, \dots, a_k nulové. Množina $f(M)$ je proto rovněž lineárně nezávislá.

(iii) \implies (iv). Obraz každé báze prostoru V je podle (iii) lineárně nezávislá množina vektorů prostoru W a podle 10.4.(vi) je zároveň množinou generátorů prostoru $\text{Im } f$.

(iv) \implies (ii). Každý nenulový vektor $v \in V$ je prvkem nějaké báze prostoru V . Podle tvrzení (iv) je jeho obraz $f(v)$ prvkem nějaké báze prostoru $\text{Im } f$ a je proto nenulový. Tedy $\text{Ker } f = O$.

(i) \implies (v). Nechť f je monomorfismus a M báze prostoru V . Protože jsme již dokázali ekvivalenci tvrzení (i) a (iv), je $f(M)$ báze podprostoru $\text{Im } f$ prostoru W . Nechť N je báze prostoru W , která obsahuje množinu $f(M)$ (báze N existuje podle věty 8.11). Definujme nyní homomorfismus g prostoru W do prostoru V určením obrazů vektorů báze N . Jestliže $w \in N \setminus f(M)$, definujeme $g(w) = o$. Jestliže $w \in f(M)$, definujeme $g(w) = v$, kde v je vektor báze M , pro který $f(v) = w$. Pro každý vektor $v \in M$ je tedy $gf(v) = v$. Endomorfismus gf prostoru V tedy zobrazuje vektory báze M stejně jako identický automorfismus prostoru V . Podle věty 10.7 je tedy $gf = 1_V$.

(v) \implies (vi). Předpokládejme, že platí tvrzení (v). Jsou-li h_1 a h_2 homomorfismy prostoru U do prostoru V , pro které $fh_1 = fh_2$, potom $gh_1 = gh_2$, tj. $h_1 = h_2$.

(vi) \implies (i). Předpokládejme, že platí tvrzení (vi) a že f není monomorfismus. Existují tedy vektory $v_1, v_2 \in V$, $v_1 \neq v_2$, pro které $f(v_1) = f(v_2)$. Zvolme jednodimenzionální prostor $[u]$ a definujme homomorfismy h_1 a h_2 takto (viz 10.7): $h_1(u) = v_1$, $h_2(u) = v_2$. Nyní $fh_1 = fh_2$ a přitom $h_1 \neq h_2$. Jestliže tedy platí tvrzení (vi), je f monomorfismus. \square

Z předchozích dvou vět vyplývá, že epimorfismy jsou právě ty homomorfismy, kterými při skládání homomorfismů můžeme krátit zprava (tj. „ze začátku“) a monomorfismy jsou právě ty homomorfismy, kterými při skládání homomorfismů můžeme krátit zleva (tj. „z konce“).

V důkazu věty o monomorfismu jsme mohli postupovat o něco efektivněji. Charakterizace monomorfismu nulovým jádrem (ekvivalence tvrzení (i) a (ii)) je však tak elementární a důležitá, že jsme ji dokázali zvlášť.

10.16. Příklad. Nechť V a W jsou reálné vektorové prostory dimenzí 2 a 1 a $M = \{v_1, v_2\}$, $N = \{w\}$ jejich báze. Zobrazení g báze M do prostoru W definujeme rovnostmi $g(v_1) = g(v_2) = w$. Homomorfismus f rozšiřující zobrazení g (viz 10.7) není monomorfismus, ale přesto je obrazem báze M prostoru V báze N prostoru $\text{Im } f = W$. Uvědomme si však, že neplatí tvrzení (iv) věty 10.15, tj. není pravda, že obrazem každé báze prostoru V je báze prostoru $\text{Im } f$. Např. báze $\{2v_1, v_2\}$

prostoru V se homomorfismem f zobrazí na množinu $\{2w, w\}$, která je lineárně závislá.

10.17. Definice. Nechť f je homomorfismus prostoru V do prostoru W . *Hodnotí* $r(f)$ homomorfismu f budeme rozumět dimenzi podprostoru $\text{Im } f$ prostoru W . *Defektem* $d(f)$ homomorfismu f budeme rozumět dimenzi podprostoru $\text{Ker } f$ prostoru V .

Hodnost a defekt homomorfismu f jsou tedy definovány rovnostmi

$$r(f) = \dim \text{Im } f, \quad d(f) = \dim \text{Ker } f.$$

Monomorfismy, izomorfismy a automorfismy mají tedy nulový defekt; defekt můžeme chápat jako míru porušení injektivitu homomorfismu.

10.18. Věta o hodnotě a defektu. *Pro homomorfismus f prostoru V do prostoru W platí rovnost*

$$\dim V = r(f) + d(f).$$

Důkaz. Nejprve provedeme důkaz v případě, že má prostor V konečnou dimenzi.

Nechť $\{v_1, \dots, v_k\}$ je báze prostoru $\text{Ker } f$ a $M = \{v_1, \dots, v_k, v_{k+1}, \dots, v_m\}$ báze prostoru V (taková báze existuje podle věty 8.11). Ukážeme, že množina $N = \{f(v_{k+1}), \dots, f(v_m)\}$ je bází prostoru $\text{Im } f$. Podle 10.4(vi) je N množinou generátorů prostoru $\text{Im } f$, neboť $f(v_1) = \dots = f(v_k) = o$.

Nejprve ukážeme, že vektory $f(v_{k+1}), \dots, f(v_m)$ jsou navzájem různé. Kdyby bylo např. $f(v_{k+1}) = f(v_m)$, byl by vektor $v_{k+1} - v_m$ prvkem $\text{Ker } f$ a byl by tedy lineární kombinací vektorů v_1, \dots, v_k . To však není možné, neboť M je báze.

Nyní ukážeme, že množina N je lineárně nezávislá. Jestliže je

$$\sum_{i=k+1}^m a_i f(v_i) = o,$$

potom je

$$f\left(\sum_{i=k+1}^m a_i v_i\right) = o$$

a odtud

$$\sum_{i=k+1}^m a_i v_i \in \text{Ker } f.$$

Existují tedy skaláry $b_1, \dots, b_k \in T$ takové, že

$$\sum_{i=k+1}^m a_i v_i = \sum_{j=1}^k b_j v_j.$$

Odtud vyplývá rovnost

$$\sum_{j=1}^k b_j v_j - \sum_{i=k+1}^m a_i v_i = o .$$

Protože je množina M lineárně nezávislá, je $a_{k+1} = \dots = a_m = 0$ (a rovněž $b_1 = \dots = b_k = 0$) a množina N je tedy také lineárně nezávislá, tj. N je bázi prostoru $\text{Im } f$. Vzhledem k tomu, že $\dim V = m$, $d(f) = k$ a $r(f) = m - k$, je tvrzení dokázáno.

V obecném případě, kdy je dimenze prostoru V jakákoliv, postupujeme obdobně. Bázi K podprostoru $\text{Ker } f$ rozšíříme na bázi M prostoru V . Množina $N = f(M \setminus K)$ generuje podprostor $\text{Im } f$; pro každé dva vektory $x, y \in M \setminus K$ je $f(x) \neq f(y)$, proto homomorfismus f vzájemně jednoznačně zobrazuje množinu $M \setminus K$ na množinu N .

Jestliže je nějaká lineární kombinace vektorů množiny N rovna nulovému vektoru, tj.

$$\sum_{v \in M \setminus K} a_v f(v) = o ,$$

potom

$$\sum_{v \in M \setminus K} a_v v \in \text{Ker } f .$$

Existují tedy skaláry $b_v \in T$, $v \in K$, takové, že

$$\sum_{v \in M \setminus K} a_v v = \sum_{v \in K} b_v v .$$

Protože je množina M lineárně nezávislá, jsou všechny koeficienty a_v , $v \in M \setminus K$ (a rovněž koeficienty b_v , $v \in K$) rovny nule, takže množina N je také lineárně nezávislá a je tedy bázi podprostoru $\text{Im } f$. Je tedy

$$\dim V = |M| = |K| + |M \setminus K| = |K| + |N| = d(f) + r(f) . \quad \square$$

Větu o hodnotě a defektu jsme zformulovali a dokázali zcela obecně víceméně z metodických důvodů. Věta má však význam pouze tehdy, když má prostor V konečnou dimenzi. V tom případě totiž můžeme ze znalosti libovolných dvou ze tří čísel $\dim V$, $d(f)$ a $r(f)$ určit číslo zbývající. Má-li prostor V dimenzi nekonečnou, není to vždy možné (nelze odčítat nekonečná kardinální čísla).

10.19. Důsledek. *Jestliže je W podprostorem prostoru V , potom je*

$$\dim V = \dim W + \dim V/W .$$

Důkaz. Pro přirozený homomorfismus ν prostoru V na faktorový prostor V/W je zřejmé $\text{Ker } \nu = W$ a $\text{Im } \nu = V/W$. Nyní stačí užít větu o hodnotě a defektu. \square

10.20. Věta. *Nechť U, V, W jsou vektorové prostory nad tělesem T . Nechť f je homomorfismus prostoru V do prostoru W a g je homomorfismus prostoru U do prostoru V . Potom je*

$$d(fg) \leq d(f) + d(g) .$$

Důkaz. Zřejmě je $\text{Ker } g \subseteq \text{Ker } fg$. Zvolme bázi $\{u_1, \dots, u_r\}$ podprostoru $\text{Ker } g$ a rozšířme ji na bázi $\{u_1, \dots, u_s\}$ podprostoru $\text{Ker } fg$ (je tedy $r \leq s$). Víme (např. z důkazu věty 10.18), že vektory $g(u_{r+1}), \dots, g(u_s)$ jsou navzájem různé a lineárně nezávislé. Protože tyto vektory leží v $\text{Ker } f$, je $s-r \leq d(f)$, tj. $d(fg) \leq d(f) + d(g)$.

Poznamenejme, že tvrzení se dokáže obdobným způsobem i v případě nekonečných dimenzí. \square

10.21. Poznámka. Nechť f je homomorfismus prostoru V do prostoru W .

Jestliže je f monomorfismus, pak je $d(f) = 0$ a podle věty o hodnotě a defektu je

$$\dim V = r(f) = \dim \text{Im } f \leq \dim W ;$$

prostor W musí tedy mít dimenzi aspoň tak velkou jako prostor V .

Jestliže je f epimorfismus, pak je $r(f) = \dim W$ a podle věty o hodnotě a defektu je

$$\dim V = d(f) + \dim W \geq \dim W ;$$

prostor V musí mít tedy dimenzi aspoň tak velkou jako prostor W .

Jestliže je f izomorfismus, je tedy $\dim V = \dim W$ (viz dále věta 10.22).

Předpokládejme, že prostory V a W mají stejnou konečnou dimenzi.

Každý monomorfismus f prostoru V do prostoru W je již izomorfismem; je totiž $d(f) = 0$ a podle věty o hodnotě a defektu je

$$\dim W = \dim V = r(f) = \dim \text{Im } f ,$$

takže $\text{Im } f = W$ a f je epimorfismus.

Podobně je každý epimorfismus g prostoru V na prostor W již izomorfismem; je totiž

$$\dim W = \dim V = d(g) + r(g) = d(g) + \dim W ,$$

takže $d(g) = 0$ a g je monomorfismus.

10.22. Věta. *Dva vektorové prostory jsou izomorfní právě tehdy, když mají stejnou dimenzi.*

Důkaz. Předpokládejme, že prostory V a W jsou izomorfní a že f je nějaký izomorfismus prostoru V na prostor W . Je tedy $d(f) = 0$, $r(f) = \dim W$ a podle věty o hodnotě a defektu je $\dim V = d(f) + r(f) = \dim W$.

Jiný důkaz: Nechť M je báze prostoru V . Protože je f monomorfismus, zobrazuje bázi M vzájemně jednoznačně na nějakou bázi N prostoru $\text{Im } f$. Protože je f epimorfismus, je N bázi prostoru W , tedy $\dim V = |M| = |N| = \dim W$.

Předpokládejme naopak, že V a W jsou prostory téže dimenze a M a N jejich báze. Pak existuje vzájemně jednoznačné zobrazení g množiny M na množinu N . Podle věty 10.7 je tímto zobrazením g určen homomorfismus f prostoru V do prostoru W , který je určen vztahem

$$f\left(\sum_{v \in M} a_v v\right) = \sum_{v \in M} a_v g(v) .$$

Protože je báze N prostoru W obsažena v obraze $\text{Im } f$, je f epimorfismus. Vzhledem k tomu, že homomorfismus f zobrazuje lineární kombinaci vektorů báze M na lineární kombinaci vektorů báze N se stejnými koeficienty a_v , je obrazem každé netriviální lineární kombinace opět netriviální lineární kombinace, tj. obrazem nenulového vektoru prostoru V je nenulový vektor prostoru W . Homomorfismus f je tedy monomorfismus.

Jiný důkaz: Předpokládejme, že V je prostor dimenze α a M nějaká jeho báze. Přiřadíme-li každému vektoru $x = \sum_{v \in M} a_v v \in V$ soubor jeho souřadnic $(a_v)_{v \in M}$, dostáváme zřejmě izomorfismus prostoru V na prostor $K(T^M)$, tj. na direktní součet α exemplářů tělesa T (viz 9.12). Jsou-li V a W prostory dimenze α , jsou oba izomorfní s direktním součtem α exemplářů tělesa T a tedy izomorfní navzájem. \square

V osmém paragrafu jsme viděli (viz 8.22), že vektorový prostor konečné dimenze neobsahuje vlastní podprostory téže dimenze a že tato vlastnost prostoru konečné dimenze charakterizuje; každý vektorový prostor nekonečné dimenze totiž obsahuje vlastní podprostory téže dimenze. V následující větě budeme prostory konečné dimenze charakterizovat jiným způsobem, který však s výše uvedeným úzce souvisí.

10.23. Věta. *Nechť V je vektorový prostor nad tělesem T . Následující tvrzení jsou ekvivalentní:*

- (i) *Prostor V má konečnou dimenzi.*
- (ii) *Každý injektivní endomorfismus prostoru V je automorfismem.*
- (iii) *Každý surjektivní endomorfismus prostoru V je automorfismem.*

Důkaz. Jestliže má prostor konečnou dimenzi, pak podle poznámky 10.21 platí (ii) a (iii).

Předpokládejme, že má prostor V nekonečnou dimenzi. Existuje tedy jeho vlastní podprostor V' , který má stejnou dimenzi (viz 8.22) a podle věty 10.22 existuje izomorfismus f prostoru V na prostor V' ; zobrazení f však můžeme chápat jako endomorfismus prostoru V , který je monomorfismem, ale není epimorfismem.

Rozšíříme-li nějakým způsobem izomorfismus f^{-1} podprostoru V' na prostor V na endomorfismus prostoru V , dostaneme surjektivní endomorfismus, který není monomorfismem. Neplatí-li tvrzení (i), neplatí tedy ani tvrzení (ii) ani tvrzení (iii).

Jiný důkaz: Nechť M je nějaká báze prostoru V nekonečné dimenze a necht' v_1, v_2, \dots jsou navzájem různé vektory báze M . Definujme endomorfismus f prostoru V určením obrazů vektorů báze M :

$$\begin{aligned} \forall i = 1, 2, \dots & \quad f(v_i) = v_{i+1}, \\ \forall v \in M, v \neq v_i & \quad f(v) = v. \end{aligned}$$

Zřejmě je f injektivním endomorfismem prostoru V , který není automorfismem (neboť $v_1 \notin \text{Im } f$).

Definujme dále endomorfismus g prostoru V takto:

$$\begin{aligned} g(v_1) &= 0, \\ \forall i = 2, 3, \dots & \quad g(v_i) = v_{i-1}, \\ \forall v \in M, v \neq v_i & \quad g(v) = v. \end{aligned}$$

Endomorfismus g je epimorfismus, ale není injektivní (neboť $v_1 \in \text{Ker } g$). \square

10.24. Důsledek. *Nechť α je libovolné kardinální číslo. Každý vektorový prostor dimenze α nad tělesem T je izomorfní s direktním součtem α exemplářů tělesa T .*

Důkaz. Tento fakt jsme dokázali v druhé části důkazu věty 10.22. \square

Všechny vektorové prostory nad tělesem T jsou tedy právě všechny direktní součty exemplářů tělesa T (a jejich izomorfní obrazy) a pro každé kardinální číslo α existuje (až na izomorfní obrazy) právě jediný vektorový prostor nad tělesem T , který má dimenzi α . Všechny vektorové prostory konečné dimenze nad tělesem T jsou tedy reprezentovány vektorovými prostory O, T, T^2, T^3, \dots .

10.25. Důsledek. *Dimenze prostoru \mathbb{R} všech reálných čísel nad tělesem \mathbb{Q} racionálních čísel je nekonečná.*

Důkaz. Pokud by dimenzí prostoru \mathbb{R} bylo přirozené číslo n , byl by prostor \mathbb{R} izomorfní s direktním součtem n exemplářů tělesa \mathbb{Q} . To však není možné, neboť množina \mathbb{R} je nespočetná a množina \mathbb{Q}^n spočetná. \square

10.26. Věta. *Izomorfismus vektorových prostorů je ekvivalence na třídě všech vektorových prostorů nad tělesem T .*

Důkaz. Každý prostor V je izomorfní sám se sebou (neboť 1_V je izomorfismus). Jestliže je prostor V izomorfní s prostorem W , pak je rovněž prostor W izomorfní s prostorem V (přejdeme k inverznímu izomorfismu). Jestliže je prostor U izomorfní s prostorem V a prostor V izomorfní s prostorem W , pak je i prostor U izomorfní s prostorem W (složení izomorfismů je izomorfismus). \square

Právě zmíněná ekvivalence určuje disjunktní rozklad třídy všech vektorových prostorů nad tělesem T na třídy navzájem izomorfních prostorů. Podle věty 10.22 je to rozklad na třídy vektorových prostorů stejné dimenze. Ke každému kardinálnímu číslu α existuje právě jediná takováto třída, ve které jsou právě všechny prostory nad tělesem T , které mají dimenzi α . Za reprezentanta této třídy můžeme považovat direktní součet α exemplářů tělesa T .

10.27. Věta. *Nechť V a W jsou vektorové prostory nad tělesem T . Množina $\text{Hom}(V, W)$ je podprostorem vektorového prostoru W^V .*

Důkaz. Připomeňme nejprve, že vektorový prostor W^V všech zobrazení prostoru V do prostoru W jsme definovali v příkladu 7.8(ix).

Množina $\text{Hom}(V, W)$ obsahuje nulový homomorfismus prostoru V do prostoru W a je tedy neprázdná. Zbývá dokázat, že je uzavřena vzhledem ke sčítání vektorů i vzhledem k násobení vektorů skaláry z tělesa T . Nechť $f, g \in \text{Hom}(V, W)$, $v, v_1, v_2 \in V$, $a, b \in T$. Nyní je

$$\begin{aligned}(f + g)(v_1 + v_2) &= f(v_1 + v_2) + g(v_1 + v_2) = f(v_1) + f(v_2) + g(v_1) + g(v_2) = \\ &= f(v_1) + g(v_1) + f(v_2) + g(v_2) = (f + g)(v_1) + (f + g)(v_2) .\end{aligned}$$

Při první a čtvrté rovnosti jsme užili definici sčítání zobrazení prostoru V do prostoru W (sčítání vektorů prostoru W^V), při druhé rovnosti jsme využili toho, že f a g jsou homomorfismy, při třetí rovnosti jsme užili komutativitu sčítání vektorů prostoru W . Obdobně je

$$(f + g)(av) = f(av) + g(av) = a \cdot f(v) + a \cdot g(v) = a \cdot (f(v) + g(v)) = a \cdot (f + g)(v) .$$

Součet $f + g$ homomorfismů f, g je tedy homomorfismus, tj. $f + g \in \text{Hom}(V, W)$. Dále je

$$\begin{aligned}(af)(v_1 + v_2) &= a \cdot f(v_1 + v_2) = a \cdot (f(v_1) + f(v_2)) = a \cdot f(v_1) + a \cdot f(v_2) = \\ &= (af)(v_1) + (af)(v_2) ,\end{aligned}$$

$$(af)(bv) = a \cdot f(bv) = a \cdot (b \cdot f(v)) = (ab) \cdot f(v) = (ba) \cdot f(v) = b \cdot (a \cdot f(v)) = b \cdot (af)(v) .$$

Násobek af homomorfismu f je tedy homomorfismus, tj. $af \in \text{Hom}(V, W)$.

Podmnožina $\text{Hom}(V, W)$ prostoru W^V je tedy uzavřená vzhledem ke sčítání vektorů (tj. homomorfismů) i vzhledem k násobení vektorů (tj. homomorfismů) skaláry a je tedy podprostorem prostoru W^V . \square

Popšimněme si, že při důkazu rovnosti $(af)(bv) = b \cdot (af)(v)$ jsme poprvé využili komutativitu násobení v tělese T .

10.28. Věta. *Nechť V je vektorový prostor nad tělesem T . Množina $\text{End } V$ se sčítáním a skládáním endomorfismů a násobením endomorfismů skaláry je lineární algebrou nad tělesem T , která má jednotkový prvek.*

Důkaz. Podle předchozí věty je množina $\text{End } V = \text{Hom}(V, V)$ se sčítáním endomorfismů a násobením endomorfismů skaláry vektorovým prostorem nad tělesem T . Skládání endomorfismů je asociativní, jednotkovým prvkem vzhledem

k této operaci je identický automorfismus. Zřejmě platí i oba distributivní zákony a vazba skládání endomorfismů a násobení endomorfismů skaláry: pro každé $f, g, h \in \text{End } V$ a $a \in T$ je

$$f(g + h) = fg + fh, \quad (f + g)h = fh + gh,$$

$$(af)g = a \cdot (fg) = f(ag).$$

Množina $\text{End } V$ s uvažovanými operacemi je tedy lineární algebrou nad tělesem T ; navíc má tato algebra jednotkový prvek 1_V . \square

10.29. Věta. *Nechť V je vektorový prostor nad tělesem T . Množina $\text{Aut } V$ s operací skládání automorfismů je grupa.*

Důkaz. Skládání automorfismů prostoru V je asociativní binární operace na množině $\text{Aut } V$, identický automorfismus 1_V je jednotkovým prvkem, inverzním prvkem k automorfismu f je inverzní automorfismus f^{-1} . \square

Uvědomme si, že součet dvou automorfismů prostoru V nemusí být automorfismem; triviálním příkladem je rovnost $f + (-f) = 0$. Podmnožina $\text{Aut } V$ prostoru (resp. lineární algebry) $\text{End } V$ tedy není uzavřena vzhledem ke sčítání.

Skládání endomorfismů (automorfismů) prostoru V není komutativní. Jestliže pro endomorfismy $f, g \in \text{End } V$ platí rovnost $fg = gf$, potom říkáme, že f a g komutují, nebo že jsou *záměnné*.

V závěru tohoto paragrafu uvedeme definici homomorfismu lineárních algeber a několik příkladů.

10.30. Definice. Nechť V a W jsou lineární algebry nad tělesem T . Zobrazení f algebry V do algebry W se nazývá *homomorfismus*, jestliže

- (i) $\forall x, y \in V \quad f(x + y) = f(x) + f(y)$,
- (ii) $\forall x, y \in V \quad f(xy) = f(x) \cdot f(y)$,
- (iii) $\forall x \in V \quad \forall a \in T \quad f(ax) = a \cdot f(x)$.

Jestliže je homomorfismus f injektivní, resp. surjektivní, resp. bijektivní, nazývá se *monomorfismus*, resp. *epimorfismus*, resp. *izomorfismus*.

Jestliže existuje izomorfismus lineární algebry V na lineární algebru W , pak říkáme, že jsou algebry V a W *izomorfní* a píšeme $V \cong W$.

10.31. Příklady.

(i) Zobrazení reálné algebry \mathbb{C} všech komplexních čísel do reálné lineární algebry \mathbb{H} všech kvaternionů, které každému komplexnímu číslu $a + bi$ přiřazuje kvaternion $a + bi$, je monomorfismus lineární algebry \mathbb{C} do lineární algebry \mathbb{H} .

Zobrazení g algebry \mathbb{H} do algebry \mathbb{C} , které každému kvaternionu $a + bi + cj + dk$ přiřazuje komplexní číslo $a + bi$, je epimorfismus.

(ii) Zobrazení f lineární algebry \mathbb{H} všech kvaternionů do lineární algebry $\mathbb{C}^{2 \times 2}$ čtvercových komplexních matic řádu 2, které každému kvaternionu $a+bi+cj+dk$ přiřazuje matici

$$\begin{pmatrix} a + di & b + ci \\ -b + ci & a - di \end{pmatrix}$$

je monomorfismus algebry \mathbb{H} do algebry $\mathbb{C}^{2 \times 2}$. Množina všech matic výše uvedeného typu, tj. $\text{Im } f$, je podalgebrou algebry $\mathbb{C}^{2 \times 2}$.

Další příklady poznáme později.

III. MATICE

11. MATICOVÁ REPREZENTACE HOMOMORFISMŮ

V tomto paragrafu budeme vyšetřovat jen vektorové prostory konečné dimenze. Jejich báze budeme vždy chápat jako úplně uspořádané množiny; tato uspořádání budou určena indexováním vektorů přirozenými čísly. V následujících definicích a větách tyto předpoklady již nebudeme uvádět.

Nechť f je homomorfismus vektorového prostoru V do vektorového prostoru W . Nechť $M = \{v_1, \dots, v_m\}$ je báze prostoru V a $N = \{w_1, \dots, w_n\}$ báze prostoru W . Obrazy $f(v_1), \dots, f(v_m)$ vektorů v_1, \dots, v_m báze M vyjádříme souřadnicemi vzhledem k bázi N :

$$\begin{aligned} \langle f(v_1) \rangle_N &= (a_{11}, a_{21}, \dots, a_{n1}), & \text{tj.} & \quad f(v_1) = \sum_{i=1}^n a_{i1} w_i, \\ & \dots & & \quad \dots \\ \langle f(v_j) \rangle_N &= (a_{1j}, a_{2j}, \dots, a_{nj}), & \text{tj.} & \quad f(v_j) = \sum_{i=1}^n a_{ij} w_i, \\ & \dots & & \quad \dots \\ \langle f(v_m) \rangle_N &= (a_{1m}, a_{2m}, \dots, a_{nm}), & \text{tj.} & \quad f(v_m) = \sum_{i=1}^n a_{im} w_i. \end{aligned}$$

Homomorfismu f nyní přiřadíme matici

$$\begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1m} \\ a_{21} & \dots & a_{2j} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nm} \end{pmatrix}$$

typu $n \times m$, tzv. matici homomorfismu f vzhledem k bázím M, N . V jejím j -tém sloupci ($j = 1, \dots, m$) jsou souřadnice obrazu j -tého vektoru báze M vzhledem k bázi N .

11.1. Definice. Nechť V a W jsou vektorové prostory dimenzí m a n nad tělesem T a f je homomorfismus prostoru V do prostoru W . Nechť $M = \{v_1, \dots, v_m\}$ je báze prostoru V a N báze prostoru W . *Maticí homomorfismu f vzhledem k bázím M, N budeme rozumět matici typu $n \times m$ nad tělesem T , ve které na místě ij stojí i -tá souřadnice vektoru $f(v_j)$ vzhledem k bázi N .*

Maticí endomorfismu g prostoru V vzhledem k bázi M budeme rozumět matici homomorfismu g prostoru V do prostoru V vzhledem k bázím M, M .

Jsou-li tedy dány báze M, N prostorů V, W , pak každému homomorfismu prostoru V do prostoru W je přiřazena jistá matice. Tato matice homomorfismu f určuje, jak ukazuje následující věta.

11.2. Věta. *Nechť V a W jsou vektorové prostory dimenzí m a n nad tělesem T a M, N báze těchto prostorů. Nechť f je homomorfismus prostoru V do prostoru W a A matice typu $n \times m$ nad tělesem T . Matice A je maticí homomorfismu f vzhledem k bázím M, N právě tehdy, když pro každý vektor $v \in V$ je*

$$\langle f(v) \rangle_N^T = A \cdot \langle v \rangle_M^T. \quad (1)$$

Důkaz. Pišme $M = \{v_1, \dots, v_m\}$, $N = \{w_1, \dots, w_n\}$ a $A = (a_{ij})$. Předpokládejme nejprve, že A je matice homomorfismu f vzhledem k bázím M, N . Pro každé $j = 1, \dots, m$ je tedy

$$f(v_j) = \sum_{i=1}^n a_{ij} w_i.$$

Nechť v je libovolný vektor prostoru V ; vyjádřeme jej souřadnicemi vzhledem k bázi M :

$$\langle v \rangle_M = (b_1, \dots, b_m), \quad \text{tj.} \quad v = \sum_{j=1}^m b_j v_j.$$

Odtud

$$f(v) = \sum_{j=1}^m b_j f(v_j) = \sum_{j=1}^m b_j \left(\sum_{i=1}^n a_{ij} w_i \right) = \sum_{i=1}^n \left(\sum_{j=1}^m a_{ij} b_j \right) \cdot w_i,$$

tj.

$$\langle f(v) \rangle_N = \left(\sum_{j=1}^m a_{1j} b_j, \dots, \sum_{j=1}^m a_{nj} b_j \right).$$

Dokázali jsme tedy, že součin matice A s maticí $\langle v \rangle_M^T$ je roven matici $\langle f(v) \rangle_N^T$; rovnost (1) tedy platí.

Předpokládejme naopak, že pro každý vektor $v \in V$ platí rovnost (1). Jestliže je B matice homomorfismu f vzhledem k bázím M, N , potom (podle právě dokázané implikace) je pro každý vektor $v \in V$

$$\langle f(v) \rangle_N^T = B \cdot \langle v \rangle_M^T. \quad (2)$$

Porovnáním rovností (1) a (2) vidíme, že pro každý vektor $v \in V$ je

$$A \cdot \langle v \rangle_M^T = B \cdot \langle v \rangle_M^T.$$

Po dosazení vektoru v_1 (první vektor báze M) tato rovnost přejde v rovnost prvních sloupců matic A a B . Postupným dosazením vektorů v_1, \dots, v_m tak dojdeme k rovnosti matic A a B . Matice A je tedy maticí homomorfismu f vzhledem k bázím M, N . \square

11.3. Příklady.

(i) Homomorfismus f prostoru \mathbb{R}^3 do prostoru \mathbb{R}^4 zobrazuje vektor (x, y, z) na vektor $(x + y, y + z, x + z, x)$. Najdeme matici tohoto homomorfismu vzhledem ke kanonickým bázím prostorů \mathbb{R}^3 a \mathbb{R}^4 .

Vektory $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ se homomorfismem f zobrazí po řadě na vektory $(1, 0, 1, 1)$, $(1, 1, 0, 0)$, $(0, 1, 1, 0)$; souřadnice těchto vektorů vzhledem ke kanonické bázi jsou tytéž čtveřice. Maticí homomorfismu f vzhledem ke kanonickým bázím je tedy matice

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Rovnost (1) z věty 11.2 má v tomto konkrétním případě tvar

$$\begin{pmatrix} x + y \\ y + z \\ x + z \\ x \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

tj. odpovídá předpisu, kterým je homomorfismus f definován.

Najdeme nyní matici homomorfismu f vzhledem k bázím

$$M = \{(1, 1, 0), (1, 0, 1), (0, -1, 0)\},$$

$$N = \{(1, 1, 0, 1), (1, 0, 0, 0), (0, 1, 1, 0), (0, 1, 1, 1)\}.$$

Vektory báze M se při f zobrazí na vektory $(2, 1, 1, 1)$, $(1, 1, 2, 1)$, $(-1, -1, 0, 0)$. Tyto vektory musíme vyjádřit souřadnicemi vzhledem k bázi N ; někdy je možno příslušné souřadnice uhodnout, jindy je třeba je vypočítat, např. pomocí soustavy lineárních rovnic. V našem případě je

$$(2, 1, 1, 1) = 2 \cdot (1, 0, 0, 0) + (0, 1, 1, 1),$$

$$(1, 1, 2, 1) = -(1, 1, 0, 1) + 2 \cdot (1, 0, 0, 0) + 2 \cdot (0, 1, 1, 1),$$

$$(-1, -1, 0, 0) = -(1, 1, 0, 1) - (0, 1, 1, 0) + (0, 1, 1, 1).$$

Maticí homomorfismu f vzhledem k bázím M, N je tedy matice

$$B = \begin{pmatrix} 0 & -1 & -1 \\ 2 & 2 & 0 \\ 0 & 0 & -1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Rovnost (1) z věty 11.2 má tvar

$$\begin{pmatrix} -b - c \\ 2a + 2b \\ -c \\ a + 2b + c \end{pmatrix} = \begin{pmatrix} 0 & -1 & -1 \\ 2 & 2 & 0 \\ 0 & 0 & -1 \\ 1 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix};$$

tato rovnost definuje homomorfismus f v souřadnicích vzhledem k bázím M, N .

(ii) Maticí identického automorfismu 1_V prostoru V vzhledem k libovolné bázi prostoru V je jednotková matice.

(iii) Endomorfismus f prostoru všech polynomů stupně nejvýše 5 s reálnými koeficienty, který každému polynomu přiřazuje jeho derivaci, má vzhledem k bázi $\{1, x, x^2, x^3, x^4, x^5\}$ matici

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Vzhledem k bázi

$$\{1, 1+x, 1+x+x^2, 1+x+x^2+x^3, 1+x+x^2+x^3+x^4, 1+x+x^2+x^3+x^4+x^5\}$$

má tento endomorfismus matici

$$\begin{pmatrix} 0 & 1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 2 & -1 & -1 & -1 \\ 0 & 0 & 0 & 3 & -1 & -1 \\ 0 & 0 & 0 & 0 & 4 & -1 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

11.4. Věta. *Nechť U, V, W jsou vektorové prostory nad tělesem T a K, M, N po řadě jejich báze, nechť f je homomorfismus prostoru V do prostoru W a nechť g je homomorfismus prostoru U do prostoru V . Jestliže A je maticí homomorfismu f vzhledem k bázím M, N a B maticí homomorfismu g vzhledem k bázím K, M , potom je součin AB maticí homomorfismu fg vzhledem k bázím K, N .*

Tvrzení věty 11.4 je spjato s následujícím schématem:

$$\begin{array}{ccccc} & & \overbrace{\hspace{10em}}^{fg} & & \\ & & \underbrace{\hspace{10em}}_{AB} & & \\ W & \xleftarrow{f} & V & \xleftarrow{g} & U \\ N & & M & & K \end{array}$$

V takovýchto schématech kreslíme šipky zprava doleva, neboť při skládání homomorfismů zapisujeme jednotlivé symboly také zprava doleva (nejprve se provádí g a potom f).

Důkaz. Podle předchozí věty (užijeme ji dvakrát: nejprve pro f a pak pro g) je pro každý vektor $u \in U$

$$\langle (fg)(u) \rangle_N^T = \langle f(g(u)) \rangle_N^T = A \cdot \langle g(u) \rangle_M^T = A \cdot (B \cdot \langle u \rangle_K^T) = (AB) \cdot \langle u \rangle_K^T.$$

Znovu podle předchozí věty (tentokrát využijeme opačné implikace) je matice AB maticí homomorfismu fg vzhledem k bázím K, N . \square

11.5. Důsledek. *Nechť V a W jsou vektorové prostory téže dimenze, M, N jejich báze, f je izomorfismus prostoru V do prostoru W a A matice homomorfismu f vzhledem k bázím M, N . Matice A je invertibilní, právě když je f izomorfismus; matice A^{-1} je potom maticí izomorfismu f^{-1} vzhledem k bázím N, M .*

Důkaz. Nechť f je izomorfismus a B matice izomorfismu f^{-1} vzhledem k bázím N, M . Podle předchozí věty je AB maticí identického automorfismu 1_W vzhledem k bázi N a BA maticí identického automorfismu 1_V vzhledem k bázi M . Podle 11.3(ii) je $AB = BA = E$, tj. $B = A^{-1}$.

Nechť A je invertibilní a g homomorfismus prostoru W do prostoru V , jehož maticí vzhledem k bázím N, M je matice A^{-1} . Podle předchozí věty je $E = A \cdot A^{-1}$ maticí endomorfismu fg prostoru W vzhledem k bázi N a $E = A^{-1}A$ maticí endomorfismu gf prostoru V vzhledem k bázi M . Proto je $fg = 1_W$ a $gf = 1_V$, tj. f je izomorfismus. \square

11.6. Definice. Nechť V je vektorový prostor a M, N jeho dvě báze. *Maticí přechodu od báze M k bázi N budeme rozumět matici identického automorfismu prostoru V vzhledem k bázím M, N .*

11.7. Transformace souřadnic. *Nechť M, N jsou báze prostoru V . Jestliže je A maticí přechodu od báze M k bázi N , potom pro každý vektor $v \in V$ je*

$$\langle v \rangle_N^T = A \cdot \langle v \rangle_M^T. \quad (3)$$

Důkaz. Tvrzení ihned vyplývá z věty 11.2 a definice matice přechodu 11.6. \square

V literatuře najdeme pro matici A definovanou v 11.6 obvykle termín *matice přechodu od báze N k bázi M* . Je to proto, že ve sloupcích matice A jsou souřadnice vektorů báze M vzhledem k bázi N ; známe-li tedy bázi N a matici A , vypočteme snadno vektory báze M ; od báze N tedy „přejdeme“ k bázi M . My jsme zavedli pro matici A méně obvyklý termín *matice přechodu od báze M k bázi N* ze dvou důvodů:

- Matice A slouží k přechodu od souřadnic vzhledem k bázi M k souřadnicím vzhledem k bázi N (viz vzorec (3)).
- Slovní spojení „od báze M k bázi N “ vyjadřuje směr šipky identického automorfismu, jehož je A maticí:

$$\begin{array}{ccc} V & \xleftarrow{1_V} & V \\ N & & M \\ & & A \end{array}$$

Následující tvrzení vyplývají z 11.4 a 11.5.

11.8. Důsledky.

- (i) Matice A přechodu od báze M k bázi N je rovna součinu BC matice B přechodu od báze K k bázi N a matice C přechodu od báze M k bázi K .
- (ii) Každá matice přechodu je invertibilní. Jestliže A je maticí přechodu od báze M k bázi N , potom je A^{-1} maticí přechodu od báze N k bázi M . Jestliže je tedy pro každý vektor $v \in V$

$$\langle v \rangle_N^T = A \cdot \langle v \rangle_M^T,$$

potom je

$$\langle v \rangle_M^T = A^{-1} \cdot \langle v \rangle_N^T. \quad \square$$

11.9. Příklad. Uvažujme báze

$$M = \{(2, 1, 1), (1, 2, 1), (1, 1, 2)\}, \quad N = \{(1, 1, 1), (1, 1, 0), (1, 0, 0)\}$$

vektorového prostoru \mathbb{Z}_5^3 . Vektory báze M vyjádříme pomocí vektorů báze N takto:

$$\begin{aligned} (2, 1, 1) &= (1, 1, 1) + (1, 0, 0), \\ (1, 2, 1) &= (1, 1, 1) + (1, 1, 0) + 4 \cdot (1, 0, 0), \\ (1, 1, 2) &= 2 \cdot (1, 1, 1) + 4 \cdot (1, 1, 0). \end{aligned}$$

Matice přechodu od báze M k bázi N tedy vypadá takto:

$$A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 4 \\ 1 & 4 & 0 \end{pmatrix}$$

Matici A jsme mohli získat též jako součin BC , kde B je matice přechodu od kanonické báze k bázi N a C je matice přechodu od báze M ke kanonické bázi (viz 11.4, resp. 11.8(i)):

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 4 \\ 1 & 4 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

Jsou-li (x, y, z) souřadnice vektoru $v \in \mathbb{Z}_5^3$ vzhledem k bázi M , jsou

$$(x + y + 2z, y + 4z, x + 4y)$$

souřadnice tohoto vektoru vzhledem k bázi N ; tuto skutečnost zjistíme užitím vzorce (3).

Vyjádřeme ještě vektory báze N pomocí vektorů báze M :

$$\begin{aligned}(1, 1, 1) &= 4 \cdot (2, 1, 1) + 4 \cdot (1, 2, 1) + 4 \cdot (1, 1, 2), \\(1, 1, 0) &= 3 \cdot (2, 1, 1) + 3 \cdot (1, 2, 1) + 2 \cdot (1, 1, 2), \\(1, 0, 0) &= 2 \cdot (2, 1, 1) + (1, 2, 1) + (1, 1, 2).\end{aligned}$$

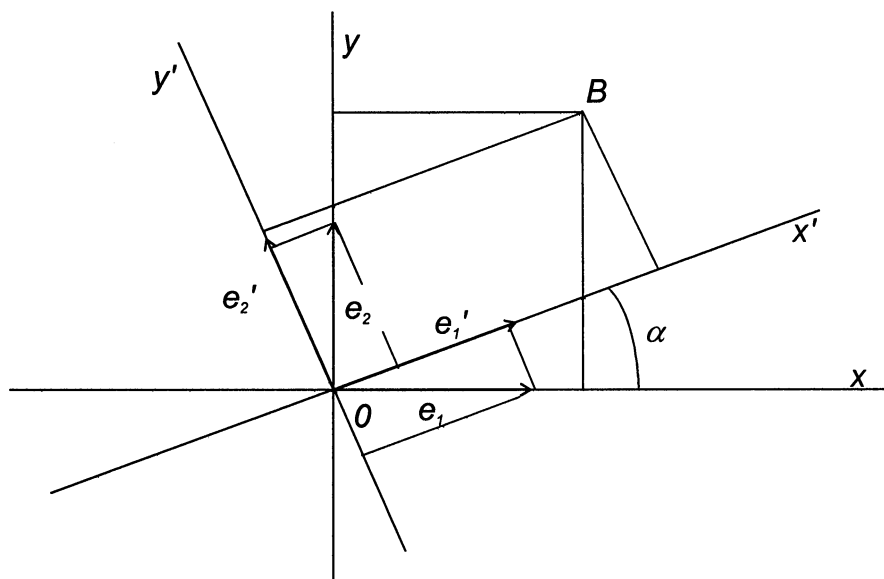
Maticí přechodu od báze N k bázi M je tedy matice

$$\begin{pmatrix} 4 & 3 & 2 \\ 4 & 3 & 1 \\ 4 & 2 & 1 \end{pmatrix};$$

snadno se přesvědčíme, že jde o matici A^{-1} . Tuto matici můžeme získat též jako součin matice přechodu od kanonické báze k bázi M a matice přechodu od báze N ke kanonické bázi (jde o matice C^{-1} a B^{-1}):

$$C^{-1} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

(Povšimněme si, že matice C je sama k sobě inverzní.) Jsou-li (a, b, c) souřadnice vektoru $v \in \mathbb{Z}_5^3$ vzhledem k bázi N , jsou $(4a + 3b + 2c, 4a + 3b + c, 4a + 2b + c)$ souřadnice tohoto vektoru vzhledem k bázi M .



11.10. Příklad. Mějme v rovině dvě kartézské soustavy souřadnic se společným počátkem O . Vzájemný vztah těchto soustav S a S' je určen úhlem α ; říkáme též,

že soustava S' vznikla otočením soustavy S kolem počátku O o úhel α . Chceme určit vztah souřadnic vzhledem k soustavám S a S' . Označme (x, y) souřadnice libovolně zvoleného bodu B vzhledem k soustavě S a (x', y') souřadnice tohoto bodu vzhledem k soustavě S' . Jde vlastně o souřadnice vektoru \overrightarrow{OB} vzhledem k bázi $\{e_1, e_2\}$ a vzhledem k bázi $\{e'_1, e'_2\}$, kde e_1, e_2, e'_1, e'_2 jsou jednotkové vektory ležící na příslušných osách. Vztah nečárkovaných a čárkovaných souřadnic se velmi snadno určí pomocí vzorce (3) pro transformaci souřadnic. Souřadnice vektorů e_1, e_2 vzhledem k bázi $\{e'_1, e'_2\}$ získáme promítnutím těchto vektorů na osy souřadnicové soustavy S' :

$$e_1 = \cos \alpha \cdot e'_1 - \sin \alpha \cdot e'_2, \quad e_2 = \sin \alpha \cdot e'_1 + \cos \alpha \cdot e'_2.$$

Maticí přechodu od báze $\{e_1, e_2\}$ k bázi $\{e'_1, e'_2\}$ je tedy matice

$$A = \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix}.$$

Užitím vzorce (3) nyní získáme vzorce pro transformaci souřadnic:

$$\begin{aligned} x' &= \cos \alpha \cdot x + \sin \alpha \cdot y, \\ y' &= -\sin \alpha \cdot x + \cos \alpha \cdot y. \end{aligned}$$

Podobně je matice

$$A^{-1} = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

maticí přechodu od báze $\{e'_1, e'_2\}$ k bázi $\{e_1, e_2\}$ a tedy

$$\begin{aligned} x &= \cos \alpha \cdot x' - \sin \alpha \cdot y', \\ y &= \sin \alpha \cdot x' + \cos \alpha \cdot y'. \end{aligned}$$

Později se dozvíme, proč je v tomto případě $A^{-1} = A^T$.

11.11. Věta. *Nechť V, W jsou vektorové prostory, M, M' , resp. N, N' dvě báze prostoru V , resp. W a f homomorfismus prostoru V do prostoru W . Jestliže A je maticí homomorfismu f vzhledem k bázím M, N a jestliže B je maticí přechodu od báze N' k bázi N a C maticí přechodu od báze M' k bázi M , potom je $B^{-1}AC$ maticí homomorfismu f vzhledem k bázím M', N' .*

Důkaz. Vyjádříme-li homomorfismus f jako složení tří homomorfismů $f = 1_W f 1_V$, pak podle věty 11.4 a důsledku 11.5 dostáváme, že maticí f vzhledem k bázím M', N' je matice $B^{-1}AC$. \square

Tvrzení věty i její důkaz se snadno pamatuje pomocí následujícího schématu:

$$\begin{array}{ccccccc}
 & & \overbrace{\hspace{10em}}^f & & & & \\
 W & \xleftarrow{1_W} & W & \xleftarrow{f} & V & \xleftarrow{1_V} & V \\
 N' & & N & & M & & M' \\
 & & \underbrace{\hspace{10em}}_{B^{-1}AC} & & & & \\
 & & B^{-1} & & A & & C
 \end{array}$$

Uvědomme si, že matice B^{-1} je maticí přechodu od báze N k bázi N' . Matici homomorfismu f vzhledem k bázím M', N' je tedy možno vyjádřit jako součin DAC , kde D je matice přechodu od báze N k bázi N' a C je matice přechodu od báze M' k bázi M . Formulaci uvedené ve větě 11.11 jsme dali přednost proto, že z ní v případě $V = W$, $M = N$ a $M' = N'$ vyplývá následující užitečné tvrzení o změně matice endomorfismu.

Jestliže A je maticí endomorfismu f prostoru V vzhledem k bázi M , potom maticí tohoto endomorfismu vzhledem k bázi M' je matice $B^{-1}AB$, kde B je maticí přechodu od báze M' k bázi M .

Matice A a $B^{-1}AB$ jsou tedy maticemi téhož endomorfismu (vzhledem k různým bázím); takovéto matice se nazývají *podobné*. Pojmeme podobnosti matic se budeme zabývat později.

11.12. Příklad. V příkladu 11.3(i) jsme našli matici A homomorfismu f vzhledem ke kanonickým bázím a matici B tohoto homomorfismu vzhledem k bázím M, N . Matici B však můžeme podle věty 11.11 (resp. podle následující poznámky) získat také tak, že matici A vynásobíme zleva maticí přechodu od kanonické báze k bázi N a zprava maticí přechodu od báze M ke kanonické bázi. Přesvědčte se, že je opravdu

$$B = \begin{pmatrix} 0 & 1 & -1 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & -1 & 1 & 1 \end{pmatrix} \cdot A \cdot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} .$$

11.13. Věta. *Nechť V a W jsou vektorové prostory nad tělesem T , které mají dimenze m, n . Vektorový prostor $\text{Hom}(V, W)$ je izomorfní s prostorem $T^{n \times m}$; dimenze prostoru $\text{Hom}(V, W)$ je mn .*

Důkaz. Zvolme báze $M = \{v_1, \dots, v_m\}$, resp. $N = \{w_1, \dots, w_n\}$ prostorů V , resp. W a označme Φ zobrazení prostoru $\text{Hom}(V, W)$ do prostoru $T^{n \times m}$, které každému homomorfismu prostoru V do prostoru W přiřadí jeho matici vzhledem k bázím M, N . Zobrazení Φ je injektivní: dva různé homomorfismy prostoru V do prostoru W nemohou mít totiž podle 11.2 stejnou matici vzhledem k bázím M, N .

Každá matice A typu $n \times m$ reprezentuje m vektorů prostoru W (ve sloupcích jsou jejich souřadnice vzhledem k bázi N). Podle věty 10.7 existuje homomorfismus, který zobrazuje vektory báze M po řadě na těchto m vektorů prostoru W . Tento homomorfismus má vzhledem k bázím M, N matici A . Zobrazení Φ je tedy také surjektivní.

Dokážeme, že Φ je homomorfismus. Předpokládejme, že homomorfismy f, g prostoru V do prostoru W mají vzhledem k bázím M, N po řadě matice $A = (a_{ij})$, $B = (b_{ij})$. Pro každé $j = 1, \dots, m$ je tedy

$$(f + g)(v_j) = f(v_j) + g(v_j) = \sum_{i=1}^n a_{ij} w_i + \sum_{i=1}^n b_{ij} w_i = \sum_{i=1}^n (a_{ij} + b_{ij}) w_i ,$$

takže homomorfismus $f + g$ má vzhledem k bázím M, N matici $A + B$. Pro libovolné $c \in T$ a $j = 1, \dots, m$ je

$$(cf)(v_j) = c \cdot f(v_j) = c \cdot \sum_{i=1}^n a_{ij} w_i = \sum_{i=1}^n (ca_{ij}) w_i ,$$

takže homomorfismus cf má vzhledem k bázím M, N matici cA . Zobrazení Φ je tedy izomorfismus. Podle věty 10.22 je tedy

$$\dim \text{Hom}(V, W) = \dim T^{n \times m} = mn . \quad \square$$

11.14. Věta. *Nechť V je vektorový prostor dimenze n nad tělesem T . Potom platí:*

- (i) *Lineární algebra $\text{End } V$ je izomorfní s lineární algebrou $T^{n \times n}$.*
- (ii) *Grupa $\text{Aut } V$ je izomorfní s grupou $\text{GL}(n)$.*

Důkaz. Zvolme bázi M prostoru V a označme Φ zobrazení algebry $\text{End } V$ do algebry $T^{n \times n}$, které každému endomorfismu prostoru V přiřazuje jeho matici vzhledem k bázi M . Podle předchozí věty je Φ izomorfismus prostoru $\text{End } V$ na prostor $T^{n \times n}$. Podle věty 11.4 však Φ zobrazuje složení dvou endomorfismů na součin jejich matic, tj. platí rovnost

$$\Phi(fg) = \Phi(f) \cdot \Phi(g) .$$

Zobrazení Φ je tedy izomorfismus lineárních algeber.

Jestliže je f automorfismus prostoru V , je $\Phi(f)$ invertibilní matice podle důsledku 11.5. Jestliže je naopak A invertibilní matice a f, g endomorfismy prostoru V , jejichž maticemi vzhledem k bázi M jsou matice A, A^{-1} (tj. $\Phi(f) = A$, $\Phi(g) = A^{-1}$), potom je

$$\Phi(fg) = \Phi(f) \cdot \Phi(g) = A \cdot A^{-1} = E .$$

Podle věty 11.2 (viz též 11.3(ii)) je $fg = 1_V$, tj. f je automorfismus.

Při zobrazení Φ si tedy vzájemně jednoznačně odpovídají automorfismy prostoru V a invertibilní matice algebry $T^{n \times n}$. Vzhledem k tomu, že zobrazení Φ převádí složení automorfismů v součin jejich matic, dostáváme zúžením zobrazení Φ izomorfismus grupy $\text{Aut } V$ na grupu $\text{GL}(n)$. \square

12. HODNOST MATICE, ELEMENTÁRNÍ ÚPRAVY

Nechť A je matice typu $n \times m$ nad tělesem T . Na řádky matice A se budeme často dívat jako na vektory prostoru T^m a na sloupce matice A jako na vektory prostoru T^n . V tomto smyslu budeme mluvit o nulovém řádku nebo sloupci, o vynásobení nějakého řádku nebo sloupce prvkem $b \in T$, o přičtení b -násobku nějakého řádku (sloupce) k jinému řádku (sloupci), o lineární závislosti či nezávislosti řádků (sloupců), o dimenzi podprostoru prostoru T^n generovaného sloupci matice A (resp. podprostoru prostoru T^m generovaného řádky matice A) apod.

12.1. Definice. Nechť A je matice typu $n \times m$ nad tělesem T . *Hodností* $r(A)$ matice A budeme rozumět dimenzi vektorového prostoru generovaného sloupci matice A (jako vektory prostoru T^n).

Hodnost $r(A)$ matice A typu $n \times m$ je tedy rovna maximálnímu počtu lineárně nezávislých sloupců matice A . (Později uvidíme, že se obdobným způsobem vyjádří hodnost matice pomocí řádků — viz 12.27.) Hodnost matic můžeme proto zjišťovat stejným způsobem, jako dimenzi lineárního obalu daných vektorů prostoru T^n (viz 7.14(viii) a 8.20).

12.2. Definice. Čtvercová matice se nazývá *regulární*, jestliže je její hodnost rovna jejímu řádu; v opačném případě, tj. když je její hodnost menší než její řád, se nazývá *singulární*.

Sloupce regulární matice jsou tedy lineárně nezávislé a tvoří bázi prostoru T^n ; sloupce singulární matice jsou lineárně závislé.

12.3. Příklady. Hodnost diagonální matice je rovna počtu jejích nenulových prvků; nenulové sloupce diagonální matice jsou totiž lineárně nezávislé. Hodnost jednotkové matice řádu n je rovna n ; každá jednotková matice je regulární. Hodnost nulové matice je rovna nule. Výše zmíněnou metodou pro zjištění dimenze podprostoru (viz 7.14(viii) a 8.20) více nebo méně snadno ověříme, že hodnost reálných matic

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 2 \\ 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

je po řadě 3, 2, 4 a že hodnost matic

$$\begin{pmatrix} 1 & 3 & 4 & 2 \\ 3 & 2 & 0 & 1 \\ 2 & 2 & 4 & 4 \end{pmatrix}, \quad \begin{pmatrix} 2 & 3 & 4 & 1 \\ 6 & 1 & 2 & 3 \\ 3 & 2 & 4 & 5 \\ 4 & 6 & 1 & 3 \end{pmatrix}$$

nad tělesem \mathbb{Z}_5 , resp. \mathbb{Z}_7 je 2, resp. 4; třetí a pátá matice jsou tedy regulární, ostatní jsou singulární.

12.4. Věta. *Nechť V a W jsou vektorové prostory konečných dimenzí nad tělesem T a M, N jejich báze. Jestliže f je homomorfismus prostoru V do prostoru W a A jeho matice vzhledem k bázím M, N , potom je hodnota matice A rovna hodnotě homomorfismu f .*

Důkaz. Pišme $M = \{v_1, \dots, v_m\}$; necht' $\dim W = n$. Zřejmě je

$$r(f) = \dim \operatorname{Im} f = \dim [f(v_1), \dots, f(v_m)]$$

(viz 10.4(vi)). Při izomorfismu prostoru W na prostor T^n , který vektorům prostoru W přiřazuje jejich souřadnice vzhledem k bázi N , se vektory $f(v_1), \dots, f(v_m)$ zobrazí po řadě na sloupce matice A . Tedy $\dim [f(v_1), \dots, f(v_m)] = r(A)$ a proto $r(f) = r(A)$. \square

Tvrzení věty 12.4 jde stručně vyjádřit takto: Hodnota homomorfismu je rovna hodnotě jeho matice. Z tohoto zjištění ihned plyne, že všechny matice daného homomorfismu — utvořené vzhledem ke všem možným dvojicím bází — mají stejnou hodnotu.

12.5. Důsledek. *Čtvercová matice je regulární právě tehdy, když je invertibilní.*

Důkaz. Necht' A je čtvercová matice řádu n nad tělesem T ; matice A je maticí nějakého endomorfismu f prostoru T^n vzhledem ke kanonické bázi. Matice A je invertibilní právě tehdy, když je f automorfismus (viz 11.5), tj. právě tehdy, když je f epimorfismus (viz 10.23), tj. když $r(f) = n$. Podle předchozí věty je tedy A invertibilní právě tehdy, když je $r(A) = n$, tj. když je A regulární. \square

Izomorfismům vektorových prostorů tedy odpovídají regulární matice a regulárním maticím odpovídají izomorfismy. Všechny matice přechodu jsou regulární. Součin regulárních matic je opět regulární matice (viz 4.14).

12.6. Věta. *Nechť A, B, C jsou matice nad tělesem T ; matice A je typu $n \times m$, B je regulární matice řádu n a C je regulární matice řádu m . Potom je hodnota matice BAC rovna hodnotě matice A .*

Důkaz. Necht' V a W jsou vektorové prostory nad tělesem T , které mají po řadě dimenze m a n . Necht' M, N jsou báze prostorů V a W . Matice A je maticí nějakého homomorfismu f prostoru V do prostoru W vzhledem k bázím M, N . Matice B je maticí nějakého endomorfismu g prostoru W vzhledem k bázi N a matice C je maticí nějakého endomorfismu h prostoru V vzhledem k bázi M :

$$\begin{array}{ccccccc} W & \xleftarrow{g} & W & \xleftarrow{f} & V & \xleftarrow{h} & V \\ N & & N & & M & & M \\ & & B & & A & & C \end{array}$$

Protože jsou matice B a C regulární, jsou g a h automorfismy, takže

$$\dim \operatorname{Im} f = \dim \operatorname{Im} gfh .$$

Je tedy $r(f) = r(gfh)$ a podle věty 12.4 je $r(A) = r(BAC)$. \square

12.7. Věta. *Nechť A, B jsou matice typů $n \times m$ a $m \times k$ nad tělesem T . Potom je*

$$r(A) + r(B) - m \leq r(AB) \leq \min(r(A), r(B)) .$$

Důkaz. Nechť U, V, W jsou vektorové prostory nad tělesem T , které mají po řadě dimenze k, m, n ; nechť K, M, N jsou nějaké báze těchto prostorů. Matice A je maticí nějakého homomorfismu f prostoru V do prostoru W vzhledem k bázím M, N a matice B je maticí nějakého homomorfismu g prostoru U do prostoru V vzhledem k bázím K, M :

$$\begin{array}{ccccc} W & \xleftarrow{f} & V & \xleftarrow{g} & U \\ N & & M & & K \\ & & A & & B \end{array}$$

Zřejmě je $r(fg) \leq r(f)$ a $r(fg) \leq r(g)$, takže podle věty 12.4 je

$$r(AB) \leq r(A) \quad \text{a} \quad r(AB) \leq r(B) .$$

Tím je dokázána jedna nerovnost.

Podle věty o hodnotě a defektu je

$$\begin{aligned} m &= r(f) + d(f) , \\ k &= r(g) + d(g) , \\ k &= r(fg) + d(fg) . \end{aligned}$$

Odečteme-li třetí rovnost od součtu první a druhé, dostaneme rovnost

$$m = r(f) + r(g) - r(fg) + d(f) + d(g) - d(fg) .$$

Protože je podle 10.20 $d(f) + d(g) - d(fg) \geq 0$, je

$$m - r(f) - r(g) + r(fg) \geq 0$$

a tedy

$$r(f) + r(g) - m \leq r(fg) .$$

Odtud vyplývá nerovnost $r(A) + r(B) - m \leq r(AB)$. \square

12.8. Příklad. Matice

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

nad tělesem T mají hodnotu 1. Je $AB = O$, $AA = A$, takže

$$r(AB) = 0 < 1 = \min(r(A), r(B)),$$

$$r(A) + r(A) - 2 = 0 < 1 = r(AA).$$

Nerovnosti v předchozí větě tedy mohou být ostré.

V maticovém počtu i jeho aplikacích mají velký význam tzv. elementární transformační matice a s nimi související elementární úpravy matic.

12.9. Definice. *Elementární transformační maticí* budeme rozumět každou invertibilní matici, která se nejméně na jednom místě liší od jednotkové matice.

Rozeznáváme dva typy elementárních transformačních matic:

- (i) V matici jsou mimo hlavní diagonálu samé nuly. Na hlavní diagonále jsou jedničky s výjimkou místa ii , kde stojí nenulový prvek b (prvek b musí být nenulový, neboť matice má být invertibilní). Je-li $b = 1$, jde o jednotkovou matici.
- (ii) V matici jsou na hlavní diagonále samé jedničky. Mimo hlavní diagonálu jsou nuly s výjimkou místa ij , kde stojí prvek b . Je-li $b = 0$, jde o jednotkovou matici.

Vynásobíme-li nějakou matici A výše uvedenou elementární transformační maticí prvního typu zprava, je výsledkem matice, která se od matice A liší pouze tím, že její i -tý sloupec je b -násobkem i -tého sloupce matice A .

Vynásobíme-li nějakou matici A výše uvedenou elementární transformační maticí prvního typu zleva, je výsledkem matice, která se od matice A liší pouze tím, že její i -tý řádek je b -násobkem i -tého řádku matice A .

Vynásobíme-li matici A výše uvedenou elementární transformační maticí druhého typu zprava, je výsledkem matice, která se od matice A liší pouze tím, že její j -tý sloupec je součtem j -tého sloupce a b -násobku i -tého sloupce matice A (b -násobek i -tého sloupce se přičte k j -tému sloupci).

Vynásobíme-li matici A výše uvedenou elementární transformační maticí druhého typu zleva, je výsledkem matice, která se od matice A liší pouze tím, že její i -tý řádek je součtem i -tého řádku a b -násobku j -tého řádku matice A (b -násobek j -tého řádku se přičte k i -tému řádku).

Dvě elementární transformační matice prvního typu, které mají na stejném místě hlavní diagonály prvek b , resp. b^{-1} , jsou navzájem inverzní. Dvě elementární transformační matice druhého typu, které mají na stejném místě mimo hlavní diagonálu prvek b , resp. $-b$, jsou navzájem inverzní.

12.10. Příklady. Matice

$$F = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

je reálná elementární transformační matice prvního typu. Při násobení maticí F zleva se zdvojnásobí druhý řádek v násobené matici:

$$F \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 10 & 12 & 14 & 16 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Při násobení maticí F zprava se zdvojnásobí druhý sloupec v násobené matici:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \cdot F = \begin{pmatrix} 1 & 4 & 3 \\ 4 & 10 & 6 \\ 7 & 16 & 9 \end{pmatrix}$$

Matice

$$G = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

je elementární transformační matice druhého typu. Při násobení maticí G zleva se v násobené matici přičte dvojnásobek třetího řádku k prvnímu řádku:

$$G \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 8 & 7 & 6 \\ 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Při násobení maticí G zprava se v násobené matici přičte dvojnásobek prvního sloupce ke třetímu sloupci:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \cdot G = \begin{pmatrix} 1 & 2 & 5 \\ 4 & 5 & 14 \\ 7 & 8 & 23 \end{pmatrix}$$

Matice F a G jsou invertibilní,

$$F^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad G^{-1} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

12.11. Definice. Při práci s maticemi budeme *sloupcovými elementárními úpravami* rozumět:

- (i) vynásobení nějakého sloupce nenulovým prvkem $b \in T$;
- (ii) přičtení b -násobku nějakého sloupce k jinému sloupci (přitom $b \in T$).

Podobně budeme *řádkovými elementárními úpravami* rozumět:

- (i) vynásobení nějakého řádku nenulovým prvkem $b \in T$;
- (ii) přičtení b -násobku nějakého řádku k jinému řádku (přitom $b \in T$).

Sloupcové elementární úpravy odpovídají vynásobení příslušné matice elementárními transformačními maticemi prvního či druhého typu a to zprava. Někdy se za sloupcovou elementární úpravu považuje i prohození dvou sloupců; tuto úpravu však získáme složením čtyř sloupcových elementárních úprav výše uvedených. Chceme-li prohodit i -tý a j -tý sloupec, postupujeme takto: k j -tému sloupci přičteme i -tý, k i -tému sloupci přičteme (-1) -násobek j -tého, k j -tému sloupci přičteme i -tý a nakonec i -tý sloupec vynásobíme číslem -1 .

Řádkové elementární úpravy odpovídají vynásobení příslušné matice elementárními transformačními maticemi prvního či druhého typu a to zleva. Někdy se za řádkovou elementární úpravu považuje i prohození dvou řádků; tuto úpravu však získáme složením čtyř řádkových elementárních úprav výše uvedených.

Zdůrazněme ještě jednou, že sloupcové elementární úpravy získáme násobením příslušné matice elementárními transformačními maticemi zprava a řádkové elementární úpravy násobením elementárními transformačními maticemi zleva.

12.12. Věta. *Provádění sloupcových a řádkových elementárních úprav nemění hodnot.*

Důkaz. Předpokládejme, že od matice A dospějeme k matici A' postupným prováděním řádkových a sloupcových elementárních úprav. Podle předešlého je matice A' součinem matice A a elementárních transformačních matic. Hodnosti matic A a A' jsou tedy podle věty 12.6 stejné. \square

Uvědomme si, že při zjišťování dimenze lineárního obalu vektorů v_1, \dots, v_k prostoru T^n jsme s vektory v_1, \dots, v_k pracovali tak, jako bychom prováděli řádkové elementární úpravy matic (viz 7.14(viii) a 8.20).

12.13. Věta.

- (i) *Každou matici je možno pomocí konečně mnoha sloupcových a řádkových elementárních úprav převést na diagonální matici.*
- (ii) *Ke každé matici A existují regulární matice B, C takové, že BAC je diagonální matice.*

Důkaz. Nechť A je matice typu $n \times m$. Jestliže je A diagonální, pak nemusíme provádět žádné elementární úpravy, vezmeme za B a C jednotkové matice řádů n a m a důkaz je hotov.

Předpokládejme tedy, že matice A není diagonální; v matici A je tedy např. na místě ij nenulový prvek a . Jestliže je v levém horním rohu matice A nulový prvek, pak přehodíme první a i -tý řádek a první a j -tý sloupec; v levém horním rohu vzniklé matice pak bude nenulový prvek a . Vhodné násobky prvního řádku budeme nyní postupně přičítat k ostatním řádkům tak, abychom v prvním sloupci na druhém až n -tém místě dostali samé nuly. Jestliže je např. na prvním místě druhého řádku prvek b , přičteme ke druhému řádku $(-\frac{b}{a})$ -násobek prvního řádku; takto postupujeme dále. Potom budeme vhodné násobky prvního sloupce přičítat k ostatním sloupcům tak, abychom v prvním řádku na druhém až m -tém místě dostali samé nuly. Jestliže vzniklá matice ještě není diagonální, budeme provádět obdobné úpravy na druhý až n -tý řádek a na druhý až m -tý sloupec. První řádek a první sloupec se při těchto úpravách již nebudou měnit. Po konečném počtu úprav dospějeme od matice A k diagonální matici

$$D = B_r \dots B_2 B_1 A C_1 C_2 \dots C_s ,$$

kde $B_1, \dots, B_r, C_1, \dots, C_s$ jsou elementární transformační matice, které odpovídají provedeným elementárním úpravám. Součiny

$$B_r \dots B_2 B_1 , \quad C_1 C_2 \dots C_s$$

označme B, C . Matice B, C jsou (jako součiny regulárních matic) regulární a je $D = BAC$. Důkaz obou tvrzení je proveden. \square

Důkaz předchozí věty dává přímý návod, jak pomocí řádkových a sloupcových elementárních úprav dojít od matice A typu $n \times m$ k diagonální matici $D = BAC$. Chceme-li ještě najít příslušné regulární matice B a C , pak uvažujeme takto: Dospějeme-li od matice A řádkovými elementárními úpravami k matici BA , pak týmiž úpravami dospějeme od jednotkové matice E řádu n k matici $BE = B$. Dospějeme-li od matice A sloupcovými elementárními úpravami k matici AC , pak týmiž úpravami dospějeme od jednotkové matice E řádu m k matici $EC = C$. V konkrétním případě vyjdeme od schématu

$$\left(\begin{array}{c|c} A & E \\ \hline - & - \\ E & \end{array} \right) ,$$

kde jsme k matici A připsali jednotkové matice řádů n a m . Řádkové úpravy provádíme s n řádky délky $m+n$ a sloupcové úpravy s m sloupci délky $n+m$. Po konečném počtu kroků dojdeme ke schématu

$$\left(\begin{array}{c|c} D & B \\ \hline - & - \\ C & \end{array} \right) ,$$

kde $D = BAC$ je diagonální matice.

12.14. Příklad. Matici

$$A = \begin{pmatrix} 3 & 2 & 0 & 6 \\ 1 & 5 & 4 & 2 \\ 4 & 2 & 5 & 5 \\ 3 & 3 & 6 & 1 \\ 5 & 4 & 0 & 2 \end{pmatrix}$$

nad tělesem \mathbb{Z}_7 převedeme řádkovými a sloupcovými elementárními úpravami na diagonální matici $D = BAC$ a najdeme příslušné regulární matice B, C .

K matici A připišme jednotkové matice pátého a čtvrtého řádu:

$$\left(\begin{array}{cccc|cccc} 3 & 2 & 0 & 6 & 1 & 0 & 0 & 0 & 0 \\ 1 & 5 & 4 & 2 & 0 & 1 & 0 & 0 & 0 \\ 4 & 2 & 5 & 5 & 0 & 0 & 1 & 0 & 0 \\ 3 & 3 & 6 & 1 & 0 & 0 & 0 & 1 & 0 \\ 5 & 4 & 0 & 2 & 0 & 0 & 0 & 0 & 1 \\ - & - & - & - & - & - & - & - & - \\ 1 & 0 & 0 & 0 & & & & & \\ 0 & 1 & 0 & 0 & & & & & \\ 0 & 0 & 1 & 0 & & & & & \\ 0 & 0 & 0 & 1 & & & & & \end{array} \right)$$

Nyní postupně přičteme dvojnásobek prvního řádku ke druhému, první řádek ke třetímu, šestinásobek prvního řádku ke čtvrtému a trojnásobek prvního řádku k pátému. Dostaneme schéma:

$$\left(\begin{array}{cccc|cccc} 3 & 2 & 0 & 6 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 4 & 5 & 4 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 6 & 2 & 6 & 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 6 & 3 & 0 & 0 & 0 & 1 \\ - & - & - & - & - & - & - & - & - \\ 1 & 0 & 0 & 0 & & & & & \\ 0 & 1 & 0 & 0 & & & & & \\ 0 & 0 & 1 & 0 & & & & & \\ 0 & 0 & 0 & 1 & & & & & \end{array} \right)$$

Nyní přičteme čtyřnásobek, resp. pětínásobek prvního sloupce ke druhému, resp. čtvrtému sloupci. Dále přičteme pětínásobek, trojnásobek a dvojnásobek druhého

řádku po řadě ke třetímu, čtvrtému a pátému řádku. Dostaneme schéma:

$$\left(\begin{array}{cccc|cccc} 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & 4 & 4 & 5 & 1 & 0 & 0 \\ 0 & 0 & 4 & 2 & 5 & 3 & 0 & 1 & 0 \\ 0 & 0 & 1 & 6 & 0 & 2 & 0 & 0 & 1 \\ - & - & - & - & - & - & - & - & - \\ 1 & 4 & 0 & 5 & & & & & \\ 0 & 1 & 0 & 0 & & & & & \\ 0 & 0 & 1 & 0 & & & & & \\ 0 & 0 & 0 & 1 & & & & & \end{array} \right)$$

Nyní přičteme pětinasobek druhého sloupce ke třetímu. Dále přičteme šestinasobek, resp. pětinasobek třetího řádku ke čtvrtému, resp. pátému řádku:

$$\left(\begin{array}{cccc|cccc} 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & 4 & 4 & 5 & 1 & 0 & 0 \\ 0 & 0 & 0 & 5 & 1 & 5 & 6 & 1 & 0 \\ 0 & 0 & 0 & 5 & 6 & 6 & 5 & 0 & 1 \\ - & - & - & - & - & - & - & - & - \\ 1 & 4 & 6 & 5 & & & & & \\ 0 & 1 & 5 & 0 & & & & & \\ 0 & 0 & 1 & 0 & & & & & \\ 0 & 0 & 0 & 1 & & & & & \end{array} \right)$$

Nakonec přičteme šestinasobek třetího sloupce ke čtvrtému sloupci a šestinasobek čtvrtého řádku k pátému řádku:

$$\left(\begin{array}{cccc|cccc} 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 4 & 5 & 1 & 0 & 0 \\ 0 & 0 & 0 & 5 & 1 & 5 & 6 & 1 & 0 \\ 0 & 0 & 0 & 0 & 5 & 1 & 6 & 6 & 1 \\ - & - & - & - & - & - & - & - & - \\ 1 & 4 & 6 & 6 & & & & & \\ 0 & 1 & 5 & 2 & & & & & \\ 0 & 0 & 1 & 6 & & & & & \\ 0 & 0 & 0 & 1 & & & & & \end{array} \right)$$

Od schématu

$$\left(\begin{array}{c|c} A & E \\ - & - \\ E & - \end{array} \right) \quad \text{jsme dospěli ke schématu} \quad \left(\begin{array}{c|c} D & B \\ - & - \\ C & - \end{array} \right),$$

kde D je diagonální matice. Snadno ověříme, že $D = BAC$. Na diagonále je možno ještě čísla 3, 2, 4, 5 nahradit jedničkami; stačí např. vynásobit řádky po řadě čísly 5, 4, 2, 3 (změní se tím ovšem matice B).

Věta 12.13 tvrdí pouze to, že k dané matici A existují diagonální matice D a regulární matice B, C takové, že $D = BAC$. Tato diagonální matice D však není určena jednoznačně; ani odpovídající regulární matice B, C nejsou k matici A (a k nalezené matici D) určeny jednoznačně. To je ostatně vidět už v důkazu věty 12.13 či v příkladu 12.14; stačí si uvědomit, že elementárními úpravami můžeme od matice A přejít k nějaké diagonální matici mnoha různými způsoby. Všechny diagonální matice, ke kterým dospějeme od matice A elementárními úpravami, však mají podle věty 12.12 (resp. 12.6) stejnou hodnotu; je rovna hodnotě matice A .

V teorii soustav lineárních rovnic mají velký význam tzv. odstupňované matice.

12.15. Definice. Matice $A = (a_{ij})$ typu $n \times m$ nad tělesem T se nazývá *odstupňovaná*, jestliže pro její prvky platí:

- (i) Je-li $n > 1$, pak $a_{21} = 0$.
- (ii) Jestliže pro nějaké $i \in \{1, \dots, n-1\}$ a $k \in \{1, \dots, m-1\}$ je

$$a_{i,1} = a_{i,2} = \dots = a_{i,k} = 0,$$

potom je též

$$a_{i+1,1} = a_{i+1,2} = \dots = a_{i+1,k+1} = 0.$$

V odstupňované matici tedy každý nenulový řádek začíná větším počtem nul než řádek předcházející (pokud tento existuje). Podmínka (i) říká, že druhý řádek (pokud existuje) začíná alespoň jednou nulou; třetí řádek tedy začíná alespoň dvěma nulami a obecně i -tý řádek alespoň $(i-1)$ nulami. Snadno usoudíme, že hodnota odstupňované matice je rovna počtu jejích nenulových řádků; právě tolik (a ne více) lineárně nezávislých sloupců v ní lze totiž najít.

12.16. Příklad. Následující reálné matice jsou odstupňované:

$$\begin{pmatrix} 1 & -3 & 8 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 3 & -1 & 5 & 1 \\ 0 & 0 & 2 & 1 & -1 \\ 0 & 0 & 0 & 0 & -3 \end{pmatrix};$$

mají po řadě hodnotu 3, 2, 3.

Nulová matice je odstupňovaná, jednotková matice je odstupňovaná, každá matice typu $1 \times m$ je odstupňovaná.

12.17. Věta.

- (i) Každou matici je možno řádkovými elementárními úpravami převést na odstupňovanou matici.
 (ii) Ke každé matici A existuje regulární matice B taková, že matice BA je odstupňovaná.

Důkaz. Důkaz probíhá podobně jako důkaz věty 12.13.

Nechť A je matice typu $n \times m$. Jestliže je A už odstupňovaná, položíme $B = E$ a důkaz je hotov. Předpokládejme tedy, že matice A není odstupňovaná. Nechť j je nejmenší přirozené číslo takové, že v j -tém sloupci matice A je nenulový prvek (v praktických příkladech je téměř vždy $j = 1$). Případným přehozením řádků tento prvek dostaneme na místo $1j$. Přičítáním vhodných násobků prvního řádku k řádkům ostatním dostaneme v j -tém sloupci na druhém až n -tém místě samé nuly. Jestliže vzniklá matice není odstupňovaná, budeme v dalším provádět obdobným způsobem řádkové elementární úpravy pro menší matici složenou z druhého až n -tého řádku. Po konečně mnoha krocích tak dospějeme k odstupňované matici. Úpravy, které jsme prováděli, odpovídají přechodu od matice A k odstupňované matici $C = B_r \dots B_1 A$, kde B_1, \dots, B_r jsou elementární transformační matice. Matice $B = B_r \dots B_1$ je regulární; důkaz obou tvrzení je tedy proveden. \square

Důkaz věty 12.17 dává opět přímý návod, jak dospět pomocí řádkových elementárních úprav od matice A k odstupňované matici BA . Rovněž v tomto případě je často užitečné najít příslušnou matici B . V konkrétním příkladu vyjdeme od matice $(A | E)$, provádíme elementární úpravy s n řádky délky $m + n$, až dojdeme k matici $(C | B)$, kde $C = BA$ je odstupňovaná matice.

12.18. Příklad. Reálnou matici

$$A = \begin{pmatrix} 1 & 3 & -2 & 0 & 1 & 3 \\ 2 & 6 & 1 & 10 & 0 & 1 \\ -1 & -3 & 0 & -4 & 1 & 0 \\ 5 & 15 & -9 & 2 & 3 & 12 \end{pmatrix}$$

převeďme řádkovými elementárními úpravami na odstupňovanou matici $C = BA$ a najdeme i příslušnou regulární matici B .

K matici A připišeme nejprve jednotkovou matici čtvrtého řádu. Ke druhému, třetímu a čtvrtému řádku přičteme po řadě (-2) -násobek prvního řádku, první řádek a (-5) -násobek prvního řádku. Dostaneme matici

$$\left(\begin{array}{cccccc|cccc} 1 & 3 & -2 & 0 & 1 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 5 & 10 & -2 & -5 & -2 & 1 & 0 & 0 \\ 0 & 0 & -2 & -4 & 2 & 3 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & -2 & -3 & -5 & 0 & 0 & 1 \end{array} \right).$$

Nyní nejprve přehodíme druhý a čtvrtý řádek. Ke třetímu, resp. čtvrtému řádku přičteme dvojnásobek, resp. (-5) -násobek druhého. Ke čtvrtému řádku potom

přičteme čtyřnásobek třetího. Dostaneme matici

$$\left(\begin{array}{cccccc|cccc} 1 & 3 & -2 & 0 & 1 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & -2 & -3 & -5 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -2 & -3 & -9 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & -2 & -13 & 1 & 4 & 3 \end{array} \right).$$

Od schématu $(A|E)$ jsme dospěli ke schématu $(C|B)$, kde C je odstupňovaná matice. Snadno ověříme, že je skutečně $C = BA$.

Různými postupy můžeme od matice A dospět k různým odstupňovaným maticím. Přejdeme-li takto od matice A k odstupňované matici C , pak ani regulární matice B , pro kterou $C = BA$, není určena jednoznačně. Všechny odstupňované matice, ke kterým dospějeme od matice A řádkovými elementárními úpravami, však mají podle věty 12.12 stejnou hodnotu; je rovna hodnotě matice A .

12.19. Metoda zjištění hodnoty matice.

Chceme-li zjistit hodnotu matice A , můžeme postupovat takto. Od matice A přejdeme postupným prováděním elementárních úprav k nějaké vhodné matici B , jejíž hodnotu už umíme určit podle definice. Protože se při provádění elementárních úprav hodnota zachovává, je hodnota matice A rovna hodnotě matice B . Matici A můžeme převést až na diagonální matici, jejíž hodnota je rovna počtu jejích nenulových prvků. Stačí však převést matici A na matici odstupňovanou, jejíž hodnota je rovna počtu jejích nenulových řádků.

12.20. Příklad. Zjistíme hodnotu reálné matice

$$A = \begin{pmatrix} 2 & 1 & 2 & 1 \\ 1 & 2 & -1 & 3 \\ -1 & 1 & 2 & -2 \\ 3 & 4 & -2 & -1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Nejprve přehodíme první řádek a druhý řádek. Potom ke druhému, třetímu, čtvrtému a pátému řádku přičteme po řadě (-2) -násobek prvního řádku, první řádek, (-3) -násobek prvního řádku a (-1) -násobek prvního řádku. Dostaneme matici

$$\begin{pmatrix} 1 & 2 & -1 & 3 \\ 0 & -3 & 4 & -5 \\ 0 & 3 & 1 & 1 \\ 0 & -2 & 1 & -10 \\ 0 & -1 & 2 & -3 \end{pmatrix}.$$

Přehodíme druhý a pátý řádek. Ke třetímu, čtvrtému a pátému řádku pak přičteme po řadě trojnásobek, (-2) -násobek, (-3) -násobek druhého řádku. Dostaneme ma-

tici

$$\begin{pmatrix} 1 & 2 & -1 & 3 \\ 0 & -1 & 2 & -3 \\ 0 & 0 & 7 & -8 \\ 0 & 0 & -3 & -4 \\ 0 & 0 & -2 & 4 \end{pmatrix}.$$

Nyní už je vidět, že sloupce jsou lineárně nezávislé, takže hodnost matice A je 4. Chceme-li dále upravovat, přičteme nejprve trojnásobek pátého řádku ke třetímu. Potom přičteme trojnásobek, resp. dvojnásobek třetího řádku ke čtvrtému, resp. pátému řádku. Nakonec přičteme $(-\frac{3}{2})$ -násobek čtvrtého řádku k pátému. Dostaneme odstupňovanou matici

$$\begin{pmatrix} 1 & 2 & -1 & 3 \\ 0 & -1 & 2 & -3 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 8 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Každou matici můžeme pomocí řádkových a sloupcových elementárních úprav převést na diagonální matici (viz 12.13); pomocí řádkových elementárních úprav dospějeme obecně jen k matici odstupňované (viz 12.17). Jde-li však o regulární matici, můžeme pomocí řádkových elementárních úprav dojít až k jednotkové matici. Tento fakt uvidíme v důkazu následující věty.

12.21. Věta. *Každá regulární matice je součinem elementárních transformačních matic.*

Důkaz. Nechť A je regulární matice řádu n . Matici A převedeme řádkovými elementárními úpravami na odstupňovanou matici. Ta je horní trojúhelníková a všechny její prvky na diagonále jsou nenulové, neboť výchozí matice A je regulární. Dalšími řádkovými elementárními úpravami převedeme tuto matici na matici jednotkovou. Nejprve vynásobíme jednotlivé řádky vhodnými prvky tak, aby na diagonále byly jedničky. Potom přičítáme vhodné násobky posledního řádku k ostatním řádkům tak, aby v posledním sloupci na prvním až $(n-1)$ -ním místě byly samé nuly. Vhodné násobky předposledního řádku pak přičítáme k prvním až $(n-2)$ -hému řádku tak, aby v předposledním sloupci byly nuly na prvním až $(n-2)$ -hém místě. Po konečném počtu kroků dospějeme k jednotkové matici. Získali jsme ji vynásobením matice A zleva elementárními transformačními maticemi, tj.

$$E = B_k \dots B_1 A.$$

Tedy

$$A^{-1} = B_k \dots B_1 \quad \text{a} \quad A = (B_k \dots B_1)^{-1} = B_1^{-1} \dots B_k^{-1}.$$

Vzhledem k tomu, že inverzní matice k elementárním transformačním maticím jsou opět elementární transformační matice, je věta dokázána. \square

12.22. Metoda výpočtu inverzní matice.

V důkazu předchozí věty jsme viděli, že regulární matici A můžeme řádkovými elementárními úpravami převést na jednotkovou matici a že součin B elementárních transformačních matic použitých při tomto postupu je matice A^{-1} . Stačí tedy zjistit tento součin elementárních transformačních matic. Postupujeme tedy takto: Matici $(A|E)$ typu $n \times 2n$ převedeme řádkovými elementárními úpravami na matici $(E|B)$; matice B je součinem elementárních transformačních matic, které odpovídají použitým řádkovým úpravám. Podle předešlého víme, že $B = A^{-1}$.

Poznamenejme, že podobně můžeme sloupcovými elementárními úpravami dojít od matice

$$\begin{pmatrix} A \\ - \\ E \end{pmatrix} \quad \text{k matici} \quad \begin{pmatrix} E \\ - \\ A^{-1} \end{pmatrix}.$$

Známe-li matice A a C a potřebujeme-li vypočítat součin $A^{-1}C$, pak můžeme postupovat takto: Matici $(A|C)$ převedeme řádkovými elementárními úpravami na matici $(E|A^{-1}C)$. Tuto metodu uijeme např. při výpočtu matic přechodu (viz dále 12.25). Podobně můžeme sloupcovými elementárními úpravami dojít od matice

$$\begin{pmatrix} A \\ - \\ C \end{pmatrix} \quad \text{k matici} \quad \begin{pmatrix} E \\ - \\ CA^{-1} \end{pmatrix}$$

a vypočítat tak součin CA^{-1} .

12.23. Příklad. K matici

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 3 \\ 1 & 4 & 4 \end{pmatrix}$$

nad tělesem \mathbb{Z}_5 vypočteme inverzní matici.

Vyjdeme od matice $(A|E)$ typu 3×6 . Čtyřnásobek prvního řádku přičteme ke třetímu řádku a potom přičteme dvojnásobek druhého řádku ke třetímu. Dostaneme matici

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 4 & 3 & 0 & 1 & 0 \\ 0 & 0 & 2 & 4 & 2 & 1 \end{array} \right).$$

V této matici vynásobíme druhý, resp. třetí řádek číslem 4, resp. 3. Potom přičteme trojnásobek třetího řádku ke druhému a dvojnásobek třetího k prvnímu. Dostaneme matici

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 2 & 1 & 3 \end{array} \right).$$

Nakonec přičteme trojnásobek druhého řádku k prvnímu. Od matice $(A|E)$ jsme dospěli k matici $(E|A^{-1})$, kde

$$A^{-1} = \begin{pmatrix} 3 & 3 & 3 \\ 1 & 2 & 4 \\ 2 & 1 & 3 \end{pmatrix}.$$

Metodu pro výpočet inverzní matice, kterou jsme právě popsali, úspěšně užijeme pro výpočet inverzních matic k maticím řádu n , jejichž prvky jsou v matici rozmístěny podle určitých pravidel.

12.24 Příklad. Vypočteme inverzní matici k reálné matici

$$A = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & 0 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 0 \end{pmatrix}$$

řádu n , která má na hlavní diagonále nuly a všude jinde jedničky.

V matici $(A|E)$ typu $n \times 2n$ provedeme postupně následující řádkové elementární úpravy:

- (i) Druhý až n -tý řádek přičteme k prvnímu.
- (ii) První řádek vydělíme číslem $n - 1$.
- (iii) První řádek odečteme od všech ostatních řádků.
- (iv) Druhý až n -tý řádek přičteme k prvnímu.
- (v) Druhý až n -tý řádek vynásobíme číslem -1 .

Těmito úpravami dospějeme od matice $(A|E)$ k matici $(E|A^{-1})$, kde

$$A^{-1} = \frac{1}{n-1} \begin{pmatrix} 2-n & 1 & \dots & 1 \\ 1 & 2-n & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 2-n \end{pmatrix}.$$

Poznamenejme, že reálná matice A je regulární pro $n > 1$. Pokud bychom matici A řádu n uvažovali nad tělesem \mathbb{Z}_p , byla by matice A regulární právě tehdy, když $n \neq 1 \pmod{p}$; výpočet matice A^{-1} i výsledek vypadá stejně (po převedení čísel modulo p).

12.25. Výpočet matice přechodu.

Mějme báze M, N vektorového prostoru T^n . Označme symbolem A , resp. B matice přechodu od báze M , resp. N ke kanonické bázi. Tyto matice získáme tak, že vektory báze M , resp. N napíšeme do sloupců.

Matice přechodu od báze M k bázi N je podle 11.8 rovna součinu $B^{-1}A$. Matici přechodu od báze M k bázi N tedy vypočítáme podle odstavce 12.22 tak, že řádkovými elementárními úpravami přejdeme od matice $(B|A)$ k matici $(E|B^{-1}A)$.

Místo kanonické báze je možno zvolit libovolnou jinou bázi, vzhledem ke které se snadno zjistí souřadnice vektorů báze M a N . Tohoto faktu využijeme zejména v případě, kdy nejde o prostor T^n a kdy tedy o kanonické bázi nemůžeme mluvit.

12.26. Věta. *Hodnost navzájem transponovaných matic je stejná.*

Důkaz. Nechť A je matice typu $n \times m$. Dospějeme-li od matice A pomocí elementárních úprav k diagonální matici D , pak pomocí transponovaných elementárních úprav, které provádíme ve stejném pořadí, dospějeme od matice A^T k matici D^T (tj. úpravy, které provádíme v matici A se sloupci/řádky, provádíme v matici A^T s řádky/sloupci). Vzhledem k tomu, že provádění elementárních úprav nemění hodnost (viz 12.12), je

$$r(A) = r(D) = r(D^T) = r(A^T). \quad \square$$

12.27. Důsledek. *Nechť A je matice typu $n \times m$ nad tělesem T . Hodnost $r(A)$ matice A je rovna dimenzi vektorového prostoru generovaného řádky matice A (jako vektory prostoru T^m); číslo $r(A)$ je tedy rovno maximálnímu počtu lineárně nezávislých řádků matice A . \square*

Při úpravách čtvercových matic budeme *symetrickými úpravami* rozumět následující dvojice elementárních úprav.

- (i) Vynásobení i -tého řádku nenulovým prvkem b a vynásobení i -tého sloupce stejným prvkem b .
- (ii) Přičtení b -násobku i -tého řádku k j -tému řádku a přičtení b -násobku i -tého sloupce k j -tému sloupci.

Každá dvojice takovýchto elementárních úprav odpovídá dvojici elementárních transformačních matic B^T a B . Provedení symetrické úpravy tedy odpovídá přechodu od matice A k matici $B^T A B$. Jestliže je matice A symetrická, tj. $A^T = A$, potom je matice $B^T A B$ rovněž symetrická, neboť

$$(B^T A B)^T = B^T A^T (B^T)^T = B^T A B.$$

Poznamenejme, že prohození i -tého a j -tého řádku a prohození i -tého a j -tého sloupce lze složit ze čtyř symetrických úprav.

12.28. Věta. *Nechť T je těleso, jehož charakteristika není 2. Potom platí:*

- (i) *Každou symetrickou matici nad tělesem T je možno symetrickými úpravami převést na diagonální matici.*
- (ii) *Ke každé symetrické matici A nad tělesem T existuje regulární matice B taková, že $B^T A B$ je diagonální matice.*

Důkaz. Nechť A je symetrická matice řádu n nad tělesem T .

(a) Předpokládejme, že v levém horním rohu matice A je nenulový prvek. Vhodný násobek prvního řádku přičteme ke druhému řádku, abychom na prvním místě druhého řádku dostali nulu. Když přičteme stejný násobek prvního sloupce ke druhému sloupci, dostaneme nulu i na prvním místě druhého sloupce, neboť matice A je symetrická. Provedli jsme symetrickou úpravu; matice A přešla v symetrickou matici, která má na místech 12 a 21 nuly. Dalším prováděním symetrických

úprav dojdeme k symetrické matici, která má až na levý horní roh v prvním řádku a prvním sloupci samé nuly.

(b) Předpokládejme, že v levém horním rohu matice A je nula. Jestliže je na diagonále matice A na místě jj nenulový prvek, pak prohozením prvního a j -tého řádku a prvního a j -tého sloupce přejde tento prvek do levého horního rohu. Dále pokračujeme jako v případě (a).

(c) Předpokládejme, že matice A má na hlavní diagonále samé nuly. Jestliže je v prvním sloupci na j -tém místě nenulový prvek b , pak vzhledem k symetrii je tento prvek i na j -tém místě v prvním řádku. Přičteme-li j -tý řádek k prvnímu řádku a pak j -tý sloupec k prvnímu sloupci, dospějeme k symetrické matici, která má v levém horním rohu nenulový prvek $2b$. Nenulovost tohoto prvku vyplývá z předpokladu $\text{char } T \neq 2$. Po provedení této symetrické úpravy pokračujeme jako v případě (a).

(d) Jestliže má matice A v celém prvním řádku a tedy i v prvním sloupci nuly, pak neprovádíme žádné úpravy.

Pomocí postupů uvedených v (a)–(d) jsme dospěli k symetrické matici, která má na druhém až n -tém místě prvního řádku a prvního sloupce samé nuly. Nyní budeme obdobným způsobem provádět symetrické úpravy na druhý až n -tý řádek a druhý až n -tý sloupec. Po konečném počtu kroků dospějeme k diagonální matici. Uvedený postup odpovídá přechodu od matice A k diagonální matici

$$D = B_k^T \dots B_2^T B_1^T A B_1 B_2 \dots B_k ,$$

kde dvojice navzájem transponovaných matic $B_1, B_1^T, B_2, B_2^T, \dots, B_k, B_k^T$ odpovídají provedeným symetrickým úpravám. Položíme-li $B = B_1 B_2 \dots B_k$, je $D = B^T A B$. \square

Uvedený důkaz dává návod, jak pomocí symetrických úprav dojít od symetrické matice A k diagonální matici $B^T A B$. Chceme-li zjistit transformační matici B , pak postupujeme takto: Vyjdeme od matice $(A | E)$. Symetrickými úpravami dojdeme od matice A k matici D a současně řádkovými úpravami, které jsme přitom použili, dojdeme od matice E k matici B^T . Od matice $(A | E)$ tak dospějeme k matici $(D | B^T)$.

12.29. Příklad. Reálnou symetrickou matici

$$A = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 0 & 2 \\ 3 & 2 & 0 \end{pmatrix}$$

převédeme symetrickými úpravami na diagonální matici D a nalezneme nějakou regulární matici B , pro kterou $D = B^T A B$.

Vyděme od matice $(A|E)$ typu 3×6 . Přičteme druhý řádek k prvnímu a druhý sloupec k prvnímu. Dostaneme matici

$$\left(\begin{array}{ccc|ccc} 2 & 1 & 5 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 & 1 & 0 \\ 5 & 2 & 0 & 0 & 0 & 1 \end{array} \right),$$

jejíž levá část je opět symetrická. Abychom se vyhnuli počítání se zlomky, vynásobíme druhý a třetí řádek a druhý a třetí sloupec číslem 2. Potom ke druhému řádku přičteme (-1) -násobek prvního, ke třetímu řádku (-5) -násobek prvního. Totéž provedeme ve sloupcích. Dostaneme matici

$$\left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 1 & 0 \\ 0 & -2 & -2 & -1 & 1 & 0 \\ 0 & -2 & -50 & -5 & -5 & 2 \end{array} \right).$$

Nyní přičteme (-1) -násobek druhého řádku ke třetímu a (-1) -násobek druhého sloupce ke třetímu a získáme matici

$$\left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 1 & 0 \\ 0 & -2 & 0 & -1 & 1 & 0 \\ 0 & 0 & -48 & -4 & -6 & 2 \end{array} \right).$$

Od matice $(A|E)$ jsme dospěli k matici $(D|B^T)$. Snadno se přesvědčíme, že je $D = B^T A B$.

Při úpravách čtvercových komplexních matic budeme *hermitovskými úpravami* rozumět následující dvojice elementárních úprav (symbolem \bar{b} rozumíme číslo komplexně sdružené k číslu b):

- (i) Vynásobení i -tého řádku nenulovým komplexním číslem b a vynásobení i -tého sloupce číslem \bar{b} .
- (ii) Přičtení b -násobku i -tého řádku k j -tému řádku a přičtení \bar{b} -násobku i -tého sloupce k j -tému sloupci.

Každá dvojice takovýchto elementárních úprav odpovídá dvojici elementárních transformačních matic B^T a \bar{B} . Provedení hermitovské úpravy tedy odpovídá přechodu od matice A k matici $B^T A \bar{B}$. Jestliže je matice A hermitovská, tj. $\bar{A}^T = A$, potom je matice $B^T A \bar{B}$ rovněž hermitovská, neboť

$$\overline{(B^T A \bar{B})^T} = (\bar{B}^T \bar{A} B)^T = B^T \bar{A}^T \bar{B} = B^T A \bar{B}.$$

Poznamenejme, že prohození i -tého a j -tého řádku a prohození i -tého a j -tého sloupce lze složit ze čtyř hermitovských úprav.

12.30. Věta.

- (i) Každou hermitovskou matici je možno hermitovskými úpravami převést na reálnou diagonální matici.
- (ii) Ke každé hermitovské matici A existuje regulární komplexní matice B taková, že $B^T A \bar{B}$ je reálná diagonální matice.

Důkaz. Důkaz této věty je prakticky stejný jako důkaz věty 12.28, místo symetrických úprav se však provádějí úpravy hermitovské. Jediný drobný rozdíl je ve třetím případě, kdy má matice A na hlavní diagonále samé nuly a v prvním sloupci na místě j -tém nenulový prvek b (a na j -tém místě v prvním řádku tedy prvek \bar{b}). Přičtením j -tého řádku k prvnímu řádku a j -tého sloupce k prvnímu sloupci dospějeme k hermitovské matici, která má v levém horním rohu reálné číslo $b + \bar{b}$. Jestliže je číslo b ryze imaginární, pak je $b + \bar{b} = 0$. V tomto případě je třeba k prvnímu řádku přičíst i -násobek j -tého řádku a k prvnímu sloupci $(-i)$ -násobek j -tého sloupce (symbol i zde představuje komplexní jednotku). V levém horním rohu získané matice pak bude nenulové reálné číslo $bi - \bar{b}i$.

Uvedený postup odpovídá přechodu od hermitovské matice A k hermitovské diagonální (tj. reálné diagonální) matici

$$D = B_k^T \dots B_2^T B_1^T A \bar{B}_1 \bar{B}_2 \dots \bar{B}_k ,$$

kde dvojice matic $B_1^T, \bar{B}_1, \dots, B_k^T, \bar{B}_k$ odpovídají provedeným hermitovským úpravám. Položíme-li $B = B_1 \dots B_k$, je

$$D = B^T A \bar{B}. \quad \square$$

12.31. Příklad. Hermitovskou matici

$$A = \begin{pmatrix} 1 & -i & 1-i \\ i & 1 & 1 \\ 1+i & 1 & 2 \end{pmatrix}$$

převеdeme pomocí hermitovských úprav na reálnou diagonální matici D a najdeme nějakou regulární matici B , pro kterou $D = B^T A \bar{B}$.

Vyjděme od matice $(A | E)$ typu 3×6 . Přičtěme $(-i)$ -násobek prvního řádku ke druhému a $(-1-i)$ -násobek prvního řádku ke třetímu. Potom přičtěme i -násobek prvního sloupce ke druhému a $(-1+i)$ -násobek prvního sloupce ke třetímu. Dostaneme matici

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -i & -i & 1 & 0 \\ 0 & i & 0 & -1-i & 0 & 1 \end{array} \right) .$$

Nyní přičtěme i -násobek třetího řádku ke druhému a $(-i)$ -násobek třetího sloupce ke druhému. Získáme matici

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -2 & -i & 1-2i & 1 & i \\ 0 & i & 0 & -1-i & 0 & 1 \end{array} \right) .$$

Abychom nepočítali se zlomky, vynásobíme třetí řádek a třetí sloupec číslem 2. Potom přičteme i -násobek druhého řádku ke třetímu řádku a $(-i)$ -násobek druhého sloupce ke třetímu sloupci. Dostaneme matici

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -2 & 0 & 1-2i & 1 & i \\ 0 & 0 & 2 & -i & i & 1 \end{array} \right).$$

Od matice $(A|E)$ jsme tedy dospěli k matici $(D|B^T)$. Snadno se přesvědčíme, že $D = B^T A \bar{B}$.

13.2. Věta. *Nechť A je matice typu $n \times m$ nad tělesem T a y necht' je n -tice prvků tělesa T . Potom platí:*

- (i) *Soustava lineárních rovnic $Ax = y$ je řešitelná tehdy a jen tehdy, když je $r(A|y^T) = r(A)$.*
- (ii) *Jestliže je soustava $Ax = y$ řešitelná, potom množina všech jejích řešení je lineární množina $x_0 + W$ v prostoru T^m , kde x_0 je libovolně zvolené řešení soustavy $Ax = y$ a W je podprostor tvořený právě všemi řešeními odpovídající homogenní soustavy $Ax = o$. Dimenze podprostoru W je $m - r(A)$.*

Důkaz. Necht' f je homomorfismus prostoru T^m do prostoru T^n , který každé m -tici $x \in T^m$ přiřazuje n -tici $y \in T^n$, pro kterou $y^T = A \cdot x^T$. Vzhledem ke kanonickým bázím prostorů T^m a T^n je maticí homomorfismu f právě matice A ; sloupce matice A jsou obrazy vektorů kanonické báze prostoru T^m a generují tedy podprostor $\text{Im } f$.

Pro dané $y \in T^n$ je množina všech $x \in T^m$, pro která je $A \cdot x^T = y^T$, úplným vzorem vektoru y při homomorfismu f .

(i) Soustava $Ax = y$ je tedy řešitelná právě tehdy, když je $y \in \text{Im } f$. Vzhledem k tomu, že podprostor $\text{Im } f$ je generován sloupci matice A , je $y \in \text{Im } f$ právě tehdy, když je y lineární kombinací sloupců matice A , tj. právě tehdy, když je $r(A|y^T) = r(A)$.

(ii) Podle 10.4(ix) je úplným vzorem vektoru $y \in \text{Im } f$ lineární množina $x_0 + \text{Ker } f$, kde x_0 je libovolně zvolený vektor prostoru T^m , pro který je $f(x_0) = y$; je tedy $A \cdot x_0^T = y^T$, tj. x_0 je nějaké řešení soustavy $Ax = y$. Dále je $\text{Ker } f$ množinou všech vektorů $x \in T^m$, pro které je $A \cdot x^T = o^T$; podprostor $\text{Ker } f$ je tedy množinou všech řešení homogenní soustavy $Ax = o$. Podle věty 10.18 (věta o hodnotě a defektu) a věty 12.4 je

$$m = d(f) + r(f) = \dim \text{Ker } f + r(A) ,$$

takže

$$\dim \text{Ker } f = m - r(A). \quad \square$$

Soustava lineárních rovnic $Ax = y$ je tedy řešitelná právě tehdy, když je hodnota matice soustavy rovna hodnotě rozšířené matice soustavy. Jak jsme uvedli v předchozím důkazu, nastane to právě tehdy, když je sloupec pravých stran lineární kombinací sloupců matice soustavy. Tuto skutečnost můžeme velmi názorně demonstrovat, zapíšeme-li soustavu rovnic (1) „sloupcově“:

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} \cdot x_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix} \cdot x_2 + \cdots + \begin{pmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ a_{nm} \end{pmatrix} \cdot x_m = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

Z tohoto zápisu je ihned vidět nutná a postačující podmínka řešitelnosti soustavy (1) i smysl množiny všech řešení této soustavy.

- Soustava je řešitelná právě tehdy, když je sloupec pravých stran lineární kombinací sloupců matice soustavy.
- Všechny m -tice koeficientů těchto lineárních kombinací tvoří právě množinu všech řešení uvažované soustavy $Ax = y$.

Poznamenejme ještě, že jestliže je soustava $Ax = y$ řešitelná, pak je jejím řešením podle předchozí věty lineární množina, jejíž dimenze je rovna *rozdílu počtu neznámých a hodnosti matice soustavy*.

Při řešení soustav lineárních rovnic se často hovoří o lineárně závislých či nezávislých rovnicích. Je tím vlastně míněna lineární závislost či nezávislost odpovídajících řádků rozšířené matice soustavy. V tomto smyslu můžeme říci, že dimenze lineární množiny všech řešení soustavy $Ax = y$ je rovna *rozdílu počtu neznámých a počtu lineárně nezávislých rovnic soustavy*.

13.3. Důsledek. *Nechť A je matice typu $n \times m$ nad tělesem T . Potom platí:*

- (i) *Soustava $Ax = y$ je řešitelná pro každé $y \in T^n$ právě tehdy, když $r(A) = n$.*
- (ii) *Pro dané $y \in T^n$ má soustava $Ax = y$ právě jediné řešení tehdy a jen tehdy, když $r(A | y^T) = r(A) = m$.*
- (iii) *Homogenní soustava $Ax = 0$ je vždy řešitelná. Množina všech jejích řešení je podprostorem prostoru T^m . Soustava $Ax = 0$ má právě jediné řešení právě tehdy, když je $r(A) = m$.*

Důkaz.

- (i) Pro každé $y \in T^n$ je $r(A | y^T) = r(A)$ právě tehdy, když je $r(A) = n$.
- (ii) Soustava $Ax = y$ je řešitelná právě tehdy, když je $r(A | y^T) = r(A)$; navíc má právě jediné řešení, když dimenze lineární množiny všech řešení je nula, tj. právě když je $r(A) = m$.
- (iii) Tvrzení plyne z předchozí věty a z tvrzení (ii). \square

Poznamenejme, že nastane-li případ (i), je nutně $n \leq m$, a nastane-li případ (ii), je nutně $m \leq n$.

Homogenní soustava $Ax = 0$ má vždy tzv. *triviální* neboli *nulové řešení*, tj. nulový vektor prostoru T^m . Každé jiné řešení se nazývá *netriviální*, resp. *nenulové*. Jestliže je tedy $r(A) = m$, pak má soustava $Ax = 0$ pouze triviální řešení. Jestliže je $r(A) < m$, pak má soustava $Ax = 0$ i netriviální řešení.

Ve větě 13.2 jsme zodpověděli otázky řešitelnosti a popisu množiny všech řešení soustavy $Ax = y$. Zbývá popsat metody vedoucí k nalezení množiny všech řešení. Nejprve uvedeme jednoduché, ale velmi užitečné lemma.

13.4. Lemma. *Nechť A je matice typu $n \times m$ nad tělesem T a nechť y je n -tice prvků tělesa T . Jestliže B je regulární matice řádu n , $C = BA$ a jestliže z je n -tice prvků tělesa T určená vztahem $z^T = B \cdot y^T$, potom soustava $Ax = y$ má stejnou množinu řešení jako soustava $Cx = z$.*

Důkaz. Jestliže pro vektor $x \in T^m$ je $A \cdot x^T = y^T$, potom je též $(BA) \cdot x^T = B \cdot y^T$, tj. $C \cdot x^T = z^T$; když je naopak $C \cdot x^T = z^T$, tj. $(BA) \cdot x^T = B \cdot y^T$, potom je $B^{-1}(BA) \cdot x^T = B^{-1}B \cdot y^T$ a tedy $A \cdot x^T = y^T$. \square

13.5. Důsledek. *Nechť A je regulární matice řádu n nad tělesem T a y nechť je n -tice prvků tělesa T . Potom má soustava rovnic $Ax = y$ právě jediné řešení $x \in T^n$, pro které je $x^T = A^{-1} \cdot y^T$.*

Důkaz. Podle důsledku 13.3 má soustava $Ax = y$ právě jediné řešení. Podle předchozího lemmatu má soustava $Ax = y$ stejnou množinu řešení jako soustava $Ex = z$, kde $z^T = A^{-1}y^T$. Soustava $Ex = z$ má jediné řešení $x = z$. \square

13.6. Gaussův eliminační algoritmus.

Nechť $Ax = y$ je soustava lineárních rovnic, kde A je matice typu $n \times m$ nad tělesem T a y je n -tice prvků tělesa T . Podle věty 12.17 existuje regulární matice B řádu n taková, že matice $B \cdot (A|y^T) = (BA|B \cdot y^T)$ je odstupňovaná. Podle lemmatu 13.4 má výchozí soustava $Ax = y$ stejnou množinu řešení jako soustava $Cx = z$, kde $C = BA$ a $z^T = B \cdot y^T$. V praktickém případě přejdeme pomocí řádkových elementárních úprav od matice $(A|y^T)$ k odstupňované matici $(C|z^T)$; tyto dvě matice reprezentují podle lemmatu 13.4 dvě soustavy lineárních rovnic se stejnou množinou řešení.

V následujícím předpokládejme, že $Ax = y$ je soustava lineárních rovnic nad tělesem T a že matice $(A|y^T)$ typu $n \times (m+1)$ je již odstupňovaná. Protože je hodnost odstupňované matice rovna počtu jejích nenulových řádků, je ihned vidět, zda je $r(A) = r(A|y^T)$, tj. zda je soustava $Ax = y$ řešitelná. Jestliže tomu tak je, definujme číslo k rovností $k = m - r(A)$. K určení množiny všech řešení stačí podle věty 13.2 najít jedno řešení x_0 soustavy $Ax = y$ a k lineárně nezávislých řešení x_1, \dots, x_k odpovídající homogenní soustavě $Ax = o$. Lineární množina

$$x_0 + [x_1, \dots, x_k]$$

je potom množinou všech řešení soustavy $Ax = y$.

Matice A má $r(A)$ nenulových řádků. Předpokládejme, že první nenulový prvek v prvním řádku má sloupcový index j_1 (v praktických příkladech je $j_1 = 1$), že první nenulový prvek v druhém řádku má sloupcový index j_2, \dots a první nenulový prvek v $r(A)$ -tém řádku má sloupcový index $j_{r(A)}$; tedy $j_1 < j_2 < \dots < j_{r(A)} \leq m$. Ostatní sloupcové indexy matice soustavy označme $r_1 < r_2 < \dots < r_k$; platí tedy rovnost

$$\{j_1, j_2, \dots, j_{r(A)}\} \cup \{r_1, r_2, \dots, r_k\} = \{1, 2, \dots, m\}.$$

Vzhledem k tomu, že je matice A odstupňovaná, je možno velmi jednoduše najít vektory x_0 a x_1, \dots, x_k . Obecný postup popíšeme v následujících dvou odstavcích a objasníme ho na jednoduchém schématu. Teoreticky se tento postup špatně popisuje, praktické provedení však obtížné není.

Výpočet řešení x_0 .

Složky m -tice x_0 s indexy r_1, \dots, r_k zvolíme libovolně (můžeme je např. položit rovné nule). Složky s indexy $j_{r(A)}, j_{r(A)-1}, \dots, j_1$ postupně vypočítáváme z jednotlivých rovnic soustavy $Ax = y$: z $r(A)$ -té rovnice vypočteme složku s indexem $j_{r(A)}$, z $(r(A) - 1)$ -ní rovnice vypočteme složku s indexem $j_{r(A)-1}, \dots$ a nakonec z první rovnice vypočteme složku s indexem j_1 . Složky řešení x_0 indexované čísly r_1, \dots, r_k můžeme volit postupně, aby byl výpočet co nejjednodušší.

Výpočet řešení x_1, \dots, x_k .

Složky s indexy r_1, \dots, r_k zvolíme: složku s indexem r_1 vektoru x_1 , složku s indexem r_2 vektoru x_2, \dots a složku s indexem r_k vektoru x_k položíme rovnou jedničce (pro zjednodušení výpočtu můžeme volit vhodné nenulové prvky tělesa T), další složky indexované čísly r_1, \dots, r_k vektorů x_1, \dots, x_k položíme rovny nule. Touto volbou je zaručeno, že vektory x_1, \dots, x_k jsou lineárně nezávislé. Ostatní složky budeme postupně vypočítávat z rovnic odpovídající homogenní soustavy $Ax = 0$: z $r(A)$ -té rovnice vypočteme složku s indexem $j_{r(A)}, \dots$ a nakonec z první rovnice vypočteme složku s indexem j_1 .

Výpočet složek vektorů x_0, x_1, \dots, x_k indexovaných čísly $j_{r(A)}, \dots, j_1$ je možno vždy provést, neboť při výpočtu každé z těchto složek se využije jediná lineární rovnice o jedné neznámé, u které je *nenulový* koeficient; za ostatní neznámé jsou dosazeny dříve vypočtené hodnoty.

Na následujícím schématu je znázorněna odstupňovaná matice řešitelné soustavy lineárních rovnic typu 4×8 (hvězdičky značí nenulové prvky), pro kterou je $j_1 = 1, j_2 = 2, j_3 = 5, j_4 = 6, r_1 = 3, r_2 = 4, r_3 = 7, r_4 = 8$. Naznačena je i volba jednotlivých složek vektorů x_0, x_1, x_2, x_3, x_4 ; složky označené symbolem \times při Gaussově algoritmu postupně vypočítáváme (vyznačeno šipkami), jak je výše uvedeno. Pro konkrétní výpočet je výhodné zachovat i úpravu naznačenou ve schématu a psát vektory x_0, x_1, x_2, x_3, x_4 tak, aby jejich složky byly přesně pod odpovídajícími koeficienty matice soustavy.

$$\begin{array}{cccccccc|cccc}
 * & . & . & . & . & . & . & . & | & . & & | & 0 \\
 0 & * & . & . & . & . & . & . & | & . & & | & 0 \\
 0 & 0 & 0 & 0 & * & . & . & . & | & . & & | & 0 \\
 0 & 0 & 0 & 0 & 0 & * & . & . & | & . & & | & 0 \\
 \\
 \downarrow & \downarrow & & & \downarrow & \downarrow & & & & & & & \\
 (\times & \times & 0 & 0 & \times & \times & 0 & 0) & = & x_0 \\
 \\
 (\times & \times & 1 & 0 & \times & \times & 0 & 0) & = & x_1 \\
 (\times & \times & 0 & 1 & \times & \times & 0 & 0) & = & x_2 \\
 (\times & \times & 0 & 0 & \times & \times & 1 & 0) & = & x_3 \\
 (\times & \times & 0 & 0 & \times & \times & 0 & 1) & = & x_4
 \end{array}$$

Řešení soustavy lineárních rovnic pomocí Gaussova eliminačního algoritmu objasníme na následujících příkladech.

13.7. Příklad. Nalezneme množinu všech řešení následující soustavy lineárních rovnic nad tělesem reálných čísel.

$$\begin{aligned}x - y + z + u - 2v &= 0, \\2x + y - z - u + v &= 1, \\3x + 3y - 3z - 3u + 4v &= 2, \\4x + 5y - 5z - 5u + 7v &= 3.\end{aligned}$$

Nejprve přejdeme standardním způsobem pomocí řádkových elementárních úprav od rozšířené matice dané soustavy k odstupňované matici

$$\left(\begin{array}{ccccc|c} 1 & -1 & 1 & 1 & -2 & 0 \\ 0 & 3 & -3 & -3 & 5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right),$$

která odpovídá soustavě rovnic

$$\begin{aligned}x - y + z + u - 2v &= 0, \\3y - 3z - 3u + 5v &= 1,\end{aligned}\tag{2}$$

která má stejnou množinu řešení jako zadaná soustava. Ihned je vidět, že tato soustava je řešitelná, lineární množina všech jejích řešení má dimenzi $5 - 2 = 3$ a má tedy tvar $x_0 + [x_1, x_2, x_3]$. Při výpočtu vektorů x_0, x_1, x_2, x_3 budeme volit jejich třetí, čtvrtou a pátou složku a počítat jejich druhou a první složku. Volme tedy

$$\begin{aligned}x_0 &= (\cdot, \cdot, 0, 0, 0), \\x_1 &= (\cdot, \cdot, 1, 0, 0), \\x_2 &= (\cdot, \cdot, 0, 1, 0), \\x_3 &= (\cdot, \cdot, 0, 0, 1).\end{aligned}$$

Dosazením „částečně známého“ vektoru x_0 nejprve do druhé a potom do první rovnice soustavy (2) postupně vypočteme

$$x_0 = \left(\frac{1}{3}, \frac{1}{3}, 0, 0, 0 \right).$$

Postupným dosazením „částečně známých“ vektorů x_1, x_2, x_3 nejprve do druhé a pak do první rovnice odpovídající homogenní soustavy

$$\begin{aligned}x - y + z + u - 2v &= 0, \\3y - 3z - 3u + 5v &= 0\end{aligned}$$

vypočteme

$$x_1 = (0, 1, 1, 0, 0), \quad x_2 = (0, 1, 0, 1, 0), \quad x_3 = \left(\frac{1}{3}, -\frac{5}{3}, 0, 0, 1\right).$$

Řešením dané soustavy je tedy lineární množina

$$\left(\frac{1}{3}, \frac{1}{3}, 0, 0, 0\right) + \left[(0, 1, 1, 0, 0), (0, 1, 0, 1, 0), (1, -5, 0, 0, 3) \right].$$

Mohli jsme postupovat také trochu jinak; bylo možné vypočítat ze soustavy (2) neznámé y a x v závislosti na ostatních neznámých, které jsou „volitelné“.

$$y = \frac{1}{3}(1 + 3z + 3u - 5v),$$

$$x = \frac{1}{3}(1 + 3z + 3u - 5v) - z - u + 2v.$$

Nyní zapíšeme neznámé x, y, z, u, v do pětice a upravíme:

$$\begin{aligned} & \left(\frac{1}{3} + \frac{1}{3}v, \frac{1}{3} + z + u - \frac{5}{3}v, z, u, v\right) = \\ & = \left(\frac{1}{3}, \frac{1}{3}, 0, 0, 0\right) + z \cdot (0, 1, 1, 0, 0) + u \cdot (0, 1, 0, 1, 0) + v \cdot \left(\frac{1}{3}, -\frac{5}{3}, 0, 0, 1\right) = \\ & = \left(\frac{1}{3}, \frac{1}{3}, 0, 0, 0\right) + \left[(0, 1, 1, 0, 0), (0, 1, 0, 1, 0), (1, -5, 0, 0, 3) \right]. \end{aligned}$$

13.8. Příklad. Následující soustava lineárních rovnic nad tělesem \mathbb{Z}_3 není řešitelná.

$$\begin{aligned} y+2z+ & 2u+ v = 2, \\ x+ & z+2t+ u+2v = 1, \\ 2x+y+ & z+ t = 2, \\ y+2z & = 0. \end{aligned}$$

Řádkovými elementárními úpravami snadno převedeme rozšířenou matici této soustavy na matici

$$\left(\begin{array}{cccccc|c} 1 & 0 & 1 & 2 & 1 & 2 & 1 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{array} \right),$$

která odpovídá neřešitelné soustavě.

13.9. Příklad. Vyšetřujeme nad tělesem komplexních čísel soustavu lineárních rovnic

$$\begin{aligned}ix + y &= -1, \\3x + 3y - z &= 0, \\2x - y - 2z &= -4 + 3i.\end{aligned}$$

Pro zjednodušení výpočtu přehodíme neznámé (uvažujeme je v pořadí z, x, y) a rovnice; řádkovými elementárními úpravami dospějeme od matice

$$\left(\begin{array}{ccc|c} -1 & 3 & 3 & 0 \\ -2 & 2 & -1 & -4 + 3i \\ 0 & i & 1 & -1 \end{array} \right),$$

k matici

$$\left(\begin{array}{ccc|c} -1 & 3 & 3 & 0 \\ 0 & -4 & -7 & -4 + 3i \\ 0 & 0 & 4 - 7i & -7 - 4i \end{array} \right).$$

Soustava má tedy právě jediné řešení:

$$\begin{aligned}(4 - 7i)y &= -7 - 4i, & \text{tj.} & \quad y = -i, \\-4x + 7i &= -4 + 3i, & \text{tj.} & \quad x = 1 + i, \\z - 3(1 + i) + 3i &= 0, & \text{tj.} & \quad z = 3.\end{aligned}$$

Danou soustavu řeší jediné trojice $(1 + i, -i, 3)$.

13.10. Řešení soustavy s regulární maticí pomocí inverzní matice.

Nechť A je regulární matice řádu n a nechť y je n -tice prvků tělesa T . Podle důsledku 13.5 má soustava rovnic $Ax = y$ právě jediné řešení x , kde $x^T = A^{-1} \cdot y^T$. Řešení soustavy rovnic $Ax = y$ tedy získáme vynásobením sloupce pravých stran maticí A^{-1} zleva. Potíž je v tom, že u dané soustavy rovnic $Ax = y$ se čtvercovou maticí A zpravidla nevíme, zda je matice A regulární nebo singularní. Můžeme však řádkovými elementárními úpravami přejít od matice $(A | y^T)$ k odstupňované matici $(B | z^T)$ a mimo jiné tak zjistit, zda je matice A regulární nebo singularní. Je-li regulární, nemusíme dále postupovat podle Gaussova algoritmu, ale můžeme dalšími řádkovými elementárními úpravami přejít od matice $(B | z^T)$ k matici $(E | A^{-1} \cdot y^T)$ (viz 12.22). Řešení je tak nalezeno. Pokud je matice A singularní (a soustava $Ax = y$ řešitelná), postupujeme podle Gaussova eliminačního algoritmu.

Poznamenejme ještě, že výchozí matice A nemusí být čtvercová, ale může se během elementárních úprav na čtvercovou regulární matici zredukovat (viz následující příklad) a pak je možno užít výše popsanou metodu.

13.11. Příklad. Nad tělesem \mathbb{Z}_7 řešme následující soustavu lineárních rovnic:

$$\begin{aligned} 2x + y + 4z + t &= 1, \\ x + 3y + 6z + 2t &= 3, \\ 3x + 2y + 2z + 2t &= 1, \\ 2x + y + 2z &= 4, \\ 4x + 5y + z + 4t &= 4, \\ 5x + 5y + 3z + 2t &= 4. \end{aligned}$$

Řádkovými elementárními úpravami dojdeme od matice

$$\left(\begin{array}{cccc|c} 1 & 3 & 6 & 2 & 3 \\ 2 & 1 & 4 & 1 & 1 \\ 3 & 2 & 2 & 2 & 1 \\ 2 & 1 & 2 & 0 & 4 \\ 4 & 5 & 1 & 4 & 4 \\ 5 & 5 & 3 & 2 & 4 \end{array} \right) \quad \text{k matici} \quad \left(\begin{array}{cccc|c} 1 & 3 & 6 & 2 & 3 \\ 0 & 2 & 6 & 4 & 2 \\ 0 & 0 & 5 & 3 & 6 \\ 0 & 2 & 4 & 3 & 5 \\ 0 & 0 & 5 & 3 & 6 \\ 0 & 4 & 1 & 6 & 3 \end{array} \right)$$

a dále k matici

$$(B|z^T) = \left(\begin{array}{cccc|c} 1 & 3 & 6 & 2 & 3 \\ 0 & 2 & 6 & 4 & 2 \\ 0 & 0 & 5 & 3 & 6 \\ 0 & 0 & 0 & 3 & 4 \end{array} \right).$$

Nyní jsme dospěli k soustavě lineárních rovnic s regulární maticí. Dále můžeme postupovat dvěma způsoby:

a) Podle Gaussova algoritmu je

$$\begin{aligned} 3t &= 4, & \text{tj.} & \quad t = 6, \\ 5z + 3t &= 6, & \text{tj.} & \quad z = 6, \\ 2y + 6z + 4t &= 2, & \text{tj.} & \quad y = 6, \\ x + 3y + 6z + 2t &= 3, & \text{tj.} & \quad x = 0. \end{aligned}$$

b) Dalšími řádkovými elementárními úpravami přejdeme od matice $(B|z^T)$ k maticím

$$\left(\begin{array}{cccc|c} 1 & 3 & 6 & 2 & 3 \\ 0 & 2 & 6 & 0 & 6 \\ 0 & 0 & 5 & 0 & 2 \\ 0 & 0 & 0 & 1 & 6 \end{array} \right) \quad \cdots \quad \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 6 \\ 0 & 0 & 0 & 1 & 6 \end{array} \right).$$

Poslední sloupec pravých stran dává řešení $(0, 6, 6, 6)$.

13.12. Maticová rovnice typu $AX = Y$.

Nechť A, Y jsou matice typů $n \times m$ a $n \times k$ nad tělesem T . Vyřešit *maticovou rovnici* $AX = Y$ znamená najít všechny matice X typu $m \times k$ nad tělesem T , pro které je součin AX roven matici Y . Násobíme-li matici A prvním sloupcem matice X , dostáváme první sloupec matice Y, \dots , násobíme-li matici A posledním, tj. k -tým sloupcem matice X , dostaneme poslední, tj. k -tý sloupec matice Y . Maticová rovnice $AX = Y$ tedy představuje k soustav lineárních rovnic se stejnou maticí soustavy a k různými pravými stranami. Maticová rovnice $AX = Y$ je tedy řešitelná právě tehdy, když je $r(A|Y) = r(A)$. Matice X je řešením maticové rovnice $AX = Y$ právě tehdy, když pro každé $j = 1, \dots, k$ je j -tý sloupec matice X řešením soustavy lineárních rovnic, která má jako matici soustavy matici A a jako sloupec pravých stran j -tý sloupec matice Y . Množinu všech řešení maticové rovnice $AX = Y$ tedy dostaneme jako množinu všech možných kombinací řešení uvažovaných k soustav lineárních rovnic. Proto je dimenze řešení maticové rovnice $AX = Y$ rovna součinu $k(m - r(A))$. Při řešení maticových rovnic používáme stejné metody jako při řešení soustav lineárních rovnic.

13.13. Příklad. Nad tělesem reálných čísel řešte maticovou rovnici $AX = Y$, kde

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 0 & -1 \\ 1 & 4 & 7 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & 0 \\ 1 & -1 \\ 2 & 1 \end{pmatrix}.$$

Řádkovými elementárními úpravami dojdeme od matice $(A|Y)$ k matici

$$\left(\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 0 & 2 & 4 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{array} \right).$$

Daná maticová rovnost nemá řešení, neboť hodnost matice $(A|Y)$ je větší než hodnost matice A .

13.14. Příklad. Nad tělesem \mathbb{Z}_5 řešte maticovou rovnici $AX = Y$, kde

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Řádkovými úpravami dojdeme od matice $(A|Y)$ k matici

$$\left(\begin{array}{ccc|ccc} 1 & 0 & | & 2 & 3 & 2 \\ 0 & 1 & | & 4 & 3 & 4 \end{array} \right).$$

Užili jsme metodu řešení pomocí inverzní matice. Od matice $(A|Y)$ jsme pomocí řádkových elementárních úprav dospěli k matici $(E|A^{-1}Y)$, kde $X = A^{-1}Y$ je hledané řešení. Daná maticová rovnost má jediné řešení

$$X = \begin{pmatrix} 2 & 3 & 2 \\ 4 & 3 & 4 \end{pmatrix}.$$

13.15. Příklad. Nad tělesem reálných čísel řešte maticovou rovnici $AX = Y$, kde

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \\ -2 & 2 & 2 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & 1 \\ 0 & -2 & -4 \end{pmatrix}.$$

Řádkovými elementárními úpravami dojdeme od matice $(A|Y)$ k matici

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & -1 \\ 0 & -3 & -2 & -1 & 1 & 3 \end{array} \right).$$

Odpovídající maticová rovnice reprezentuje tři soustavy lineárních rovnic, které mají tato řešení:

$$\begin{aligned} (0, 1, -1) + [(1, -2, 3)], \\ (1, -1, 1) + [(1, -2, 3)], \\ (1, -1, 0) + [(1, -2, 3)]. \end{aligned}$$

Všechna řešení maticové rovnice $AX = Y$ mají tedy tvar lineární množiny

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & -1 \\ -1 & 1 & 0 \end{pmatrix} + \left[\begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 0 \\ 3 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & -2 & 0 \\ 0 & 3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -2 \\ 0 & 0 & 3 \end{pmatrix} \right].$$

Řešení můžeme zapsat též v tvaru

$$\begin{pmatrix} a & 1 + b & 1 + c \\ 1 - 2a & -1 - 2b & -1 - 2c \\ -1 + 3a & 1 + 3b & 3c \end{pmatrix},$$

kde a, b, c jsou parametry.

V celém paragrafu jsme se zabývali soustavami lineárních rovnic (resp. maticovými rovnicemi) nad tělesem T , tj. soustavami, ve kterých koeficienty, pravé strany i neznámé byly prvky tělesa T . Ve větě 13.2 byla podána nutná a postačující podmínka pro řešitelnost takové soustavy a popsán tvar množiny všech řešení. Pokud bychom vyšetřovali soustavy lineárních rovnic nad komutativním okruhem (nebo případně oborem integrity), platnost těchto výsledků by se nezachovala. Rovnice $2x = 2$ chápána nad okruhem \mathbb{Z}_4 má dvě řešení $x = 1, x = 3$; rovnice $2x = 1$ nad \mathbb{Z}_4 řešení nemá. Podobně nad oborem integrity \mathbb{Z} nemá rovnice $2x = 1$ řešení. O soustavách lineárních rovnic nad komutativním okruhem se něco málo dozvíme v následujícím paragrafu v partii věnované Cramerovu pravidlu.

14. DETERMINANTY

V této kapitole se budeme věnovat determinantům matic, jejichž prvky jsou brány z nějakého komutativního okruhu R . Tento přístup se nám bude později hodit v kapitole o polynomiálních maticích, tj. maticích nad oborem integrity všech polynomů s koeficienty z tělesa T . Zároveň získáme některé obecnější výsledky (věta o inverzní matici, Cramerovo pravidlo, definice hodnoty matice apod.).

Důkazy většiny tvrzení o determinantech matic nad komutativním okruhem jsou stejné jako důkazy odpovídajících tvrzení o determinantech matic nad tělesem; tímto přístupem se tedy výklad nezkomplikuje.

14.1. Úmluva. V dalším textu budeme slovem okruh a symbolem R značit komutativní okruh, který nemusí mít jednotkový prvek. Na několika místech však zcela formálně uijeme symboly 1 , -1 , δ_{ij} , a to v tomto smyslu: pro $a \in R$ je $(-1)^k a = a$, je-li k sudé, a $(-1)^k a = -a$ (prvek opačný k prvku a), je-li k liché (viz např. definice 14.2, kde tuto roli hraje $\text{sgn } P$).

14.2. Definice. Nechť $A = (a_{ij})$ je čtvercová matice řádu n nad okruhem R . *Determinant* $\det A$ matice A definujeme rovností

$$\det A = \sum_{P \in \mathbb{S}_n} \text{sgn } P \cdot a_{P(1)1} a_{P(2)2} \cdots a_{P(n)n} .$$

Místo $\det A$ píšeme též $\det (a_{ij})$ nebo

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} .$$

Řádem determinantu rozumíme řád odpovídající matice.

Determinant matice $A = (a_{ij})$ nad okruhem R je tedy prvek okruhu R . Je to součet $n!$ součinů

$$\text{sgn } P \cdot a_{P(1)1} a_{P(2)2} \cdots a_{P(n)n}$$

(sčítá se přes všechny permutace $P \in \mathbb{S}_n$); v každém z těchto součinů vystupuje jako činitel právě jediný prvek z každého sloupce a právě jediný prvek z každého řádku matice A .

Poznamenejme, že se slovo determinant užívá i v trochu jiném smyslu; míní se jím do jisté míry i matice, jejíž determinant počítáme. V tomto smyslu někdy mluvíme o řádcích, sloupcích, hlavní a vedlejší diagonále determinantu.

14.3. Poznámka. Pro matice prvního, druhého a třetího řádu je

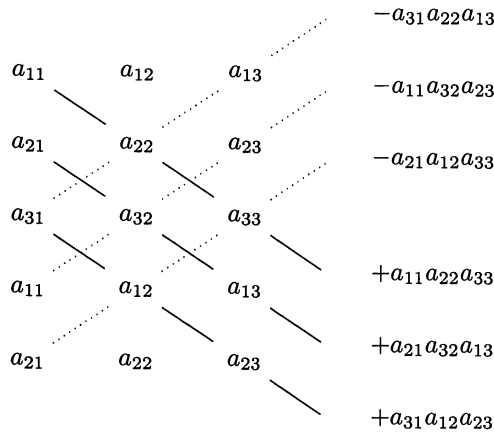
$$|a_{11}| = a_{11} ,$$

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12} ,$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - \\ - a_{31}a_{22}a_{13} - a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33} .$$

Determinant matice prvního řádu je roven prvku, který stojí v matici. Determinant matice druhého řádu je roven rozdílu součinů prvků hlavní a vedlejší diagonály.

Determinant matice třetího řádu můžeme vypočítat podle tzv. *Sarrusova pravidla*. K matici přepíšeme jako čtvrtý a pátý řádek její první a druhý řádek.



Determinant uvažované matice je nyní roven (viz obrázek) součtu šesti prvků okruhu R . První tři jsou součin prvků hlavní diagonály a součiny prvků dvou rovnoběžných linií, ty odpovídají sudým permutacím

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} , \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} , \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} ,$$

druhé tři jsou opačné prvky k součinům prvků vedlejší diagonály a dvou rovnoběžných linií, ty odpovídají lichým permutacím

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} , \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} , \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} .$$

Získáme-li při výpočtu determinantů třetího řádu trochu zběhlosti, není nutné při užití Sarrusova pravidla uvažované řádky k matici opravdu připisovat. Poznamenejme ještě, že Sarrusovo pravidlo bývá často formulováno i pomocí sloupců.

14.4. Příklady.

(i) Podle Sarrusova pravidla vypočteme determinant reálné matice třetího řádu:

$$\begin{vmatrix} 1 & 2 & -3 \\ 4 & -2 & 1 \\ 0 & 3 & 2 \end{vmatrix} =$$

$$= 1 \cdot (-2) \cdot 2 + 4 \cdot 3 \cdot (-3) + 0 \cdot 2 \cdot 1 - 0 \cdot (-2) \cdot (-3) - 1 \cdot 3 \cdot 1 - 4 \cdot 2 \cdot 2 =$$

$$= -4 - 36 - 3 - 16 = -59 .$$

(ii) Krásným příkladem je tato „zrcadlová rovnost“ determinantů druhého řádu v římských číslicích:

$$\begin{vmatrix} \text{X} & \text{IV} \\ \text{II} & \text{I} \end{vmatrix} = \text{II} = \begin{vmatrix} \text{VI} & \text{X} \\ \text{I} & \text{II} \end{vmatrix} .$$

(iii) Vypočteme determinant matice A nad okruhem \mathbb{Z}_4 :

$$A = \begin{pmatrix} 2 & 0 & 1 & 3 \\ 1 & 2 & 3 & 1 \\ 0 & 0 & 2 & 0 \\ 3 & 0 & 1 & 0 \end{pmatrix}$$

Každý součin $\text{sgn } P \cdot a_{P(1)1} a_{P(2)2} a_{P(3)3} a_{P(4)4}$ obsahuje právě jediný prvek z každého sloupce a z každého řádku matice A . Ve druhém sloupci matice A je jediný nenulový prvek $a_{22} = 2$; všechny uvažované součiny, které obsahují jiný prvek z druhého sloupce, jsou rovny nule. Rovněž ve třetím řádku je jediný nenulový prvek $a_{33} = 2$; všechny součiny, které obsahují jiný prvek ze třetího řádku, jsou rovny nule. Ve čtvrtém sloupci už nemůžeme volit prvky a_{24} a a_{34} ; zbývá $a_{14} = 3$ a $a_{44} = 0$. Jediný součin, který může být nenulový, je tedy součin $a_{22} a_{33} a_{14} a_{41} = 2 \cdot 2 \cdot 3 \cdot 3 = 0$, který odpovídá permutaci

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} .$$

Tedy $\det A = 0$.

Při teoretických úvahách i praktických výpočtech je někdy výhodné chápat matici řádu n nad okruhem R , jejíž determinant počítáme, jako n vedle sebe stojících sloupců (n -tic prvků okruhu R neboli prvků množiny R^n). Zavedeme proto následující označení.

14.5. Označení. Nechť R je okruh a $s_1, \dots, s_n \in R^n$. Symbolem $\det(s_1, \dots, s_n)$ budeme rozumět determinant matice, ve které jsou n -tice s_1, \dots, s_n po řadě prvním až n -tým sloupcem.

14.6. Lemma. Nechť A je matice řádu n nad okruhem R a t jeden ze sloupců matice A . Jestliže je $t = t_1 + t_2$, kde $t_1, t_2 \in R^n$, potom je

$$\det A = \det A_1 + \det A_2 ,$$

kde matice A_1 , resp. A_2 vznikne z matice A nahrazením jejího sloupce t sloupcem t_1 , resp. t_2 .

Důkaz. Předpokládejme pro jednoduchost, že t je první sloupec matice $A = (a_{ij})$. Pišme

$$t_1 = (b_{11}, \dots, b_{n1}) , \quad t_2 = (c_{11}, \dots, c_{n1}) ;$$

pro každé $i = 1, \dots, n$ je tedy $a_{i1} = b_{i1} + c_{i1}$. Nyní je

$$\begin{aligned} \det A &= \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot a_{P(1)1} a_{P(2)2} \dots a_{P(n)n} = \\ &= \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot (b_{P(1)1} + c_{P(1)1}) \cdot a_{P(2)2} \dots a_{P(n)n} = \\ &= \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot b_{P(1)1} \cdot a_{P(2)2} \dots a_{P(n)n} + \\ &+ \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot c_{P(1)1} \cdot a_{P(2)2} \dots a_{P(n)n} = \det A_1 + \det A_2 . \quad \square \end{aligned}$$

Tvrzení předchozího lemmatu snadno zobecníme indukcí; užijeme-li označení 14.5, dostáváme:

$$\det(s_1, \dots, s_{i-1}, \sum_{j=1}^k t_j, s_{i+1}, \dots, s_n) = \sum_{j=1}^k \det(s_1, \dots, s_{i-1}, t_j, s_{i+1}, \dots, s_n) .$$

Lemma 14.6 se velmi úspěšně užívá k obecnému odvozování i k výpočtům některých determinantů řádu n .

Nechť $A = (a_{ij})$ je čtvercová matice řádu n . Řekneme, že matice $B = (b_{ij})$ vznikla provedením permutace $Q \in \mathbb{S}_n$ na sloupce (resp. řádky) matice A , jestliže pro každé $i, j = 1, \dots, n$ je $a_{ij} = b_{iQ(j)}$ (resp. $a_{ij} = b_{Q(i)j}$). Permutace Q tedy z j -tého sloupce (resp. i -tého řádku) matice A „udělá“ $Q(j)$ -tý sloupec (resp. $Q(i)$ -tý řádek) matice B .

14.7. Základní vlastnosti determinantů.

- (i) *Determinant matice, která má nulový sloupec (řádek), je roven nule.*
- (ii) *Determinant horní (dolní) trojúhelníkové matice je roven součinu všech prvků na její hlavní diagonále.*
- (iii) *Determinanty navzájem transponovaných matic jsou si rovny.*
- (iv) *Vynásobíme-li nějaký sloupec (řádek) matice A prvkem $c \in R \cup \{-1\}$, je determinant vzniklé matice roven $c \cdot \det A$.*
- (v) *Determinant matice, která má dva stejné sloupce (řádky), je roven nule.*
- (vi) *Přičteme-li k nějakému sloupci (řádku) matice A c -násobek nějakého jiného sloupce (řádku), kde $c \in R \cup \{1, -1\}$, je determinant vzniklé matice roven determinantu matice A .*
- (vii) *Prohodíme-li v matici A dva sloupce (řádky), je determinant vzniklé matice roven $-\det A$.*
- (viii) *Jestliže je A matice řádu n a $c \in R \cup \{-1\}$, pak je $\det(cA) = c^n \cdot \det A$.*
- (ix) *Přičteme-li k nějakému sloupci (řádku) matice A lineární kombinaci ostatních sloupců (řádků) matice A s koeficienty $c \in R \cup \{1, -1\}$, je determinant vzniklé matice roven determinantu matice A .*
- (x) *Jestliže matice B vznikla provedením permutace Q na sloupce (resp. řádky) matice A , potom je $\det B = \operatorname{sgn} Q \cdot \det A$.*
- (xi) *Matice A nad tělesem T je singulární právě tehdy, je-li její determinant roven nule, a regulární právě tehdy, když je její determinant nenulový.*

Důkaz. Nechť $A = (a_{ij})$ je matice řádu n na okruhem R .

- (i) Jestliže má matice A nulový sloupec nebo řádek, pak každý součin

$$\operatorname{sgn} P \cdot a_{P(1)1} a_{P(2)2} \cdots a_{P(n)n}$$

obsahuje nějaký prvek z tohoto nulového sloupce (řádku); je tedy $\det A = 0$.

(ii) Jestliže je A horní (dolní) trojúhelníková matice, potom jediná permutace P , pro kterou může být součin $a_{P(1)1} a_{P(2)2} \cdots a_{P(n)n}$ nenulový, je permutace identická. Odtud vyplývá rovnost $\det A = a_{11} a_{22} \cdots a_{nn}$.

(iii) Determinant matice A je součet $n!$ součinů prvků matice A braných po jednom z každého řádku a z každého sloupce a opatřených znaménkem příslušné permutace. Každý z těchto součinů je tedy jedním z $n!$ součinů tvořících determinant matice A^T . Označme $A^T = (b_{ij})$, tj. $b_{ij} = a_{ji}$ pro každé $i, j = 1, \dots, n$. Podle definice determinantu je

$$\begin{aligned} \det A &= \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot a_{P(1)1} a_{P(2)2} \cdots a_{P(n)n} = \\ &= \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot b_{1P(1)} b_{2P(2)} \cdots b_{nP(n)}. \end{aligned}$$

Nyní využijeme komutativitu násobení v okruhu R a změníme pořadí činitelů v součinu $b_{1P(1)}b_{2P(2)}\dots b_{P(n)n}$ (seřadíme činitele podle sloupcových indexů); užijeme též rovnosti $\operatorname{sgn} P = \operatorname{sgn} P^{-1}$. Je tedy

$$\det A = \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P^{-1} \cdot b_{P^{-1}(1)1} b_{P^{-1}(2)2} \dots b_{P^{-1}(n)n} .$$

Probíhá-li permutace P množinu \mathbb{S}_n , probíhá i permutace $P^{-1} = Q$ množinu \mathbb{S}_n , takže je

$$\det A = \sum_{Q \in \mathbb{S}_n} \operatorname{sgn} Q \cdot b_{Q(1)1} b_{Q(2)2} \dots b_{Q(n)n} = \det A^T .$$

(iv) Vynásobme i -tý sloupec matice A prvkem $c \in R \cup \{-1\}$; vzniklou matici označme symbolem B . Nyní je

$$\begin{aligned} \det B &= \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot a_{P(1)1} \dots (c \cdot a_{P(i)i}) \dots a_{P(n)n} = \\ &= c \cdot \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot a_{P(1)1} \dots a_{P(i)i} \dots a_{P(n)n} = c \cdot \det A . \end{aligned}$$

(v) Předpokládejme, že matice A má stejný i -tý a j -tý sloupec, kde $i < j$; pro každé $k = 1, \dots, n$ je tedy $a_{ki} = a_{kj}$. Nechť $Q \in \mathbb{S}_n$ je transpozice, která zaměňuje i a j . Všechny prvky grupy \mathbb{S}_n uspořádáme do dvojic P, PQ , kde P probíhá všechny sudé permutace; permutace PQ pak probíhá všechny liché permutace (viz 6.8). Těmto dvojicím permutací odpovídají při tvoření determinantu $\det A$ součiny, které se ruší:

$$\begin{aligned} \operatorname{sgn} PQ \cdot a_{PQ(1)1} \dots a_{PQ(i)i} \dots a_{PQ(j)j} \dots a_{PQ(n)n} &= \\ = -a_{P(1)1} \dots a_{P(j)i} \dots a_{P(i)j} \dots a_{P(n)n} &= \\ = -a_{P(1)1} \dots a_{P(j)j} \dots a_{P(i)i} \dots a_{P(n)n} &= \\ = -\operatorname{sgn} P \cdot a_{P(1)1} \dots a_{P(n)n} . \end{aligned}$$

Determinant matice A je tedy roven nule.

(vi) Předpokládejme, že např. ke druhému sloupci přičteme c -násobek prvního sloupce. Podle lemmatu 14.6 a tvrzení (iv) a (v) je

$$\begin{aligned} \det(s_1, s_2 + c \cdot s_1, \dots, s_n) &= \det(s_1, s_2, \dots, s_n) + c \cdot \det(s_1, s_1, \dots, s_n) = \\ &= \det(s_1, s_2, \dots, s_n) . \end{aligned}$$

(vii) Prohození i -tého a j -tého sloupce matice A dosáhneme takto (viz poznámka za 12.11): Přičteme i -tý sloupec k j -tému, odečteme j -tý sloupec od i -tého, přičteme i -tý sloupec k j -tému a i -tý sloupec vynásobíme číslem -1 . Podle tvrzení (vi) se

při prvních třech úpravách determinant nezmění. Při čtvrté úpravě změní podle tvrzení (iv) znaménko.

(viii)–(x) Tato tvrzení vyplývají z předchozích tvrzení. Vzhledem k tomu, že každou sudou, resp. lichou permutací je možno složit ze sudého, resp. lichého počtu transpozic, vyplývá z tvrzení (vii) tvrzení (x).

(xi) Připomeňme nejprve, že pojem singulární a regulární matice jsme zatím definovali pouze pro matice nad tělesem (pro matice nad okruhem tyto pojmy zavedeme až v 14.22). Jestliže je matice A singulární, je některý její sloupec lineární kombinací ostatních sloupců. Odečteme-li od tohoto sloupce zmíněnou lineární kombinaci, dostaneme matici s nulovým sloupcem, jejíž determinant je podle tvrzení (i) roven nule. Determinant této matice je však podle tvrzení (ix) roven determinantu matice A . Jestliže je matice A regulární, můžeme ji elementárními úpravami převést na jednotkovou matici (viz 12.21), jejíž determinant je roven jedné. Protože elementární úpravy zachovávají nulovost a nenulovost determinantu, je determinant regulární matice nenulový. Viz též 14.19.

Platnost tvrzení (iv)–(x) ve formulacích pro řádky vyplývá z již dokázaných tvrzení pro sloupce a z tvrzení (iii). \square

Výpočet determinantů můžeme provádět přímo podle definice, jak už bylo ukázáno pro determinanty prvního, druhého a třetího řádu (viz 14.3 a 14.4). Velmi užitečná metoda výpočtu determinantů se zakládá na výše uvedených základních vlastnostech determinantů (viz 14.7): elementárními úpravami přejdeme od dané matice k matici odstupňované (trojúhelníkové) (viz 12.17) a determinant dané matice nyní vypočteme podle tvrzení (ii) s přihlédnutím k úpravám, které jsme provedli — viz tvrzení (iv)–(x). Výpočet tohoto typu je uveden v následujícím příkladu.

14.8. Příklad. Vypočteme determinant matice

$$A = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 2 & 2 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 2 & 2 & 1 & 2 \end{pmatrix}$$

nad tělesem \mathbb{Z}_3 a nad okruhem \mathbb{Z}_4 .

Na tělesem \mathbb{Z}_3 : Dvojnásobek prvního řádku přičteme ke druhému a čtvrtému řádku, první řádek přičteme ke třetímu. Potom přičteme druhý řádek ke třetímu a dvojnásobek druhého řádku ke čtvrtému. Dostáváme determinant matice se dvěma stejnými řádky, který je roven nule.

$$\det A = \begin{vmatrix} 2 & 1 & 1 & 0 \\ 2 & 2 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 2 & 2 & 1 & 2 \end{vmatrix} = \begin{vmatrix} 2 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{vmatrix} = \begin{vmatrix} 2 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{vmatrix} = 0$$

Nad okruhem \mathbb{Z}_4 : Nejprve přehodíme první a třetí řádek, potom přičteme dvojnásobek prvního řádku ke druhému, třetímu a čtvrtému řádku. Přehodíme druhý a třetí řádek. Potom přičteme dvojnásobek čtvrtého řádku ke třetímu a nakonec přehodíme třetí a čtvrtý řádek. Přehození řádků vždy změní znaménko.

$$\begin{aligned} \det A &= - \begin{vmatrix} 1 & 1 & 1 & 0 \\ 2 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 2 & 2 & 1 & 2 \end{vmatrix} = - \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 3 & 3 & 0 \\ 0 & 0 & 3 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 3 & 3 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 3 & 2 \end{vmatrix} = \\ &= \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 3 & 3 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 2 \end{vmatrix} = - \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 3 & 3 & 0 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 \end{vmatrix} = -1 \cdot 3 \cdot 3 \cdot 1 = 3 \end{aligned}$$

14.9. Věta. *Determinant horní (dolní) trojúhelníkové blokové matice je roven součinu determinantů všech jejích bloků stojících na diagonále.*

Důkaz. Uvažujme matici

$$A = \begin{pmatrix} B & C \\ O & D \end{pmatrix},$$

kde B je čtvercová matice řádu n , D čtvercová matice řádu m a O nulová matice typu $m \times n$. Pišme $A = (a_{ij})$, $B = (b_{ij})$ a $D = (d_{kl})$. Je tedy

$$\begin{aligned} b_{ij} &= a_{ij} && \text{pro } i, j = 1, \dots, n, \\ d_{kl} &= a_{n+k, n+l} && \text{pro } k, l = 1, \dots, m. \end{aligned}$$

Podle definice determinantu je

$$\det A = \sum_{P \in \mathbb{S}_{n+m}} \operatorname{sgn} P \cdot a_{P(1)1} a_{P(2)2} \dots a_{P(n+m), n+m}.$$

V tomto součtu mohou být nenuloví pouze ti sčítanci, pro které se v součinu $a_{P(1)1} a_{P(2)2} \dots a_{P(n+m), n+m}$ nevyskytuje prvek z nulové matice O , tj. členy, pro které je

$$P(1) \leq n, \dots, P(n) \leq n$$

a tedy rovněž

$$P(n+1) > n, \dots, P(n+m) > n.$$

Můžeme tedy sčítat jen přes všechny permutace, které permutují zvlášť čísla $1, 2, \dots, n$ a zvlášť čísla $n+1, \dots, n+m$. Pro takovouto permutaci $P \in \mathbb{S}_{n+m}$ definujeme permutace $Q \in \mathbb{S}_n$ a $T \in \mathbb{S}_m$ takto:

$$\begin{aligned} Q(i) &= P(i) && \text{pro } i = 1, \dots, n, \\ T(i) &= P(i+n) - n && \text{pro } i = 1, \dots, m. \end{aligned}$$

Vzhledem k tomu, že permutace P permutuje zvlášť čísla $1, \dots, n$ a zvlášť čísla $n+1, \dots, n+m$, je $\text{in } P = \text{in } Q + \text{in } T$ a tedy $\text{sgn } P = \text{sgn } Q \cdot \text{sgn } T$. Probíhá-li P uvažovanou množinou permutací, probíhá Q grupu \mathbb{S}_n a T grupu \mathbb{S}_m a naopak. Je tedy

$$\begin{aligned} \det A &= \sum_{Q \in \mathbb{S}_n} \sum_{T \in \mathbb{S}_m} \text{sgn } Q \cdot \text{sgn } T \cdot a_{Q(1)1} \dots a_{Q(n)n} \cdot a_{T(1)+n,1+n} \dots a_{T(m)+n,m+n} = \\ &= \sum_{Q \in \mathbb{S}_n} \text{sgn } Q \cdot b_{Q(1)1} \dots b_{Q(n)n} \cdot \sum_{T \in \mathbb{S}_m} \text{sgn } T \cdot d_{T(1)1} \dots d_{T(m)m} = \\ &= \det B \cdot \det D . \end{aligned}$$

Indukcí se uvedené tvrzení dokáže pro libovolný počet bloků stojících na diagonále horní trojúhelníkové blokové matice. Protože jsou si determinanty navzájem transponovaných matic rovny, platí uvedené tvrzení i pro dolní trojúhelníkové blokové matice. \square

14.10. Příklad. Vypočtěme determinant matice

$$A = \begin{pmatrix} 2 & 2 & 1 & 6 & 4 & 3 \\ 3 & 1 & 5 & 0 & 1 & 4 \\ 0 & 0 & 6 & 5 & 2 & 7 \\ 0 & 0 & 3 & 2 & 5 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 3 & 7 \end{pmatrix}$$

nad okruhem \mathbb{Z}_8 .

Podle předchozí věty je

$$\det A = \begin{vmatrix} 2 & 2 \\ 3 & 1 \end{vmatrix} \cdot \begin{vmatrix} 6 & 5 \\ 3 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 \\ 3 & 7 \end{vmatrix} = (2-6)(4-7)(7-0) = 4 \cdot 5 \cdot 7 = 4 .$$

14.11. Věta o rozvoji determinantu. *Nechť $A = (a_{ij})$ je matice řádu $n > 1$ nad okruhem R . Pro každé $j = 1, \dots, n$ je*

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det A_{ij} , \quad (1)$$

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{ji} \det A_{ji} , \quad (2)$$

kde A_{ij} je matice řádu $n - 1$, která vznikne z matice A vypuštěním jejího i -tého řádku a j -tého sloupce.

Důkaz. Představíme si j -tý sloupec matice A jako součet n sloupců: v každém z nich je jediný prvek a_{ij} a jinak samé nuly. Podle lemmatu 14.6 je

$$\det A = \sum_{i=1}^n \det B_i ,$$

kde B_i , $i = 1, \dots, n$, je matice, která se od matice A liší pouze j -tým sloupcem, ve kterém má na místě ij prvek a_{ij} a na ostatních místech samé nuly. Na sloupci matice B_i provedeme permutaci

$$\begin{pmatrix} 1 & 2 & \dots & j-1 & j & j+1 & \dots & n \\ 2 & 3 & \dots & j & 1 & j+1 & \dots & n \end{pmatrix} ,$$

která má znaménko $(-1)^{j-1}$, a na řádky vzniklé matice provedeme permutaci

$$\begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & n \\ 2 & 3 & \dots & i & 1 & i+1 & \dots & n \end{pmatrix} ,$$

která má znaménko $(-1)^{i-1}$ (j -tý sloupec jsme dali na první místo a ostatní sloupce „posunuli“, i -tý řádek jsme dali na první místo a ostatní řádky „posunuli“). Dostaneme matici C_i , která má v levém horním rohu prvek a_{ij} a na ostatních místech v prvním sloupci samé nuly. Vynecháním prvního řádku a prvního sloupce matice C_i dostaneme totéž jako při vynechání i -tého řádku a j -tého sloupce matice A (resp. matice B_i), sice matici A_{ij} . Podle tvrzení 14.7(x) a věty 14.9 je

$$\det B_i = (-1)^{j-1} \cdot (-1)^{i-1} \cdot \det C_i = (-1)^{i+j} \cdot a_{ij} \cdot \det A_{ij}$$

a odtud

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det A_{ij} .$$

Druhou rovnost uvedenou ve větě je možno dokázat obdobným postupem; vyplývá však z rovnosti první a ze vztahu $\det A^T = \det A$. \square

Rovnost (1), resp. (2) uvedená v předchozí větě vyjadřuje *rozvoj determinantu podle j -tého sloupce*, resp. *podle j -tého řádku*. Prvek $(-1)^{i+j} \det A_{ij}$ se často nazývá *algebraický doplněk* prvku a_{ij} .

Poznamenejme, že determinant libovolné čtvercové matice, která vznikne z matice A vynecháním nějakých sloupců a řádků, se nazývá *subdeterminant* nebo též *minor* matice A . *Řádem subdeterminantu* budeme rozumět řád odpovídající matice.

Věta o rozvoji dává další metodu pro počítání determinantů; výpočet determinantu řádu n se rozvojem převede na výpočet n determinantů řádu $n - 1$.

14.12. Příklady.

(i) Determinant matice A nad tělesem \mathbb{Z}_3 z příkladu 14.8 rozvedeme podle druhého řádku:

$$\begin{aligned} \det A &= (-1)^3 \cdot 2 \cdot \begin{vmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 2 & 1 & 2 \end{vmatrix} + (-1)^4 \cdot 2 \cdot \begin{vmatrix} 2 & 1 & 0 \\ 1 & 1 & 0 \\ 2 & 1 & 2 \end{vmatrix} + (-1)^6 \cdot 1 \cdot \begin{vmatrix} 2 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 2 & 1 \end{vmatrix} = \\ &= 0 + 2 \cdot (1 + 0 + 0 - 0 - 2 - 0) + 1 \cdot (2 + 2 + 2 - 2 - 1 - 1) = 0 + 1 + 2 = 0 \end{aligned}$$

Mohli jsme však postupovat i jinak. Rozvojem podle čtvrtého sloupce dostaneme:

$$\begin{aligned} \det A &= (-1)^6 \cdot 1 \cdot \begin{vmatrix} 2 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 2 & 1 \end{vmatrix} + (-1)^8 \cdot 2 \cdot \begin{vmatrix} 2 & 1 & 1 \\ 2 & 2 & 0 \\ 1 & 1 & 1 \end{vmatrix} = \\ &= 1 \cdot (2 + 2 + 2 - 2 - 1 - 1) + 2 \cdot (1 + 2 + 0 - 2 - 0 - 2) = 2 + 1 = 0 \end{aligned}$$

(ii) Rozvojem podle třetího sloupce vypočteme následující determinant reálné matice s parametry a, b, c, d :

$$\begin{aligned} \begin{vmatrix} 2 & 1 & c & 2 \\ 2 & 2 & a & 2 \\ -1 & 2 & b & 1 \\ 1 & 2 & d & 1 \end{vmatrix} &= c \begin{vmatrix} 2 & 2 & 2 \\ -1 & 2 & 1 \\ 1 & 2 & 1 \end{vmatrix} - a \begin{vmatrix} 2 & 1 & 2 \\ -1 & 2 & 1 \\ 1 & 2 & 1 \end{vmatrix} + b \begin{vmatrix} 2 & 1 & 2 \\ 2 & 2 & 2 \\ 1 & 2 & 1 \end{vmatrix} - d \begin{vmatrix} 2 & 1 & 2 \\ 2 & 2 & 2 \\ -1 & 2 & 1 \end{vmatrix} = \\ &= 6a - 4c - 4d \end{aligned}$$

(iii) Determinant matice A nad okruhem \mathbb{Z}_6 , kde

$$A = \begin{pmatrix} 1 & 1 & 3 & 4 \\ 3 & 2 & 2 & 5 \\ 5 & 0 & 1 & 2 \\ 2 & 3 & 0 & 5 \end{pmatrix},$$

rozvedeme podle třetího řádku. Dostáváme:

$$\begin{aligned} \det A &= (-1)^4 \cdot 5 \cdot \begin{vmatrix} 1 & 3 & 4 \\ 2 & 2 & 5 \\ 3 & 0 & 5 \end{vmatrix} + (-1)^6 \cdot 1 \cdot \begin{vmatrix} 1 & 1 & 4 \\ 3 & 2 & 5 \\ 2 & 3 & 5 \end{vmatrix} + (-1)^7 \cdot 2 \cdot \begin{vmatrix} 1 & 1 & 3 \\ 3 & 2 & 2 \\ 2 & 3 & 0 \end{vmatrix} = \\ &= 5 \cdot (4 + 0 + 3 - 0 - 0 - 0) + 1 \cdot (4 + 0 + 4 - 4 - 3 - 3) - 2 \cdot (0 + 3 + 4 - 0 - 0 - 0) = \\ &= 5 - 2 - 2 = 1 \end{aligned}$$

Srovnejte nyní předchozí výpočet s následujícím: Ke druhému řádku přičteme trojnásobek prvního řádku, ke třetímu řádku přičteme první řádek a ke čtvrtému řádku

přičteme čtyřnásobek prvního řádku. Potom přičteme druhý řádek ke třetímu a ke čtvrtému řádku a nakonec užijeme větu 14.9:

$$\det A = \begin{vmatrix} 1 & 1 & 3 & 4 \\ 0 & 5 & 5 & 5 \\ 0 & 1 & 4 & 0 \\ 0 & 1 & 0 & 3 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 3 & 4 \\ 0 & 5 & 5 & 5 \\ 0 & 0 & 3 & 5 \\ 0 & 0 & 5 & 2 \end{vmatrix} = 1 \cdot 5 \cdot \begin{vmatrix} 3 & 5 \\ 5 & 2 \end{vmatrix} = 1 \cdot 5 \cdot (0 - 1) = 1$$

Poznamenejme, že pojem determinantu je možno definovat také indukci. Je-li $A = (a)$ matice prvního řádu, definujeme $\det A = a$. Je-li $A = (a_{ij})$ matice řádu n , definujeme

$$\det A = \sum_{i=1}^n (-1)^{1+i} a_{1i} \det A_{1i} ,$$

tj. determinant matice řádu $n > 1$ je popsán rozvojem podle prvního řádku. Je však potom třeba dokázat mimo jiné větu o rozvoji determinantu podle libovolného řádku a podle libovolného sloupce.

V následující větě zobecníme tvrzení o rozvoji determinantu. Dostaneme rovnosti, které se někdy hodí při teoretickém odvozování.

14.13. Věta. *Nechť $A = (a_{ij})$ je matice řádu n nad okruhem R . Potom pro každé $j, k = 1, \dots, n$ je*

$$\sum_{i=1}^n (-1)^{i+j} a_{ik} \det A_{ij} = \delta_{jk} \cdot \det A ,$$

$$\sum_{i=1}^n (-1)^{i+j} a_{ki} \det A_{ji} = \delta_{jk} \cdot \det A .$$

Důkaz. Pro $j = k$ jde o rozvoje determinantu podle j -tého sloupce, resp. j -tého řádku (viz 14.11). Jestliže je $j \neq k$, potom je podle 14.11 uvedená suma rovna determinantu matice, která má nahrazen j -tý sloupec (j -tý řádek) k -tým sloupcem (k -tým řádkem) a má tedy dva stejné sloupce (řádky); uvažovaný determinant je proto roven nule. \square

14.14. Věta o násobení determinantů. *Determinant součinu dvou matic téhož řádu nad okruhem R je roven součinu determinantů těchto dvou matic.*

Důkaz. Nechť A a B jsou čtvercové matice nad okruhem R , které mají řád n . Označme s_1, \dots, s_n sloupce matice A a pišme $B = (b_{ij})$. Uvědomme si, že j -tý sloupec matice AB je lineární kombinací sloupců matice A s koeficienty b_{1j}, \dots, b_{nj} , které jsou prvky j -tého sloupce matice B . Při označení zavedeném v 14.5 je tedy

$$\det AB = \det \left(\sum_{i_1=1}^n b_{i_1 1} s_{i_1} , \sum_{i_2=1}^n b_{i_2 2} s_{i_2} , \dots , \sum_{i_n=1}^n b_{i_n n} s_{i_n} \right) =$$

$$= \sum_{i_1=1}^n \sum_{i_2=1}^n \dots \sum_{i_n=1}^n b_{i_1 1} b_{i_2 2} \dots b_{i_n n} \cdot \det(s_{i_1}, s_{i_2}, \dots, s_{i_n}) .$$

Vzhledem k tomu, že determinant matice se dvěma stejnými sloupci je roven nule, je možno počítat přes všechny možné permutace

$$P = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \in \mathbb{S}_n.$$

Tedy

$$\det AB = \sum_{P \in \mathbb{S}_n} b_{P(1)1} b_{P(2)2} \dots b_{P(n)n} \cdot \det (s_{P(1)}, \dots, s_{P(n)}).$$

Nyní využijeme tvrzení 14.7(x) o permutaci sloupců a dostáváme

$$\det AB = \sum_{P \in \mathbb{S}_n} b_{P(1)1} \dots b_{P(n)n} \cdot \operatorname{sgn} P \cdot \det (s_1, s_2, \dots, s_n) = \det A \cdot \det B. \quad \square$$

Matematickou indukcí dostáváme, že determinant součinu n čtvercových matic téhož řádu je roven součinu determinantů těchto matic a že determinant n -té mocniny čtvercové matice je roven n -té mocnině determinantu této matice.

14.15. Poznámka. Věta o násobení determinantů se dokazuje různými způsoby. Jde-li o matice nad okruhem s jednotkovým prvkem, můžeme postupovat také takto. Utvoříme blokovou matici

$$X = \begin{pmatrix} A & O \\ -E & B \end{pmatrix}$$

řádu $2n$, jejíž determinant je podle věty 14.9 roven $\det A \cdot \det B$. V této blokové matici budeme provádět sloupcové elementární úpravy. Lineární kombinaci prvních n sloupců matice X s koeficienty, které stojí v prvním sloupci matice B , přičteme k $(n+1)$ -nímu sloupci, \dots , lineární kombinaci prvních n sloupců s koeficienty, které stojí v n -tém sloupci matice B , přičteme k $2n$ -tému sloupci. Dojdeme tak k matici

$$Y = \begin{pmatrix} A & AB \\ -E & O \end{pmatrix}.$$

Provedeme-li na řádky této matice permutaci

$$P = \begin{pmatrix} 1 & 2 & \dots & n & n+1 & \dots & 2n \\ n+1 & n+2 & \dots & 2n & 1 & \dots & n \end{pmatrix},$$

jejíž znaménko je $(-1)^{n^2}$, získáme matici

$$Z = \begin{pmatrix} -E & O \\ A & AB \end{pmatrix}.$$

Podle vět 14.9 a 14.7 je nyní

$$\det A \cdot \det B = \det X = \det Y = (-1)^{n^2} \cdot \det Z = (-1)^{n^2} (-1)^n \cdot \det AB = \det AB .$$

Pro matice nad tělesem můžeme provést důkaz věty o násobení determinantů ještě jiným způsobem. Musíme si však uvědomit, že determinant singulární matice je roven nule (viz 14.7(xi)).

Jestliže je matice A singulární, je podle věty 12.7 i matice AB singulární, takže $\det AB = \det A \cdot \det B = 0$.

Jestliže je matice A regulární, je podle věty 12.21 součinem elementárních transformačních matic. Vzhledem k principu matematické indukce stačí předpokládat, že A je přímo elementární transformační maticí. Je-li A elementární transformační maticí prvního, resp. druhého typu, vyplývá rovnost $\det AB = \det A \cdot \det B$ z vlastnosti 14.7(iv), resp. 14.7(vi).

14.16. Definice. Nechť $A = (a_{ij})$ je čtvercová matice řádu $n > 1$ nad okruhem R . *Reciprokovou maticí* k matici A budeme rozumět matici A_{rec} řádu n , ve které na místě ij stojí algebraický doplněk prvku a_{ji} matice A , tj. prvek $(-1)^{i+j} \det A_{ji}$.

14.17. Věta. *Nechť A je čtvercová matice řádu $n > 1$ nad okruhem R . Potom platí:*

- (i) $A \cdot A_{\text{rec}} = A_{\text{rec}} \cdot A = \det A \cdot E$.
- (ii) *Jestliže se prvkem $\det A$ dá v okruhu R krátit, potom je*

$$\det A_{\text{rec}} = (\det A)^{n-1} .$$

Důkaz. Pišme $A = (a_{ij})$ a $A_{\text{rec}} = (b_{ij})$, tj. pro každé $i, j = 1, \dots, n$ je

$$b_{ij} = (-1)^{i+j} \det A_{ji} .$$

V součinu $A_{\text{rec}}A$ je podle věty 14.13 na místě jk prvek

$$\sum_{i=1}^n b_{ji} a_{ik} = \sum_{i=1}^n (-1)^{i+j} a_{ik} \det A_{ij} = \delta_{jk} \cdot \det A ,$$

v součinu $A \cdot A_{\text{rec}}$ je podle téže věty na místě kj prvek

$$\sum_{i=1}^n a_{ki} b_{ij} = \sum_{i=1}^n (-1)^{i+j} a_{ki} \det A_{ji} = \delta_{jk} \cdot \det A .$$

Tvrzení (i) tedy platí.

Podle věty o násobení determinantů vyplývá z tvrzení (i) rovnost

$$\det A \cdot \det A_{\text{rec}} = (\det A)^n .$$

Jestliže je tedy prvkem $\det A$ možno v okruhu R krátit, je

$$\det A_{\text{rec}} = (\det A)^{n-1} . \quad \square$$

Nad okruhem s jednotkovým prvkem má smysl mluvit o jednotkové matici a tedy i o invertibilních a inverzních maticích.

14.18. Věta. *Nechť R je okruh s jednotkovým prvkem a A čtvercová matice nad okruhem R . Matice A je nad okruhem R invertibilní právě tehdy, když je její determinant $\det A$ invertibilním prvkem okruhu R . Nastane-li tento případ, je*

$$A^{-1} = (\det A)^{-1} \cdot A_{\text{rec}} .$$

Důkaz. Jestliže je matice A nad okruhem R invertibilní, tj. existuje-li matice A^{-1} , pak je $A \cdot A^{-1} = E$. Podle věty o násobení determinantů je

$$\det A \cdot \det A^{-1} = 1 ,$$

tj. prvek $\det A$ je v okruhu R invertibilní.

Jestliže je naopak $\det A$ invertibilním prvkem okruhu R , je podle věty 14.17(i)

$$A \cdot ((\det A)^{-1} A_{\text{rec}}) = ((\det A)^{-1} A_{\text{rec}}) \cdot A = E ,$$

tj. matice $(\det A)^{-1} A_{\text{rec}}$ je k matici A inverzní. \square

Aplikujeme-li předchozí větu na různé okruhy, dostáváme užitečná kritéria pro invertibilitu matic.

14.19. Důsledek.

- (i) *Matice je nad tělesem invertibilní (neboli regulární) právě tehdy, když je její determinant nenulový.*
- (ii) *Matice je nad oborem integrity celých čísel invertibilní právě tehdy, když je její determinant roven buď 1 nebo -1 .*
- (iii) *Matice je nad oborem integrity Gaussových celých čísel invertibilní právě tehdy, když je její determinant roven některému z čísel $1, -1, i, -i$.*
- (iv) *Matice je nad oborem integrity $T[x]$ polynomů jedné neurčité x s koeficienty z tělesa T invertibilní právě tehdy, když je její determinant roven nenulovému prvku tělesa T .*

Důkaz. K důkazu všech čtyř tvrzení stačí připomenout, že invertibilními prvky v tělese jsou právě všechny nenulové prvky, invertibilními prvky v oboru integrity celých čísel jsou právě čísla 1 a -1 , invertibilními prvky v oboru integrity Gaussových celých čísel jsou právě čísla $1, -1, i, -i$ a invertibilními prvky v $T[x]$ jsou právě všechny nenulové prvky tělesa T . \square

14.20. Příklad.

(i) Celočíselná matice

$$A = \begin{pmatrix} 1 & 0 & 1 \\ -2 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

je v oboru integrity celých čísel invertibilní, neboť $\det A = -1$. K výpočtu matice A^{-1} musíme podle věty 14.18 znát všechny subdeterminanty druhého řádu matice A :

$$\begin{array}{lll} \det A_{11} = 1 & \det A_{12} = -2 & \det A_{13} = -2 \\ \det A_{21} = -1 & \det A_{22} = 1 & \det A_{23} = 1 \\ \det A_{31} = -1 & \det A_{32} = 2 & \det A_{33} = 1 \end{array}$$

Podle věty 14.18 je tedy

$$A^{-1} = (\det A)^{-1} \cdot \begin{pmatrix} \det A_{11} & -\det A_{21} & \det A_{31} \\ -\det A_{12} & \det A_{22} & -\det A_{32} \\ \det A_{13} & -\det A_{23} & \det A_{33} \end{pmatrix} = \begin{pmatrix} -1 & -1 & 1 \\ -2 & -1 & 2 \\ 2 & 1 & -1 \end{pmatrix}.$$

(ii) Podle věty 14.18 se snadno vypočte inverzní matice k invertibilní matici druhého řádu. Je-li matice

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

invertibilní, je

$$A^{-1} = (ad - bc)^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

(iii) Matice

$$A = \begin{pmatrix} 1 & 1 & 4 \\ 0 & 1 & 0 \\ 1 & 1 & 3 \end{pmatrix}$$

nad okruhem \mathbb{Z}_6 je invertibilní. Je $\det A = 5$ a

$$A^{-1} = \begin{pmatrix} 3 & 5 & 4 \\ 0 & 1 & 0 \\ 1 & 0 & 5 \end{pmatrix}.$$

(iv) Matice

$$A = \begin{pmatrix} 1 & x & x^2 \\ 0 & 2 & 0 \\ 0 & 2x & 3 \end{pmatrix}$$

nad $\mathbb{R}[x]$ je invertibilní. Je $\det A = 6$ a

$$A^{-1} = \frac{1}{6} \cdot \begin{pmatrix} 6 & 2x^3 - 3x & -2x^2 \\ 0 & 3 & 0 \\ 0 & -2x & 2 \end{pmatrix}.$$

Při výpočtech inverzních matic k maticím řádu $n \geq 3$ nad tělesem je výhodnější užít metodu elementárních úprav, která byla vyložena v 12.22. Při teoretických úpravách a odvozeních je však velmi užitečné, známe-li popis inverzní matice, který je dán ve větě 14.18.

První tvrzení důsledku 14.19 říká jinými slovy toto: čtvercová matice řádu n nad tělesem T má hodnotu n právě tehdy, když je její determinant nenulový. Toto tvrzení nyní podstatně zobecníme; hodnotu libovolné (obdélníkové) matice nad tělesem T vyjádříme pomocí nulovosti či nenulovosti jejích subdeterminantů.

14.21. Věta. *Nenulová matice A nad tělesem T má hodnotu k právě tehdy, když platí:*

- (i) *V matici A existuje nenulový subdeterminant řádu k .*
- (ii) *Všechny subdeterminanty matice A , které mají řád větší než k , jsou rovny nule.*

Důkaz. Nechť A je nenulová matice nad tělesem T , která má hodnotu h , a necht' k je přirozené číslo s vlastnostmi (i), (ii) uvedenými ve větě.

V matici A existuje nenulový subdeterminant řádu k . Odpovídající čtvercová matice B řádu k je tedy podle důsledku 14.19(i) invertibilní, tj. regulární, její sloupce jsou tedy lineárně nezávislé. Sloupce matice A , které maticí B procházejí, jsou proto také lineárně nezávislé a tedy $h \geq k$.

V matici A existuje h lineárně nezávislých sloupců. Vyškrtnutím ostatních sloupců dostaneme matici hodnoty h . V této matici existuje h lineárně nezávislých řádků (viz 12.27). Vyškrtnutím ostatních řádků dostaneme čtvercovou regulární matici řádu h . Její determinant je podle důsledku 14.19(i) nenulový, takže $h \leq k$. \square

Hodnota nenulové matice A nad tělesem T je tedy rovna největšímu přirozenému číslu z množiny řádů všech nenulových subdeterminantů matice A . Jestliže má matice A hodnotu k , potom pro každé $i = 1, \dots, k$ v matici A existuje nenulový subdeterminant řádu i (toto tvrzení ihned vyplývá z věty o rozvoji determinantu).

Ve větě 14.21 je vyjádřena hodnota matice nad tělesem T na základě nulovosti či nenulovosti jejích subdeterminantů. Připomeňme, že pojem hodnoty matice byl definován (viz 12.1) pouze pro matice nad tělesem, rovněž tak pojmy regulární a singulární matice. Tyto pojmy však nyní můžeme definovat obecněji i pro matice nad okruhem; obecnější definice hodnoty se nám bude hodit v paragrafu o polynomiálních maticích.

14.22. Definice. Nechť A je nenulová matice nad okruhem R . *Hodnotou $r(A)$ matice A budeme rozumět přirozené číslo k takové, že platí:*

- (i) *V matici A existuje nenulový subdeterminant řádu k .*
- (ii) *Všechny subdeterminanty matice A , které mají řád větší než k , jsou rovny nule.*

Hodnost nulové matice klademe rovnou nule.

Čtvercová matice nad okruhem R se nazývá *regulární*, je-li její hodnost rovna jejímu řádu; v opačném případě se nazývá *singulární*.

Z věty 14.21 vyplývá, že předchozí definice je rozšířením definice 12.1. Musíme si však uvědomit, že pro matice nad okruhem již není invertibilita ekvivalentní s regularitou (srovnej 12.5 pro matice nad tělesem a 14.18 a 14.22 pro matice nad okruhem); každá invertibilní matice je regulární, opak však neplatí.

14.23. Příklady. Reálná matice z příkladu 14.4(i) je regulární, neboť její determinant je nenulový. Matice A nad \mathbb{Z}_4 z příkladu 14.4(iii) má hodnost 3, protože je její determinant roven nule a subdeterminant

$$\begin{vmatrix} 2 & 1 & 3 \\ 1 & 3 & 1 \\ 3 & 1 & 0 \end{vmatrix} = 3 + 3 - 3 - 2 = 1$$

je nenulový. Matice A z příkladu 14.8 chápaná nad tělesem \mathbb{Z}_3 je singulární; má hodnost 3, neboť její subdeterminant

$$\begin{vmatrix} 2 & 1 & 1 \\ 2 & 2 & 0 \\ 1 & 1 & 1 \end{vmatrix} = 2$$

je nenulový. Tatáž matice A nad okruhem \mathbb{Z}_4 je regulární a dokonce invertibilní, neboť $\det A = 3$. Matice A nad okruhem \mathbb{Z}_8 z příkladu 14.10 je regulární, ale není invertibilní, neboť $\det A = 4$. Reálná matice z příkladu 14.12(ii) je regulární právě tehdy, když je $6a - 4c - 4d \neq 0$; v opačném případě má hodnost 3, neboť má nenulové subdeterminanty třetího řádu.

Matice

$$\begin{pmatrix} 2 & 4 \\ 3 & 6 \end{pmatrix}$$

nad okruhem celých čísel \mathbb{Z} je singulární. Přesto není žádný z řádků násobkem druhého (nad \mathbb{Z}).

14.24. Cramerovo pravidlo. *Nechť A je matice řádu n a $y = (y_1, \dots, y_n)$ n -tice prvků okruhu R . Pro každé $j = 1, \dots, n$ označme symbolem A_j matici, která vznikne z matice A nahrazením jejího j -tého sloupce n -ticí $y = (y_1, \dots, y_n)$, tj. sloupcem pravých stran. Potom platí:*

- (i) *Každé řešení soustavy lineárních rovnic $Ax = y$ je řešením následující soustavy se separovanými neznámými:*

$$\begin{aligned} \det A \cdot x_1 &= \det A_1, \\ \dots & \\ \det A \cdot x_n &= \det A_n. \end{aligned} \tag{1}$$

(ii) Jestliže má okruh R jednotkový prvek a $\det A$ je invertibilním prvkem okruhu R , potom má soustava lineárních rovnic $Ax = y$ jediné řešení:

$$x_1 = \det A_1 \cdot (\det A)^{-1}, \quad \dots, \quad x_n = \det A_n \cdot (\det A)^{-1}. \quad (2)$$

Důkaz. Předpokládejme, že n -tice $x = (x_1, \dots, x_n)$ je řešením soustavy $Ax = y$. Označíme-li $X_j, j = 1, \dots, n$, matici řádu n , která vznikne z jednotkové matice E nahrazením jejího j -tého sloupce n -ticí $x = (x_1, \dots, x_n)$, potom je pro každé $j = 1, \dots, n$

$$A \cdot X_j = A_j.$$

Podle věty o násobení determinantů je nyní pro každé $j = 1, \dots, n$

$$\det A \cdot \det X_j = \det A_j,$$

tj.

$$\det A \cdot x_1 = \det A_1, \quad \dots, \quad \det A \cdot x_n = \det A_n.$$

Jestliže má okruh R jednotkový prvek a jestliže je $\det A$ invertibilním prvkem okruhu R , potom je

$$x_1 = \det A_1 \cdot (\det A)^{-1}, \quad \dots, \quad x_n = \det A_n \cdot (\det A)^{-1}. \quad \square$$

Cramerovo pravidlo se často formuluje pro soustavu lineárních rovnic $Ax = y$, kde $A = (a_{ij})$ je regulární matice nad tělesem T . Z výsledků předchozího paragrafu vyplývá, že soustava $Ax = y$ má v tomto případě právě jediné řešení. Při důkazu Cramerova pravidla tedy stačí ověřit, že n -tice (x_1, \dots, x_n) popsaná rovnostmi (2) je řešením soustavy $Ax = y$. Přímým dosazením do i -té rovnice, užitím věty 14.11 o rozvoji determinantu (pro j -tý sloupec) a věty 14.13 dostaneme:

$$\begin{aligned} \sum_{j=1}^n a_{ij} x_j &= \sum_{j=1}^n a_{ij} \cdot \det A_j \cdot (\det A)^{-1} = \\ &= (\det A)^{-1} \sum_{j=1}^n a_{ij} \cdot \sum_{k=1}^n (-1)^{j+k} y_k \det A_{kj} = \\ &= (\det A)^{-1} \sum_{k=1}^n y_k \cdot \sum_{j=1}^n (-1)^{j+k} a_{ij} \det A_{kj} = \\ &= (\det A)^{-1} \sum_{k=1}^n y_k \cdot \delta_{ik} \det A = y_i \end{aligned}$$

Ověřili jsme tedy, že n -tice (x_1, \dots, x_n) popsaná vztahy (2) je řešením soustavy $Ax = y$.

Poznamenejme, že pro danou soustavu $Ax = y$ nad okruhem R nemusí být řešení soustavy (1) řešením soustavy $Ax = y$; tato situace nastane v případě, kdy prvek $\det A$ není v okruhu R invertibilní (viz příklad 14.25(iii)). V každém případě je však řešení soustavy $Ax = y$ možno hledat mezi řešeními soustavy (1); to je velmi jednoduché, neboť v každé rovnici soustavy (1) je jen jediná neznámá.

14.25. Příklady.

(i) Mějme soustavu lineárních rovnic nad tělesem \mathbb{Z}_5 :

$$\begin{aligned} 2x + y + 4z &= 1, \\ 3x + y + 4z &= 2, \\ 2x + 4y + 2z &= 3. \end{aligned}$$

Nejprve vypočteme determinant matice A uvažované soustavy:

$$\det A = \begin{vmatrix} 2 & 1 & 4 \\ 3 & 1 & 4 \\ 2 & 4 & 2 \end{vmatrix} = 4$$

Determinant je nenulový, matice dané soustavy rovnic je tedy regulární (invertibilní). Podle Cramerova pravidla je tedy

$$x = \det A_1 \cdot (\det A)^{-1}, \quad y = \det A_2 \cdot (\det A)^{-1}, \quad z = \det A_3 \cdot (\det A)^{-1},$$

kde

$$\det A_1 = \begin{vmatrix} 1 & 1 & 4 \\ 2 & 1 & 4 \\ 3 & 4 & 2 \end{vmatrix} = 4, \quad \det A_2 = \begin{vmatrix} 2 & 1 & 4 \\ 3 & 2 & 4 \\ 2 & 3 & 2 \end{vmatrix} = 1, \quad \det A_3 = \begin{vmatrix} 2 & 1 & 1 \\ 3 & 1 & 2 \\ 2 & 4 & 3 \end{vmatrix} = 0,$$

takže $x = 1$, $y = 4$, $z = 0$.

(ii) Mějme soustavu lineárních rovnic nad okruhem \mathbb{Z}_4 :

$$\begin{aligned} x + 3y &= 3, \\ x + y &= 2. \end{aligned}$$

Jestliže je dvojice (x, y) řešením této soustavy, je podle věty 14.24(i) tato dvojice též řešením soustavy

$$\begin{aligned} 2x &= 1, \\ 2y &= 3. \end{aligned}$$

Tato soustava nemá řešení a proto nemá řešení ani soustava výchozí.

(iii) Mějme soustavu lineárních rovnic nad okruhem \mathbb{Z}_4 :

$$\begin{aligned} x + 3y &= 1, \\ x + y &= 3. \end{aligned}$$

Jestliže je dvojice (x, y) řešením této soustavy, je též řešením soustavy

$$\begin{aligned} 2x &= 0, \\ 2y &= 2. \end{aligned}$$

Tato soustava má řešení $(0, 1)$, $(0, 3)$, $(2, 1)$, $(2, 3)$. Řešeními výchozí soustavy jsou však jen dvojice $(0, 3)$ a $(2, 1)$.

Při řešení konkrétních soustav rovnic nad tělesem užitíme zpravidla Gaussova algoritmu. Výpočet řešení soustavy n lineárních rovnic s n neznámými podle Cramerova pravidla totiž předpokládá početně náročnější výpočet $n + 1$ determinantů (viz příklad 14.26). Cramerovo pravidlo se však využívá při teoretických odvozováních, kdy je možno neznámé vyjádřit vzorcem.

14.26. Příklad. Mějme následující soustavu rovnic nad tělesem \mathbb{R} reálných čísel:

$$\begin{aligned} x + y + 2u + 3v &= 1, \\ 3x - y - u - 2v &= -4, \\ 2x + 3y - u - v &= -6, \\ x + 2y + 3u - v &= -4. \end{aligned}$$

Nejprve vypočteme determinant matice A uvedené soustavy lineárních rovnic: je $\det A = -153$. Determinant je nenulový, tj. matice uvažované soustavy rovnic je regulární. Můžeme tedy užít Cramerova pravidla. Vypočteme další čtyři determinanty, které vzniknou záměnou i -tého sloupce matice soustavy za sloupec pravých stran. Dostáváme:

$$\det A_1 = \begin{vmatrix} 1 & 1 & 2 & 3 \\ -4 & -1 & -1 & -2 \\ -6 & 3 & -1 & -1 \\ -4 & 2 & 3 & -1 \end{vmatrix} = 153, \quad \det A_2 = \begin{vmatrix} 1 & 1 & 2 & 3 \\ 3 & -4 & -1 & -2 \\ 2 & -6 & -1 & -1 \\ 1 & -4 & 3 & -1 \end{vmatrix} = 153,$$

$$\det A_3 = \begin{vmatrix} 1 & 1 & 1 & 3 \\ 3 & -1 & -4 & -2 \\ 2 & 3 & -6 & -1 \\ 1 & 2 & -4 & -1 \end{vmatrix} = 0, \quad \det A_4 = \begin{vmatrix} 1 & 1 & 2 & 1 \\ 3 & -1 & -1 & -4 \\ 2 & 3 & -1 & -6 \\ 1 & 2 & 3 & -4 \end{vmatrix} = -153.$$

Řešení uvedené soustavy je:

$$x = \frac{\det A_1}{\det A} = -1, \quad y = \frac{\det A_2}{\det A} = -1, \quad u = \frac{\det A_3}{\det A} = 0, \quad v = \frac{\det A_4}{\det A} = 1.$$

Porovnejte výše uvedené řešení s řešením podle Gaussova algoritmu.

15. METODY VÝPOČTU DETERMINANTŮ

V tomto paragrafu budeme na několika příkladech demonstrovat některé metody výpočtu determinantů. Determinanty jsou totiž jednou z mála partií lineární algebry, ve které při výpočtech nevystačíme s jedním nebo několika málo jednoduchými algoritmy. Výpočty determinantů vyžadují mnohdy zamyšlení, nápad a zkušenost. Budeme se zabývat i některými speciálními determinanty, se kterými se setkáváme zejména v analýze.¹

Příklady, které v dalším uvedeme, se budeme snažit počítat různými způsoby, abychom ukázali jednotlivé obraty a umožnili jejich srovnání.

Při výpočtech determinantů využíváme zejména základní vlastnosti zformulované v tvrzeních 14.7, dále lemma 14.6, větu 14.11 o rozvoji a větu 14.9 o determinantu horní (dolní) trojúhelníkové blokové matice.

15.1. Příklad. Vypočteme, pro která x je roven nule determinant

$$A(x) = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_1 & a_1 + a_2 - x & a_3 & \dots & a_n \\ a_1 & a_2 & a_2 + a_3 - x & \dots & a_n \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & a_{n-1} + a_n - x \end{vmatrix}$$

nad oborem integrality R .

Odečteme-li první řádek determinantu od ostatních řádků, dostaneme

$$A(x) = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ 0 & a_1 - x & 0 & \dots & 0 \\ 0 & 0 & a_2 - x & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{n-1} - x \end{vmatrix} = a_1 \cdot \prod_{i=1}^{n-1} (a_i - x).$$

Je-li $a_1 = 0$, je $A(x) = 0$ pro libovolné $x \in \mathbb{R}$. Je-li $a_1 \neq 0$, je $A(x) = 0$ pro $x = a_1, a_2, \dots, a_{n-1}$. Uvědomme si, že jsme využili předpokladu, že R je obor integrality.

15.2. Příklad. Vypočteme, pro která x je roven nule determinant

$$D(x) = \begin{vmatrix} x + a_1 & a_2 & \dots & a_n \\ a_1 & x + a_2 & \dots & a_n \\ \dots & \dots & \dots & \dots \\ a_1 & a_2 & \dots & x + a_n \end{vmatrix}$$

nad oborem integrality R .

¹ Viz např. Jarníkovy učebnice *Diferenciální počet II* a *Integrální počet II*.

K prvnímu sloupci přičteme všechny ostatní sloupce a vytkneme:

$$D(x) = \left(x + \sum_{i=1}^n a_i\right) \cdot \begin{vmatrix} 1 & a_2 & \dots & a_n \\ 1 & x + a_2 & \dots & a_n \\ \dots & \dots & \dots & \dots \\ 1 & a_2 & \dots & x + a_n \end{vmatrix}$$

Nyní od druhého, ..., n -tého sloupce odečteme po řadě a_2 -násobek, ..., a_n -násobek prvního sloupce.

$$D(x) = \left(x + \sum_{i=1}^n a_i\right) \cdot \begin{vmatrix} 1 & 0 & \dots & 0 \\ 1 & x & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 1 & 0 & \dots & x \end{vmatrix} = \left(x + \sum_{i=1}^n a_i\right) \cdot x^{n-1}$$

Je tedy $D(x) = 0$, právě když je $x = 0$ nebo $x = -\sum_{i=1}^n a_i$. Opět jsme využili toho, že R je obor integrity.

Uvedený příklad můžeme snadno vyřešit i jiným způsobem. Rozložíme determinant $D(x)$ na součet 2^n determinantů (podle lemmatu 14.6) tak, že každý sloupec uvažujeme jako součet dvou sloupců (v jednom budou samá a_i , ve druhém samé nuly a jedno x). Z těchto determinantů budou nenulové pouze ty, které mají nejvýše jeden sloupec se samými a_i ; tyto determinanty se snadno vypočítají. Tedy

$$D(x) = x^n + x^{n-1}(a_1 + \dots + a_n).$$

Poznamenejme, že není-li R oborem integrity, může být $D(x) = 0$ i v jiných případech. Pro $R = \mathbb{Z}_6$ je např. determinant

$$\begin{vmatrix} x+3 & 4 \\ 3 & x+4 \end{vmatrix} = (x+1) \cdot x$$

roven nule pro $x = 0, 2, 3, 5$.

15.3. Příklad. Bez přímého výpočtu dokážeme následující rovnost dvou determinantů nad tělesem \mathbb{R} reálných čísel.

$$\begin{vmatrix} 0 & x & y & z \\ x & 0 & z & y \\ y & z & 0 & x \\ z & y & x & 0 \end{vmatrix} = \begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & z^2 & y^2 \\ 1 & z^2 & 0 & x^2 \\ 1 & y^2 & x^2 & 0 \end{vmatrix}$$

Vynásobíme-li druhý, třetí a čtvrtý řádek determinantu vlevo po řadě yz , xz , xy , dostáváme:

$$\begin{vmatrix} 0 & x & y & z \\ x & 0 & z & y \\ y & z & 0 & x \\ z & y & x & 0 \end{vmatrix} = \frac{1}{x^2 y^2 z^2} \begin{vmatrix} 0 & x & y & z \\ xyz & 0 & yz^2 & zy^2 \\ xyz & xz^2 & 0 & zx^2 \\ xyz & xy^2 & yx^2 & 0 \end{vmatrix}$$

Nyní vytkneme ze sloupců determinantu vpravo po řadě xyz , x , y , z a dostáváme žádanou rovnost. Jelikož jsou oba determinanty spojité funkce proměnných x, y, z , platí uvedená rovnost i v případech $x = 0$, resp. $y = 0$, resp. $z = 0$.

15.4. Příklad. Vypočteme determinant

$$P(a_0, \dots, a_n) = \begin{vmatrix} x & -1 & 0 & \dots & 0 & 0 \\ 0 & x & -1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & x & -1 \\ a_0 & a_1 & a_2 & \dots & a_{n-1} & a_n \end{vmatrix}$$

řádu $n + 1$ nad okruhem R s jednotkovým prvkem. Uvedeme několik možností výpočtu tohoto determinantu.

a) Užijeme elementární úpravy: x -násobek posledního sloupce přičteme k předposlednímu, x -násobek předposledního sloupce (tj. n -tého) přičteme k $(n - 1)$ -nímu, ..., x -násobek druhého sloupce přičteme k prvnímu. Získaný determinant rozvedeme podle prvního sloupce:

$$\begin{aligned} P(a_0, \dots, a_n) &= \begin{vmatrix} 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 0 & -1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & -1 \\ \sum_{i=0}^n a_i x^i & \dots & \dots & \dots & a_{n-1} + a_n x & a_n \end{vmatrix} = \\ &= (-1)^{n+2} \cdot \sum_{i=0}^n a_i x^i \cdot (-1)^n = \sum_{i=0}^n a_i x^i . \end{aligned}$$

b) Rozvedeme determinant podle posledního sloupce a užijeme indukci:

$$\begin{aligned} P(a_0, \dots, a_n) &= (-1)^{2n+2} \cdot a_n \cdot x^n + (-1)^{2n+1} \cdot (-1) \cdot P(a_0, \dots, a_{n-1}) = \\ &= a_n x^n + P(a_0, \dots, a_{n-1}) = \sum_{i=0}^n a_i x^i . \end{aligned}$$

c) Rozvedeme determinant podle prvního sloupce a užijeme indukci:

$$\begin{aligned}
 P(a_0, \dots, a_n) &= (-1)^2 \cdot x \cdot P(a_1, \dots, a_n) + (-1)^{n+2} \cdot a_0 \cdot (-1)^n = \\
 &= a_0 + x \cdot P(a_1, \dots, a_n) = \sum_{i=0}^n a_i x^i .
 \end{aligned}$$

d) Rozvedeme-li determinant podle prvního řádku, dostaneme totéž jako v předchozím výpočtu:

$$\begin{aligned}
 P(a_0, \dots, a_n) &= (-1)^2 \cdot x \cdot P(a_1, \dots, a_n) + (-1)^3 \cdot (-1) \cdot (-1)^{n+1} \cdot a_0 \cdot (-1)^{n-1} = \\
 &= a_0 + x \cdot P(a_1, \dots, a_n) = \sum_{i=0}^n a_i x^i .
 \end{aligned}$$

e) Rozvedeme determinant podle posledního řádku:

$$\begin{aligned}
 P(a_0, \dots, a_n) &= (-1)^{n+2} \cdot a_0 \cdot (-1)^n + \dots + \\
 &+ (-1)^{n+1+i+1} \cdot a_i \cdot x^i \cdot (-1)^{n-i} + \dots + (-1)^{2n+2} \cdot a_n \cdot x^n = \sum_{i=0}^n a_i x^i .
 \end{aligned}$$

15.5. Příklad. Vypočteme determinant

$$D(a_1, \dots, a_n) = \begin{vmatrix} a_1 + x & x & \dots & x \\ x & a_2 + x & \dots & x \\ \dots & \dots & \dots & \dots \\ x & x & \dots & a_n + x \end{vmatrix}$$

řádu n nad okruhem R .

Uvedeme tři možnosti výpočtu tohoto determinantu:

a) Od prvního řádku odečteme druhý, od druhého třetí, ..., od předposledního odečteme poslední. Vzniklý determinant rozvedeme podle prvního sloupce. Dostá-

váme:

$$\begin{aligned}
 D(a_1, \dots, a_n) &= \begin{vmatrix} a_1 & -a_2 & 0 & \dots & 0 \\ 0 & a_2 & -a_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -a_n \\ x & x & x & \dots & a_n + x \end{vmatrix} = \\
 &= a_1 \cdot D(a_2, \dots, a_n) + (-1)^{n+1} \cdot x \cdot (-a_2) \dots (-a_n) = \\
 &= x \cdot a_2 \dots a_n + a_1 \cdot (a_2 \cdot D(a_3, \dots, a_n) + x \cdot a_3 \dots a_n) = \\
 &= \prod_{i=1}^n a_i + x \cdot \sum_{j=1}^n \prod_{\substack{i=1 \\ i \neq j}}^n a_i .
 \end{aligned}$$

b) K determinantu $D(a_1, \dots, a_n)$ přidáme vhodný řádek a sloupec tak, aby se hodnota determinantu nezměnila. Potom odečteme první sloupec od ostatních sloupců a determinant rozvedeme podle posledního sloupce:

$$\begin{aligned}
 D(a_1, \dots, a_n) &= \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ x & a_1 + x & x & \dots & x \\ x & x & a_2 + x & \dots & x \\ \dots & \dots & \dots & \dots & \dots \\ x & x & x & \dots & a_n + x \end{vmatrix} = \\
 &= \begin{vmatrix} 1 & -1 & -1 & \dots & -1 \\ x & a_1 & 0 & \dots & 0 \\ x & 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ x & 0 & 0 & \dots & a_n \end{vmatrix} = \\
 &= a_n \cdot D(a_1, \dots, a_{n-1}) + (-1)^{n+2} \cdot (-1) \cdot (-1)^{n+1} \cdot x \cdot a_1 \dots a_{n-1} = \\
 &= x \cdot a_1 \dots a_{n-1} + a_n \cdot (a_{n-1} \cdot D(a_1, \dots, a_{n-2}) + x \cdot a_1 \dots a_{n-2}) = \\
 &= \prod_{i=1}^n a_i + x \cdot \sum_{j=1}^n \prod_{\substack{i=1 \\ i \neq j}}^n a_i .
 \end{aligned}$$

Poslední determinant bylo vhodnější rozložit podle prvního řádku. Dostali bychom:

$$\begin{aligned} D(a_1, \dots, a_n) &= (-1)^2 \cdot 1 \cdot a_1 \dots a_n + \dots + \\ &+ (-1)^{i+1+1} \cdot (-1) \cdot (-1)^{i+1} \cdot x \cdot a_1 \dots a_{i-1} a_{i+1} \dots a_n + \dots + \\ &+ (-1)^{n+2} \cdot (-1) \cdot (-1)^{n+1} \cdot x \cdot a_1 \dots a_{n-1} = \\ &= \prod_{i=1}^n a_i + x \cdot \sum_{j=1}^n \prod_{\substack{i=1 \\ i \neq j}}^n a_i . \end{aligned}$$

Stejně vhodné bylo provést rozvoj podle prvního sloupce.

c) Rozložíme determinant $D(a_1, \dots, a_n)$ na součet 2^n determinantů tím, že každý sloupec uvažujeme jako součet dvou sloupců: v prvním budou samá x , v druhém kromě nul ještě prvek a_i — viz věta 14.6. Z těchto determinantů budou nenulové pouze ty, které mají nejvýše jediný sloupec s x . Odtud vyplývá výsledek.

15.6. Příklad. Vypočteme determinant

$$D_n = \begin{vmatrix} a+1 & a & 0 & \dots & 0 & 0 \\ 1 & a+1 & a & \dots & 0 & 0 \\ 0 & 1 & a+1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a+1 & a \\ 0 & 0 & 0 & \dots & 1 & a+1 \end{vmatrix}$$

n -tého řádu nad okruhem R s jednotkovým prvkem.

Uvedeme dvě možnosti výpočtu.

a) Rozvojem podle prvního řádku (resp. prvního sloupce, posledního řádku, posledního sloupce) dostaneme rovnost

$$D_n = (a+1) \cdot D_{n-1} - a \cdot D_{n-2} .$$

Zřejmě je

$$D_1 = a+1 , \quad D_2 = a^2 + a+1 .$$

Matematickou indukcí nyní snadno dokážeme, že

$$D_n = a^n + a^{n-1} + \dots + a+1 .$$

b) Rozdělíme determinant D_n na součet 2^n determinantů (podle lematu 14.6), každý sloupec budeme uvažovat jako součet dvou sloupců: v jednom budou kromě nul dva prvky a , ve druhém budou kromě nul ještě dvě jedničky (při rozkladu prvního sloupce však bude prvek a jen jeden, při rozkladu posledního sloupce bude jen jedna jednička). Z těchto determinantů budou nenulové pouze ty, které mají nejprve sloupce obsahující prvky a a potom sloupce s jedničkami (stojí-li za sloupcem s jedničkami sloupec s a , je determinant roven nule). Těchto determinantů je $n+1$ a jsou po řadě rovny $a^n, a^{n-1}, \dots, a^2, a, 1$. Odtud plyne výsledek.

15.7. Vandermondův determinant. *Vandermondovým determinantem* prvků a_1, \dots, a_n nad okruhem R s jednotkovým prvkem rozumíme determinant

$$V(a_1, \dots, a_n) = \begin{vmatrix} 1 & 1 & \dots & 1 & 1 \\ a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_1^2 & a_2^2 & \dots & a_{n-1}^2 & a_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_{n-1}^{n-1} & a_n^{n-1} \end{vmatrix}.$$

Při jeho výpočtu nejprve odečteme poslední sloupec od všech ostatních a pak rozvojem podle prvního řádku snížíme řád determinantu:

$$\begin{aligned} V(a_1, \dots, a_n) &= \begin{vmatrix} 0 & \dots & 0 & 1 \\ a_1 - a_n & \dots & a_{n-1} - a_n & a_n \\ a_1^2 - a_n^2 & \dots & a_{n-1}^2 - a_n^2 & a_n^2 \\ \dots & \dots & \dots & \dots \\ a_1^{n-1} - a_n^{n-1} & \dots & a_{n-1}^{n-1} - a_n^{n-1} & a_n^{n-1} \end{vmatrix} = \\ &= (-1)^{n+1} \cdot \begin{vmatrix} a_1 - a_n & \dots & a_{n-1} - a_n \\ a_1^2 - a_n^2 & \dots & a_{n-1}^2 - a_n^2 \\ \dots & \dots & \dots \\ a_1^{n-1} - a_n^{n-1} & \dots & a_{n-1}^{n-1} - a_n^{n-1} \end{vmatrix} \end{aligned}$$

Ze sloupců vytkneme prvky $a_1 - a_n, \dots, a_{n-1} - a_n$.

$$V(a_1, \dots, a_n) = \prod_{i=1}^{n-1} (a_n - a_i) \cdot \begin{vmatrix} 1 & \dots & 1 \\ a_1 + a_n & \dots & a_{n-1} + a_n \\ a_1^2 + a_1 a_n + a_n^2 & \dots & a_{n-1}^2 + a_{n-1} a_n + a_n^2 \\ \dots & \dots & \dots \\ a_1^{n-2} + \dots + a_n^{n-2} & \dots & a_{n-1}^{n-2} + \dots + a_n^{n-2} \end{vmatrix}$$

Nyní odečteme a_n -násobek prvního řádku od druhého řádku, a_n^2 -násobek prvního řádku od třetího řádku, \dots , a_n^{n-2} -násobek prvního řádku od posledního řádku. Potom odečteme a_n -násobek druhého řádku od třetího řádku, \dots , nakonec odečteme a_n -násobek předposledního řádku od posledního řádku; dostaneme Vandermondův determinant $V(a_1, \dots, a_{n-1})$. Pomocí matematické indukce dostáváme

$$\begin{aligned} V(a_1, \dots, a_n) &= \prod_{i=1}^{n-1} (a_n - a_i) \cdot V(a_1, \dots, a_{n-1}) = \\ &= \prod_{i=1}^{n-1} (a_n - a_i) \cdot \prod_{i=1}^{n-2} (a_{n-1} - a_i) \cdot \dots \cdot (a_2 - a_1) = \prod_{\substack{i,j=1 \\ j>i}}^n (a_j - a_i). \end{aligned}$$

V následujících odstavcích se budeme zabývat determinanty, jejichž prvky jsou funkce.

15.8. Věta. Necht f_{ij} , $i, j = 1, \dots, n$, jsou reálné funkce, které mají v intervalu (a, b) vlastní derivace f'_{ij} . Potom funkce F , která je na intervalu (a, b) definována vztahem

$$F(x) = \det (f_{ij}(x)) = \begin{vmatrix} f_{11}(x) & f_{12}(x) & \dots & f_{1n}(x) \\ f_{21}(x) & f_{22}(x) & \dots & f_{2n}(x) \\ \dots & \dots & \dots & \dots \\ f_{n1}(x) & f_{n2}(x) & \dots & f_{nn}(x) \end{vmatrix},$$

má na intervalu (a, b) vlastní derivaci

$$F'(x) = \sum_{i=1}^n \begin{vmatrix} f_{11}(x) & \dots & f'_{1i}(x) & \dots & f_{1n}(x) \\ f_{21}(x) & \dots & f'_{2i}(x) & \dots & f_{2n}(x) \\ \dots & \dots & \dots & \dots & \dots \\ f_{n1}(x) & \dots & f'_{ni}(x) & \dots & f_{nn}(x) \end{vmatrix},$$

resp.

$$F'(x) = \sum_{i=1}^n \begin{vmatrix} f_{11}(x) & f_{12}(x) & \dots & f_{1n}(x) \\ \dots & \dots & \dots & \dots \\ f'_{i1}(x) & f'_{i2}(x) & \dots & f'_{in}(x) \\ \dots & \dots & \dots & \dots \\ f_{n1}(x) & f_{n2}(x) & \dots & f_{nn}(x) \end{vmatrix}.$$

Důkaz. Podle definice determinantu je

$$F(x) = \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot f_{P(1)1}(x) \dots f_{P(n)n}(x)$$

a tedy

$$\begin{aligned} F'(x) &= \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot \sum_{i=1}^n f_{P(1)1}(x) \dots f'_{P(i)i}(x) \dots f_{P(n)n}(x) = \\ &= \sum_{i=1}^n \sum_{P \in \mathbb{S}_n} \operatorname{sgn} P \cdot f_{P(1)1}(x) \dots f'_{P(i)i}(x) \dots f_{P(n)n}(x) = \\ &= \sum_{i=1}^n \begin{vmatrix} f_{11}(x) & \dots & f'_{1i}(x) & \dots & f_{1n}(x) \\ f_{21}(x) & \dots & f'_{2i}(x) & \dots & f_{2n}(x) \\ \dots & \dots & \dots & \dots & \dots \\ f_{n1}(x) & \dots & f'_{ni}(x) & \dots & f_{nn}(x) \end{vmatrix}. \end{aligned}$$

S přihlédnutím k 14.7(iii) je též

$$F'(x) = \sum_{i=1}^n \begin{vmatrix} f_{11}(x) & f_{12}(x) & \dots & f_{1n}(x) \\ \dots & \dots & \dots & \dots \\ f'_{i1}(x) & f'_{i2}(x) & \dots & f'_{in}(x) \\ \dots & \dots & \dots & \dots \\ f_{n1}(x) & f_{n2}(x) & \dots & f_{nn}(x) \end{vmatrix} \cdot \square$$

15.9. Wronského determinant. Necht f_1, \dots, f_n jsou reálné funkce, které mají na intervalu (a, b) vlastní derivace až do řádu $n - 1$. Označme $f_i^{(j)}$ j -tou derivací funkce f_i na intervalu (a, b) . Wronského determinantem funkcí f_1, \dots, f_n budeme rozumět determinant

$$W(f_1, \dots, f_n)(x) = \begin{vmatrix} f_1(x) & f_2(x) & \dots & f_n(x) \\ f_1^{(1)}(x) & f_2^{(1)}(x) & \dots & f_n^{(1)}(x) \\ \dots & \dots & \dots & \dots \\ f_1^{(n-1)}(x) & f_2^{(n-1)}(x) & \dots & f_n^{(n-1)}(x) \end{vmatrix}.$$

15.10. Věta. Necht f_1, \dots, f_n jsou reálné funkce, které mají na intervalu (a, b) vlastní derivace až do řádu $n - 1$. Potom platí:

- (i) Jsou-li funkce f_1, \dots, f_n lineárně závislé jako vektory prostoru všech funkcí na intervalu (a, b) , potom pro každé $x \in (a, b)$ je $W(f_1, \dots, f_n)(x) = 0$.
- (ii) Jestliže funkce f_1, \dots, f_n mají na intervalu (a, b) vlastní derivace až do řádu n , potom

$$W'(f_1, \dots, f_n)(x) = \begin{vmatrix} f_1(x) & f_2(x) & \dots & f_n(x) \\ f_1^{(1)}(x) & f_2^{(1)}(x) & \dots & f_n^{(1)}(x) \\ \dots & \dots & \dots & \dots \\ f_1^{(n-2)}(x) & f_2^{(n-2)}(x) & \dots & f_n^{(n-2)}(x) \\ f_1^{(n)}(x) & f_2^{(n)}(x) & \dots & f_n^{(n)}(x) \end{vmatrix}.$$

Důkaz. Jestliže jsou funkce f_1, \dots, f_n lineárně závislé, potom je jedna z nich — např. f_1 — lineární kombinací ostatních, tedy

$$f_1 = a_2 f_2 + \dots + a_n f_n.$$

Pro každé $j = 1, \dots, n - 1$ je tedy

$$f_1^{(j)} = a_2 f_2^{(j)} + \dots + a_n f_n^{(j)}.$$

První sloupec determinantu $W(f_1, \dots, f_n)(x)$ je tedy lineární kombinací ostatních sloupců, tj. $W(f_1, \dots, f_n)(x) = 0$.

Tvrzení (ii) ihned vyplývá z příkladu 15.8. \square

15.11. Jacobiho determinant. Necht' f_1, \dots, f_n jsou reálné funkce n reálných proměnných x_1, \dots, x_n , které mají parciální derivace na intervalu I . *Jacobiho determinantem (jacobianem)* těchto funkcí budeme rozumět determinant

$$\frac{D(f_1, \dots, f_n)}{D(x_1, \dots, x_n)} = \begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_n} \\ \dots & \dots & \dots & \dots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_n} \end{vmatrix}.$$

15.12. Věta. Necht' f_1, f_2, \dots, f_n jsou reálné funkce n reálných proměnných x_1, x_2, \dots, x_n , které mají parciální derivace na intervalu $I = I_1 \times I_2 \times \dots \times I_n \subseteq \mathbb{R}^n$, a necht' $\varphi_1, \varphi_2, \dots, \varphi_n$ jsou reálné funkce n reálných proměnných t_1, t_2, \dots, t_n , které mají parciální derivace na intervalu $J \subseteq \mathbb{R}^n$, a každá funkce φ_i zobrazuje interval J do intervalu I_i . Definujme pro každé $i = 1, \dots, n$ funkci F_i vztahem

$$F_i(t_1, t_2, \dots, t_n) = f_i(\varphi_1(t_1, \dots, t_n), \varphi_2(t_1, \dots, t_n), \dots, \varphi_n(t_1, \dots, t_n)).$$

Mají-li funkce $\varphi_1, \varphi_2, \dots, \varphi_n$ totální diferenciály v bodě $a \in J$ a mají-li funkce f_1, f_2, \dots, f_n totální diferenciály v bodě $b = (\varphi_1(a), \varphi_2(a), \dots, \varphi_n(a))$, potom je

$$\left[\frac{D(F_1, \dots, F_n)}{D(t_1, \dots, t_n)} \right]_{t=a} = \left[\frac{D(f_1, \dots, f_n)}{D(x_1, \dots, x_n)} \right]_{x=b} \cdot \left[\frac{D(\varphi_1, \dots, \varphi_n)}{D(t_1, \dots, t_n)} \right]_{t=a}.$$

Důkaz. Vyjádříme-li prvky determinantu na levé straně rovnosti známým způsobem, tj.

$$\frac{\partial F_i(a)}{\partial t_j} = \sum_{k=1}^n \frac{\partial f_i(b)}{\partial x_k} \cdot \frac{\partial \varphi_k(a)}{\partial t_j},$$

dostáváme výše uvedený výsledek z věty o násobení determinantů. \square

Z předchozí věty jednoduše vyplývá následující tvrzení.

15.13. Důsledek. Necht' f_1, f_2, \dots, f_n jsou reálné funkce n reálných proměnných x_1, x_2, \dots, x_n , které mají parciální derivace v \mathbb{R}^n . Definujme pro každé $i = 1, \dots, n$ funkci F_i vztahem

$$F_i(t_1, \dots, t_n) = f_i(x_1, \dots, x_n),$$

kde

$$x_1 = \sum_{j=1}^n b_{1j}t_j, \quad \dots, \quad x_n = \sum_{j=1}^n b_{nj}t_j$$

a $\det(b_{ij}) \neq 0$. Potom

$$\frac{D(F_1, \dots, F_n)}{D(t_1, \dots, t_n)} = \det(b_{ij}) \cdot \frac{D(f_1, \dots, f_n)}{D(x_1, \dots, x_n)}. \quad \square$$

15.14. Hessův determinant. Nechť f je reálná funkce n reálných proměnných x_1, \dots, x_n , která má na intervalu $I \subseteq \mathbb{R}^n$ parciální derivace druhého řádu. *Hessovým determinantem (hessiánem)* funkce f budeme rozumět determinant

$$H(f) = \begin{vmatrix} \frac{\partial^2 f}{\partial x_1 \partial x_1} & \frac{\partial^2 f}{\partial x_1 \partial x_2} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \frac{\partial^2 f}{\partial x_2 \partial x_1} & \frac{\partial^2 f}{\partial x_2 \partial x_2} & \cdots & \frac{\partial^2 f}{\partial x_2 \partial x_n} \\ \dots & \dots & \dots & \dots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \frac{\partial^2 f}{\partial x_n \partial x_2} & \cdots & \frac{\partial^2 f}{\partial x_n \partial x_n} \end{vmatrix}.$$

15.15. Věta. Nechť f je reálná funkce n reálných proměnných x_1, \dots, x_n , která má v \mathbb{R}^n parciální derivace druhého řádu. Nechť F je reálná funkce n reálných proměnných t_1, \dots, t_n , která je definována vztahem

$$F(t_1, \dots, t_n) = f(x_1, \dots, x_n),$$

kde

$$x_1 = \sum_{j=1}^n b_{1j}t_j, \quad \dots, \quad x_n = \sum_{j=1}^n b_{nj}t_j,$$

a $\det(b_{ij}) \neq 0$. Potom je

$$H(F) = [\det(b_{ij})]^2 \cdot H(f).$$

Důkaz. Důkaz tohoto tvrzení se provede podobně jako důkaz věty 15.12. \square

15.16. Příklad. Následující determinant patří mezi tzv. *cirkulanty*.

$$C = \begin{vmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \\ 3 & 4 & 5 & \dots & 1 & 2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n & 1 & 2 & \dots & n-2 & n-1 \end{vmatrix}.$$

Přičteme-li všechny řádky k prvnímu a vytkneme-li, dostaneme

$$C = \frac{n(n+1)}{2} \cdot \begin{vmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 2 & 3 & 4 & \dots & n & 1 \\ 3 & 4 & 5 & \dots & 1 & 2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ n-1 & n & 1 & \dots & n-3 & n-2 \\ n & 1 & 2 & \dots & n-2 & n-1 \end{vmatrix}.$$

Odečteme-li vhodné násobky prvního řádku od ostatních řádků, dostaneme

$$C = \frac{n(n+1)}{2} \cdot \begin{vmatrix} 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 0 & 1 & 2 & \dots & n-3 & n-2 & -1 \\ 0 & 1 & 2 & \dots & n-3 & -2 & -1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & 2-n & \dots & -3 & -2 & -1 \\ 0 & 1-n & 2-n & \dots & -3 & -2 & -1 \end{vmatrix}.$$

Nyní rozvedeme determinant podle prvního sloupce a pak přičteme vhodné násobky posledního sloupce k ostatním sloupcům:

$$C = \frac{n(n+1)}{2} \cdot \begin{vmatrix} 0 & 0 & \dots & 0 & 0 & -1 \\ 0 & 0 & \dots & 0 & -n & -1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & -n & \dots & -n & -n & -1 \\ -n & -n & \dots & -n & -n & -1 \end{vmatrix} =$$

$$= \frac{n(n+1)}{2} \cdot n^{n-2} \cdot (-1)^{n-1} \cdot (-1)^{\frac{(n-2)(n-1)}{2}} = (-1)^{\frac{n(n-1)}{2}} \cdot \frac{(n+1)}{2} \cdot n^{n-1}.$$

IV. PODOBNOST

16. POLYNOMIÁLNÍ MATICE

V úvodu této kapitoly připomeneme několik pojmů z algebry; budou se nám hodit v tomto paragrafu i v paragrafech následujících.

Jestliže T je těleso, potom symbolem $T[\lambda]$ značíme *obor integrity všech polynomů neurčité λ nad tělesem T* . Polynomy z $T[\lambda]$ píšeme v tvaru

$$f(\lambda) = a_0\lambda^n + a_1\lambda^{n-1} + \dots + a_n .$$

Je-li $a_0 \neq 0$, je a_0 tzv. *vedoucí koeficient* polynomu $f(\lambda)$ a číslo n je tzv. *stupeň polynomu $f(\lambda)$* ; píšeme $n = \deg f(\lambda)$. Polynom $f(\lambda)$ se nazývá *normovaný*, je-li $a_0 = 1$. Polynomy nultého stupně jsou právě všechny nenulové prvky tělesa T , nulový prvek tělesa T je tzv. *nulový polynom*, kterému se obvykle stupeň nepřipisuje; je tedy $T \subset T[\lambda]$. Invertibilními prvky oboru integrity $T[\lambda]$ jsou právě všechny nenulové prvky tělesa T .

Připomeňme, že v oboru integrity $T[\lambda]$ je možno dělit se zbytkem; jsou-li $f(\lambda)$ a $g(\lambda) \neq 0$ polynomy z $T[\lambda]$, potom existují takové polynomy $q(\lambda)$, $r(\lambda) \in T[\lambda]$, že

$$f(\lambda) = g(\lambda) \cdot q(\lambda) + r(\lambda) , \quad \text{kde buď } r(\lambda) = 0 \quad \text{nebo} \quad \deg r(\lambda) < \deg g(\lambda) .$$

Připomeňme rovněž, že každá konečná množina prvků z $T[\lambda]$ má největšího společného dělitele a že polynomy $f(\lambda)$, $g(\lambda)$ jsou nesoudělné právě tehdy, když existují polynomy $u(\lambda) \in T[\lambda]$ a $v(\lambda) \in T[\lambda]$, pro které

$$f(\lambda) \cdot u(\lambda) + g(\lambda) \cdot v(\lambda) = 1 .$$

Každý normovaný polynom je možno rozložit v součin normovaných *ireducibilních*, tj. již dále nerozložitelných polynomů; takovýto rozklad je jednoznačný až na pořadí užitých ireducibilních polynomů.

Těleso T se nazývá *algebraicky uzavřené*, jestliže každý ireducibilní polynom z $T[\lambda]$ je prvního stupně; každý polynom z $T[\lambda]$ stupně alespoň jedna se pak rozkládá v součin polynomů prvního stupně (často se hovoří o *lineárních faktorech*). Připomeňme, že ke každému tělesu existuje algebraicky uzavřené nadtěleso. Těleso komplexních čísel je algebraicky uzavřené, tělesa racionálních čísel, reálných čísel a tělesa \mathbb{Z}_p algebraicky uzavřená nejsou.

16.1. Definice. Necht T je těleso. λ -maticí nad tělesem T budeme rozumět každou matici nad oborem integrity $T[\lambda]$. Množinu všech čtvercových λ -matic řádu n nad tělesem T budeme značit $T[\lambda]^{n \times n}$.

Každá λ -matice nad tělesem T je sestavena z polynomů neurčité λ nad tělesem T ; proto se místo λ -matice říká též *polynomiální matice*. Každou „obyčejnou“ matici nad tělesem T můžeme chápat i jako λ -matici, proto je $T^{n \times n} \subset T[\lambda]^{n \times n}$. Ve smyslu definice 14.22 můžeme hovořit o hodnotě polynomiální matice.

Polynomiální matice neboli λ -matice budeme značit

$$A(\lambda) = (a_{ij}(\lambda)), \quad B(\lambda) = (b_{ij}(\lambda))$$

atd.; často budeme mluvit stručněji o maticích $A(\lambda)$, $B(\lambda)$ apod.

Každou λ -matici nad tělesem T můžeme chápat jako tzv. *maticový polynom*, tj. polynom neurčité λ , jehož koeficienty jsou „obyčejné“ matice, tj. matice nad tělesem T . Uvažujme λ -matici $A(\lambda) = (a_{ij}(\lambda))$; symbolem h označme maximum stupňů všech polynomů $a_{ij}(\lambda)$. Pak můžeme psát

$$A(\lambda) = A_0 \lambda^h + A_1 \lambda^{h-1} + \dots + A_{h-1} \lambda + A_h,$$

kde v matici A_h stojí na místě ij absolutní člen polynomu $a_{ij}(\lambda)$, v matici A_{h-1} stojí na místě ij koeficient u první mocniny neurčité λ v polynomu $a_{ij}(\lambda)$ atd. Číslo h se nazývá *stupeň maticového polynomu* $A(\lambda)$; píšeme $h = \deg A(\lambda)$. Nenulová matice A_0 se nazývá *vedoucí koeficient* maticového polynomu $A(\lambda)$. „Obyčejné“ nenulové matice nad tělesem T mají jako maticové polynomy stupeň nula, nulové matice stupeň nepřipisujeme.

V této kapitole se budeme zabývat výhradně čtvercovými λ -maticemi; některé výsledky by však bylo možno dokázat i pro λ -matice obdélníkové.

16.2. Příklad. Reálné λ -matice

$$A(\lambda) = \begin{pmatrix} \lambda^2 + \lambda - 1 & \lambda + 1 \\ \lambda^2 - 1 & \lambda^2 + 2\lambda - 1 \end{pmatrix}, \quad B(\lambda) = \begin{pmatrix} \lambda^3 + \lambda^2 + \lambda + 1 & \lambda^3 \\ \lambda^2 + 2\lambda & \lambda^3 + \lambda + 1 \end{pmatrix}$$

druhého řádu se zapíše jako maticové polynomy takto:

$$A(\lambda) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \lambda^2 + \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \lambda + \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix},$$

$$B(\lambda) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \lambda^3 + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \lambda^2 + \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \lambda + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Maticový polynom $A(\lambda)$, resp. $B(\lambda)$ má stupeň 2, resp. 3, tj. $\deg A(\lambda) = 2$, resp. $\deg B(\lambda) = 3$. Snadno se ověří, že matice $A(\lambda)$ i $B(\lambda)$ jsou regulární (viz 14.22).

Pro polynomiální matice mají velký význam elementární úpravy a elementární transformační λ -matice; následující pasáž srovnáme s 12.9 – 12.11.

16.3. Definice. *Elementární transformační λ -maticí* budeme rozumět každou invertibilní λ -matici, která se nejméně na jednom místě liší od jednotkové matice.

Rozeznáváme dva typy elementárních transformačních λ -matic:

(i) V λ -matici jsou mimo hlavní diagonálu samé nuly. Na hlavní diagonále jsou jedničky s výjimkou místa ii , kde stojí nenulový prvek $b \in T$ (prvek b musí být nenulový, neboť jinak by uvažovaná λ -matice nebyla invertibilní; ze stejných důvodů nesmí být na místě ii polynom stupně alespoň 1). Inverzní λ -maticí k této elementární transformační λ -matici je elementární transformační λ -matice prvního typu, která má na místě ii prvek b^{-1} .

(ii) V λ -matici jsou na hlavní diagonále samé jedničky. Mimo hlavní diagonálu jsou nuly s výjimkou místa ij , kde stojí polynom $b(\lambda) \in T[\lambda]$. Inverzní λ -maticí k této λ -matici je elementární transformační λ -matice druhého typu, která má na místě ij polynom $-b(\lambda)$.

Vynásobíme-li nějakou λ -matici $A(\lambda)$ výše uvažovanou elementární transformační λ -maticí prvního typu zprava (zleva), je výsledkem λ -matice, která se od λ -matice $A(\lambda)$ liší pouze tím, že její i -tý sloupec (řádek) je b -násobkem i -tého sloupce (řádku) λ -matice $A(\lambda)$.

Vynásobíme-li nějakou λ -matici $A(\lambda)$ výše uvažovanou elementární transformační λ -maticí druhého typu zprava (zleva), je výsledkem λ -matice, která se od λ -matice $A(\lambda)$ liší pouze tím, že její j -tý sloupec je součtem j -tého sloupce a $b(\lambda)$ -násobku i -tého sloupce (i -tý řádek je součtem i -tého řádku a $b(\lambda)$ -násobku j -tého řádku) λ -matice $A(\lambda)$.

Elementární transformační matice definované v 12.9 jsou speciálním případem elementárních transformačních λ -matic.

16.4. Definice. Při počítání s λ -maticemi budeme *sloupcovými elementárními úpravami* rozumět:

- (i) vynásobení nějakého sloupce nenulovým prvkem $b \in T$,
- (ii) přičtení $b(\lambda)$ -násobku nějakého sloupce k jinému sloupci (kde $b(\lambda) \in T[\lambda]$).

Podobně budeme *řádkovými elementárními úpravami* rozumět:

- (i) vynásobení nějakého řádku nenulovým prvkem $b \in T$,
- (ii) přičtení $b(\lambda)$ -násobku nějakého řádku k jinému řádku (kde $b(\lambda) \in T[\lambda]$).

Sloupcové (resp. řádkové) elementární úpravy odpovídají vynásobení příslušné λ -matice elementární transformační λ -maticí prvního a druhého typu zprava (resp. zleva). Složením čtyř vhodných sloupcových (řádkových) elementárních úprav dosáhneme prohození dvou sloupců (řádků) stejně jako ve 12. paragrafu.

Nyní přejdeme k základnímu pojmu této kapitoly, k ekvivalenci polynomiálních matic.

16.5. Definice. Nechť $A(\lambda)$ a $B(\lambda)$ jsou λ -matice téhož řádu nad tělesem T . Řekneme, že λ -matice $A(\lambda)$ a $B(\lambda)$ jsou *ekvivalentní*, jestliže je

$$B(\lambda) = X(\lambda) \cdot A(\lambda) \cdot Y(\lambda) ,$$

kde $X(\lambda)$ a $Y(\lambda)$ jsou součiny elementárních transformačních λ -matic.

Postupné násobení λ -matice $A(\lambda)$ zprava i zleva elementárními transformačními λ -maticemi odpovídá provádění sloupcových a řádkových elementárních úprav. Matice $A(\lambda)$ a $B(\lambda)$ jsou tedy ekvivalentní právě tehdy, když je možno od λ -matice $A(\lambda)$ dojít k λ -matici $B(\lambda)$ provedením konečně mnoha sloupcových a řádkových elementárních úprav.

Ekvivalence polynomiálních matic zavedená v předchozí definici je relací na množině $T[\lambda]^{n \times n}$ všech λ -matic řádu n nad tělesem T . Tato relace je opravdu *ekvivalence*. Je zřejmě *reflexivní* a *tranzitivní*; *symetrie* vyplývá z toho, že inverzní λ -matice k elementárním transformačním λ -maticím jsou opět elementární transformační λ -matice. Množina $T[\lambda]^{n \times n}$ všech λ -matic řádu n nad tělesem T se tedy rozpadne na třídy navzájem ekvivalentních λ -matic. V dalším textu ukážeme, a to je hlavním cílem celého tohoto paragrafu, že v každé takovéto třídě existuje *právě jediná* λ -matice velmi jednoduchého tvaru, tzv. *kanonická* λ -matice.

16.6. Definice. *Kanonickou* λ -maticí řádu n nad tělesem T budeme rozumět každou diagonální matici

$$\begin{pmatrix} e_1(\lambda) & 0 & \dots & 0 \\ 0 & e_2(\lambda) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e_n(\lambda) \end{pmatrix},$$

kde

- (i) pro každé $i = 1, \dots, n-1$ je polynom $e_{i+1}(\lambda)$ násobkem polynomu $e_i(\lambda)$;
- (ii) polynomy $e_1(\lambda), \dots, e_n(\lambda)$ jsou normované.

Povšimněme si, že pro kanonickou λ -matici z předchozí definice platí tato tvrzení:

- (a) Jestliže pro nějaký index i je $e_i(\lambda) = 0$, potom je $e_i(\lambda) = \dots = e_n(\lambda) = 0$.
- (b) Jestliže pro nějaký index i je $e_i(\lambda) = 1$, potom je $e_1(\lambda) = \dots = e_i(\lambda) = 1$.

Jednotková i nulová matice jsou zřejmě kanonickými λ -maticemi.

16.7. Věta. *Každá čtvercová λ -matice je ekvivalentní s nějakou kanonickou λ -maticí.*

Důkaz. Tvrzení věty dokážeme matematickou indukcí podle řádu vyšetřovaných λ -matic.

Nechť $A(\lambda) = (f(\lambda))$ je nenulová λ -matice prvního řádu. Jestliže je b vedoucí koeficient polynomu $f(\lambda)$, potom $B(\lambda) = (b^{-1}f(\lambda))$ je kanonická λ -matice ekvivalentní s λ -maticí $A(\lambda)$.

Předpokládejme, že tvrzení platí pro všechny λ -matice řádu $n-1$. Nechť $A(\lambda)$ je nenulová λ -matice řádu n . Označme \mathfrak{A} množinu všech λ -matic, které jsou ekvivalentní s λ -maticí $A(\lambda)$ a mají v levém horním rohu nenulový normovaný polynom.

Protože je $A(\lambda)$ nenulová, je množina \mathfrak{A} neprázdná. Polynomy stojící v levém horním rohu λ -matic z množiny \mathfrak{A} mohou mít různý stupeň; označme k nejmenší ze všech těchto stupňů. Nechť $B(\lambda) \in \mathfrak{A}$ je nějaká λ -matice, jejíž polynom $e_1(\lambda)$ v levém horním rohu má právě stupeň k . Pišme

$$B(\lambda) = \begin{pmatrix} e_1(\lambda) & b_{12}(\lambda) & \dots & b_{1n}(\lambda) \\ b_{21}(\lambda) & b_{22}(\lambda) & \dots & b_{2n}(\lambda) \\ \dots & \dots & \dots & \dots \\ b_{n1}(\lambda) & b_{n2}(\lambda) & \dots & b_{nn}(\lambda) \end{pmatrix}.$$

Dokážeme, že polynom $e_1(\lambda)$ dělí všechny polynomy v prvním řádku a v prvním sloupci λ -matic $B(\lambda)$. Předpokládejme, že tomu tak není, že polynom $e_1(\lambda)$ nedělí např. polynom $b_{21}(\lambda)$, tj.

$$b_{21}(\lambda) = e_1(\lambda) \cdot q(\lambda) + r(\lambda),$$

kde $r(\lambda)$ je nenulový polynom stupně menšího než k . Od druhého řádku λ -matic $B(\lambda)$ odečteme nyní $q(\lambda)$ -násobek jejího prvního řádku a potom zaměníme první a druhý řádek vzniklé λ -matic. Dostaneme tak λ -matici, která je ekvivalentní s λ -maticí $B(\lambda)$, a tedy i s λ -maticí $A(\lambda)$. V jejím levém horním rohu je však polynom $r(\lambda)$, který má stupeň menší než k . To je spor s definicí čísla k . Polynom $e_1(\lambda)$ tedy dělí polynom $b_{21}(\lambda)$ i ostatní polynomy v prvním sloupci a v prvním řádku λ -matic $A(\lambda)$.

Vhodné násobky prvního řádku λ -matic $B(\lambda)$ nyní odečteme od ostatních řádků λ -matic $B(\lambda)$, abychom v prvním sloupci na druhém až n -tém místě dostali samé nuly. Vhodné násobky prvního sloupce vzniklé λ -matic odečteme od ostatních sloupců, abychom v prvním řádku na druhém až n -tém místě dostali samé nuly. Dostaneme λ -matici $C(\lambda)$, která je ekvivalentní s λ -maticí $B(\lambda)$ a tedy i s λ -maticí $A(\lambda)$. Pišme

$$C(\lambda) = \begin{pmatrix} e_1(\lambda) & 0 & \dots & 0 \\ 0 & c_{22}(\lambda) & \dots & c_{2n}(\lambda) \\ \dots & \dots & \dots & \dots \\ 0 & c_{n2}(\lambda) & \dots & c_{nn}(\lambda) \end{pmatrix}.$$

Podle indukčního předpokladu je nyní možno elementárními úpravami prováděnými na druhý až n -tý řádek a na druhý až n -tý sloupec přejít od λ -matic $C(\lambda)$ k λ -matici

$$D(\lambda) = \begin{pmatrix} e_1(\lambda) & 0 & \dots & 0 \\ 0 & e_2(\lambda) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e_n(\lambda) \end{pmatrix},$$

ve které jsou polynomy $e_2(\lambda), \dots, e_n(\lambda)$ normované a pro každé $i = 2, \dots, n-1$ je polynom $e_{i+1}(\lambda)$ násobkem polynomu $e_i(\lambda)$. Zbývá dokázat, že polynom $e_1(\lambda)$ dělí polynom $e_2(\lambda)$. Předpokládejme, že

$$e_2(\lambda) = e_1(\lambda) \cdot q(\lambda) + r(\lambda),$$

kde $r(\lambda)$ je nenulový polynom stupně menšího než k . V λ -matici $D(\lambda)$ přičteme druhý řádek k prvnímu a potom od druhého sloupce odečteme $q(\lambda)$ -násobek prvního sloupce. Nakonec přehodíme první a druhý sloupec. Dostaneme λ -matici, která má v levém horním rohu polynom $r(\lambda)$, který má stupeň menší než k ; tato λ -matice je ekvivalentní s λ -maticí $D(\lambda)$ a tedy i s λ -maticí $A(\lambda)$. To je spor s definicí čísla k . Polynom $e_1(\lambda)$ tedy dělí polynom $e_2(\lambda)$, tj. $D(\lambda)$ je kanonická λ -matice, která je ekvivalentní s λ -maticí $A(\lambda)$. Tím je důkaz ukončen. \square

Důkaz předchozí věty dává praktický návod, jak k dané λ -matici najít kanonickou λ -matici, která je s ní ekvivalentní. V konkrétních příkladech však mnohdy neznáme „celou“ množinu \mathfrak{A} , proto se nám asi nepodaří ihned nalézt polynom $e_1(\lambda)$. Do levého horního rohu se pak snažíme dát polynom co možná nejmenšího stupně. Pomocí dělení se zbytkem — jak je v důkazu ukázáno na dvou místech — postupně k polynomu $e_1(\lambda)$ dospějeme (viz příklad 16.15(ii)). Další metodu pro nalezení kanonické λ -matice, která je s danou λ -maticí ekvivalentní, popíšeme v následujících odstavcích.

16.8. Příklad. Najdeme kanonickou λ -matici, která je ekvivalentní s reálnou λ -maticí

$$A(\lambda) = \begin{pmatrix} \lambda^2 & \lambda^2 - \lambda & 3\lambda^2 \\ \lambda^2 - \lambda & 3\lambda^2 - \lambda & \lambda^3 + 4\lambda^2 - 3\lambda \\ \lambda^2 + \lambda & \lambda^2 + \lambda & 3\lambda^2 + 3\lambda \end{pmatrix}.$$

Nejprve od druhého a třetího řádku odečteme první. Potom zaměníme první a třetí řádek. Dostaneme λ -matici

$$\begin{pmatrix} \lambda & 2\lambda & 3\lambda \\ -\lambda & 2\lambda^2 & \lambda^3 + \lambda^2 - 3\lambda \\ \lambda^2 & \lambda^2 - \lambda & 3\lambda^2 \end{pmatrix}.$$

První řádek přičteme ke druhému, λ -násobek prvního řádku odečteme od třetího. Potom odečteme dvojnásobek a trojnásobek prvního sloupce od druhého a třetího sloupce a dostaneme λ -matici

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & 2\lambda^2 + 2\lambda & \lambda^3 + \lambda^2 \\ 0 & -\lambda^2 - \lambda & 0 \end{pmatrix}.$$

Zaměníme druhý a třetí řádek. Druhý řádek vynásobíme číslem -1 . Potom odečteme dvojnásobek druhého řádku od třetího. Získáváme kanonickou λ -matici

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda^2 + \lambda & 0 \\ 0 & 0 & \lambda^3 + \lambda^2 \end{pmatrix} = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda(\lambda + 1) & 0 \\ 0 & 0 & \lambda^2(\lambda + 1) \end{pmatrix},$$

která je ekvivalentní s danou λ -maticí $A(\lambda)$.

Zatím jsme dokázali, že v každé třídě navzájem ekvivalentních λ -matic existuje alespoň jedna kanonická λ -matice (věta 16.7). V následujících odstavcích ukážeme, že v každé třídě navzájem ekvivalentních λ -matic existuje kanonická λ -matice právě jediná.

Nechť $A(\lambda)$ je λ -matice řádu n nad tělesem T . Pro každé $i = 1, \dots, n$ označme symbolem $a_i(\lambda)$ normovaného největšího společného dělitele všech subdeterminantů λ -matice $A(\lambda)$, které mají řád i ; jestliže jsou všechny tyto subdeterminanty rovny nule, klademe $a_i(\lambda) = 0$. Z věty o rozvoji determinantu ihned vyplývá, že pro každé $i = 1, \dots, n-1$ je prvek $a_{i+1}(\lambda)$ násobkem prvku $a_i(\lambda)$. Jestliže má λ -matice $A(\lambda)$ hodnotu r , je podle definice 14.22 $a_r(\lambda) \neq 0$ a $a_{r+1}(\lambda) = \dots = a_n(\lambda) = 0$.

16.9. Definice. Nechť $A(\lambda)$ je λ -matice řádu n nad tělesem T , která má hodnotu r . Pro každé $i = 1, \dots, n$ nechť je $a_i(\lambda)$ normovaný největší společný dělitel všech subdeterminantů λ -matice $A(\lambda)$, které mají řád i . *Invariantními polynomy* λ -matice $A(\lambda)$ budeme rozumět polynomy

$$e_1(\lambda) = a_1(\lambda), \quad e_2(\lambda) = \frac{a_2(\lambda)}{a_1(\lambda)}, \quad \dots, \quad e_r(\lambda) = \frac{a_r(\lambda)}{a_{r-1}(\lambda)},$$

$$e_{r+1}(\lambda) = \dots = e_n(\lambda) = 0.$$

16.10. Příklad. Reálná λ -matice $A(\lambda)$ z příkladu 16.8 má devět subdeterminantů prvního řádu, jsou to prvky λ -matice $A(\lambda)$:

$$\lambda^2, \lambda^2 - \lambda, 3\lambda^2, \lambda^2 - \lambda, 3\lambda^2 - \lambda, \lambda^3 + 4\lambda^2 - 3\lambda, \lambda^2 + \lambda, \lambda^2 + \lambda, 3\lambda^2 + 3\lambda.$$

Jejich normovaný největší společný dělitel je

$$a_1(\lambda) = \lambda.$$

Jediný subdeterminant třetího řádu je $\det A(\lambda)$.

$$\det A(\lambda) = \lambda^3(\lambda + 1) \begin{vmatrix} \lambda & \lambda - 1 & 3\lambda \\ \lambda - 1 & 3\lambda - 1 & \lambda^2 + 4\lambda - 3 \\ 1 & 1 & 3 \end{vmatrix} =$$

$$= \lambda^3(\lambda + 1) \begin{vmatrix} 0 & -1 & 0 \\ \lambda & 3\lambda & \lambda^2 + 4\lambda \\ 1 & 1 & 3 \end{vmatrix} = \lambda^3(\lambda + 1) \begin{vmatrix} \lambda & \lambda^2 + 4\lambda \\ 1 & 3 \end{vmatrix} =$$

$$= \lambda^3(\lambda + 1)(-\lambda^2 - \lambda).$$

Tedy $a_3(\lambda) = \lambda^4(\lambda + 1)^2$ (neboť je třeba normovat); hodnota λ -matice $A(\lambda)$ je 3. Z devíti subdeterminantů druhého řádu vypočteme nejprve ten, který získáme vynecháním třetího sloupce a třetího řádku.

$$\begin{aligned} \begin{vmatrix} \lambda^2 & \lambda^2 - \lambda \\ \lambda^2 - \lambda & 3\lambda^2 - \lambda \end{vmatrix} &= \lambda^2 \begin{vmatrix} \lambda & \lambda - 1 \\ \lambda - 1 & 3\lambda - 1 \end{vmatrix} = \lambda^2(3\lambda^2 - \lambda - \lambda^2 + 2\lambda - 1) = \\ &= \lambda^2(\lambda + 1)(2\lambda - 1) . \end{aligned}$$

Vzhledem k tomu, že $a_1(\lambda) = \lambda$ dělí $a_2(\lambda)$ a $a_2(\lambda)$ dělí $a_3(\lambda) = \lambda^4(\lambda + 1)^2$, máme (s přihlédnutím k výpočtu předchozího subdeterminantu řádu 2) pro $a_2(\lambda)$ jen tyto možnosti: $\lambda, \lambda^2, \lambda(\lambda + 1), \lambda^2(\lambda + 1)$. Protože ze všech tří řádků λ -matice $A(\lambda)$ je možno vytknout λ , je každý subdeterminant druhého řádu dělitelný polynomem λ^2 . Pro $a_2(\lambda)$ tedy zbývají dvě možnosti: $\lambda^2, \lambda^2(\lambda + 1)$. Protože z třetího řádku λ -matice $A(\lambda)$ je možno vytknout $\lambda + 1$, dělí polynom $\lambda + 1$ alespoň šest subdeterminantů druhého řádu. Zbývá tedy prověřit, zda polynom $\lambda + 1$ dělí subdeterminanty vzniklé vynecháním třetího řádku a prvního či druhého sloupce.

$$\begin{vmatrix} \lambda^2 - \lambda & 3\lambda^2 \\ 3\lambda^2 - \lambda & \lambda^3 + 4\lambda^2 - 3\lambda \end{vmatrix} = \lambda^2 \begin{vmatrix} \lambda - 1 & 3\lambda \\ 3\lambda - 1 & \lambda^2 + 4\lambda - 3 \end{vmatrix} = \lambda^2(\lambda + 1)(\lambda^2 - 7\lambda + 3) ,$$

$$\begin{vmatrix} \lambda^2 & 3\lambda^2 \\ \lambda^2 - \lambda & \lambda^3 + 4\lambda^2 - 3\lambda \end{vmatrix} = \lambda^3 \begin{vmatrix} 1 & 3 \\ \lambda - 1 & \lambda^2 + 4\lambda - 3 \end{vmatrix} = \lambda^4(\lambda + 1) .$$

Tedy $a_2(\lambda) = \lambda^2(\lambda + 1)$. Invariantními polynomy λ -matice $A(\lambda)$ jsou tedy polynomy

$$e_1(\lambda) = \lambda , \quad e_2(\lambda) = \lambda(\lambda + 1) , \quad e_3(\lambda) = \lambda^2(\lambda + 1) .$$

16.11. Lemma. *Ekvivalentním λ -maticím řádu n přísluší stejná posloupnost normovaných největších společných dělitelů všech jejich subdeterminantů řádu $i = 1, \dots, n$, a tedy i táž posloupnost invariantních polynomů.*

Důkaz. Nechť $A(\lambda)$ je λ -matice řádu n a $a_1(\lambda), \dots, a_n(\lambda)$ posloupnost jejich normovaných největších společných dělitelů všech subdeterminantů řádu $i = 1, \dots, n$. Nechť $B(\lambda)$ je λ -matice, která z λ -matice $A(\lambda)$ vznikla provedením jediné elementární úpravy, a nechť $b_1(\lambda), \dots, b_n(\lambda)$ je posloupnost normovaných největších společných dělitelů všech subdeterminantů řádu $i = 1, \dots, n$ λ -matice $B(\lambda)$.

Nechť $k(\lambda)$ je nějaký subdeterminant řádu i λ -matice $B(\lambda)$ a $m(\lambda)$ odpovídající subdeterminant λ -matice $A(\lambda)$, tj. subdeterminant vzniklý vynecháním sloupců a řádků s týmiž indexy.

Předpokládejme, že λ -matice $B(\lambda)$ vznikla z λ -matice $A(\lambda)$ užitím elementární úpravy prvního typu, tj. vynásobením nějakého sloupce nebo řádku nenulovým prvkem $c \in T$. Potom je

$$k(\lambda) = m(\lambda) \quad \text{nebo} \quad k(\lambda) = c \cdot m(\lambda) ,$$

podle toho, zda uvažovaný řádek nebo sloupec byl nebo nebyl vynechán při vytvoření uvedených subdeterminantů.

Předpokládejme, že λ -matice $B(\lambda)$ vznikla z λ -matice $A(\lambda)$ užitím elementární úpravy druhého typu; uvažujme např. přičtení $f(\lambda)$ -násobku j -tého řádku k l -tému řádku. Jestliže při vytvoření uvažovaných subdeterminantů byl l -tý řádek vynechán, je

$$k(\lambda) = m(\lambda) .$$

Jestliže l -tý řádek vynechán nebyl, potom podle 14.6 a 14.7(iv) je

$$k(\lambda) = m(\lambda) + f(\lambda) \cdot m_1(\lambda) ,$$

kde $m_1(\lambda)$ je determinant, při jehož vzniku byl použit místo l -tého řádku řádek j -tý. Přitom je buď $m_1(\lambda) = 0$ — pokud při vytváření subdeterminantů $k(\lambda)$ a $m(\lambda)$ nebyl j -tý řádek vynechán (v $m_1(\lambda)$ jsou totiž dva stejné řádky) — nebo je $m_1(\lambda) = \pm m_2(\lambda)$, kde $m_2(\lambda)$ je nějaký subdeterminant řádu i matice $A(\lambda)$ (znaménko je zde proto, že j -tý řádek není na svém místě). Je tedy buď

$$k(\lambda) = m(\lambda) \quad \text{nebo} \quad k(\lambda) = m(\lambda) \pm f(\lambda) \cdot m_2(\lambda) .$$

Stejně vztahy dostaneme v případě, kdy λ -matice $B(\lambda)$ vznikla z λ -matice $A(\lambda)$ přičtením $f(\lambda)$ -násobku j -tého sloupce k l -tému sloupci.

Z výše odvozených vztahů je zřejmé, že libovolný subdeterminant $k(\lambda)$ matice $B(\lambda)$, který má řád i , je dělitelný největším společným dělitelem $a_i(\lambda)$ všech subdeterminantů řádu i λ -matice $A(\lambda)$. Proto $a_i(\lambda)$ dělí $b_i(\lambda)$. Vzhledem k tomu, že naopak λ -matice $A(\lambda)$ vznikne z λ -matice $B(\lambda)$ provedením jedné elementární úpravy, dělí (podle již dokázaného) polynom $b_i(\lambda)$ polynom $a_i(\lambda)$. Protože jsou tyto polynomy normované, je $a_i(\lambda) = b_i(\lambda)$.

Provedením jedné, a tedy i konečně mnoha elementárních úprav se nemění posloupnost normovaných největších společných dělitelů všech subdeterminantů řádu $i = 1, \dots, n$. Nemění se tedy (viz definice 16.9) ani posloupnost invariantních polynomů. \square

16.12. Věta. *Každá čtvercová λ -matice $A(\lambda)$ je ekvivalentní s jedinou kanonickou λ -maticí. Tato kanonická λ -matice má na diagonále invariantní polynomy λ -matice $A(\lambda)$.*

Důkaz. Předpokládejme, že λ -matice $A(\lambda)$ je ekvivalentní s kanonickou λ -maticí

$$C(\lambda) = \begin{pmatrix} f_1(\lambda) & 0 & \dots & 0 \\ 0 & f_2(\lambda) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & f_n(\lambda) \end{pmatrix} ;$$

matice $C(\lambda)$ existuje podle věty 16.7. Podle lemmatu 16.11 mají λ -matice $A(\lambda)$ a $C(\lambda)$ stejnou posloupnost normovaných největších společných dělitelů $a_1(\lambda), \dots,$

$a_n(\lambda)$ všech subdeterminantů řádu $i = 1, \dots, n$. Z tvaru λ -matice $C(\lambda)$ (viz definice 16.6) vyplývá, že

$$\begin{aligned} a_1(\lambda) &= f_1(\lambda), \\ a_2(\lambda) &= f_1(\lambda)f_2(\lambda), \\ &\dots\dots\dots \\ a_n(\lambda) &= f_1(\lambda)\dots f_n(\lambda). \end{aligned}$$

Jestliže r je hodnota λ -matice $A(\lambda)$, potom je

$$a_r(\lambda) \neq 0 \quad \text{a} \quad a_{r+1}(\lambda) = \dots = a_n(\lambda) = 0.$$

Odtud

$$f_r(\lambda) \neq 0 \quad \text{a} \quad f_{r+1}(\lambda) = \dots = f_n(\lambda) = 0.$$

Invariantní polynomy λ -matice $A(\lambda)$ tedy jsou (viz definice 16.9):

$$\begin{aligned} e_1(\lambda) &= a_1(\lambda) = f_1(\lambda), \\ e_2(\lambda) &= \frac{a_2(\lambda)}{a_1(\lambda)} = f_2(\lambda), \\ &\dots\dots\dots \\ e_r(\lambda) &= \frac{a_r(\lambda)}{a_{r-1}(\lambda)} = f_r(\lambda), \\ e_{r+1}(\lambda) &= \dots = e_n(\lambda) = 0. \end{aligned}$$

Kanonická λ -matice $C(\lambda)$, která je ekvivalentní s λ -maticí $A(\lambda)$, je tedy určena invariantními polynomy $e_1(\lambda), \dots, e_n(\lambda)$ λ -matice $A(\lambda)$. \square

16.13. Definice. Nechť $A(\lambda)$ je čtvercová λ -matice nad tělesem T . *Kanonickým tvarem* λ -matice $A(\lambda)$ budeme rozumět jednoznačně určenou kanonickou λ -maticí, která je s λ -maticí $A(\lambda)$ ekvivalentní.

16.14. Důsledek. *Nechť $A(\lambda)$ a $B(\lambda)$ jsou λ -matice řádu n nad tělesem T . Následující tvrzení jsou ekvivalentní:*

- (i) $A(\lambda)$ a $B(\lambda)$ jsou ekvivalentní;
- (ii) $A(\lambda)$ a $B(\lambda)$ mají stejnou posloupnost normovaných největších společných dělitelů všech subdeterminantů řádu $i = 1, \dots, n$;
- (iii) $A(\lambda)$ a $B(\lambda)$ mají stejnou posloupnost invariantních polynomů;
- (iv) $A(\lambda)$ a $B(\lambda)$ mají stejný kanonický tvar. \square

Poznamenejme, že věta 16.12 dává spolu s definicí 16.9 další návod k nalezení kanonického tvaru polynomiální matice. Pro některé λ -matice je užitečné užít

metodu elementárních úprav popsanou v důkazu věty 16.7, pro jiné λ -matice je vhodnější užít metodu normovaných největších společných dělitelů. Obě uvedené metody se s úspěchem kombinují. Často se nejprve provádějí elementární úpravy, kterými přejdeme k jednodušší λ -matici, potom se najde posloupnost normovaných největších společných dělitelů a posloupnost invariantních polynomů.

16.15. Příklady.

(i) λ -matici $A(\lambda)$ z příkladu 16.8 jsme převedli na kanonický tvar oběma výše uvedenými způsoby; v příkladu 16.8 pomocí elementárních úprav, v příkladu 16.10 stanovením invariantních polynomů pomocí výpočtu subdeterminantů. Ani v jednom případě jsme však nemluvili o kanonickém tvaru, bylo to ještě před definicí 16.13.

(ii) Pro reálnou λ -matici

$$A(\lambda) = \begin{pmatrix} \lambda(\lambda - 1) & 0 & 0 \\ 0 & \lambda(\lambda - 2) & 0 \\ 0 & 0 & (\lambda - 1)(\lambda - 2) \end{pmatrix}$$

je zřejmě $a_1(\lambda) = 1$, neboť tři polynomy na diagonále jsou nesoudělné, dále je $\det A(\lambda) = \lambda^2(\lambda - 1)^2(\lambda - 2)^2 = a_3(\lambda)$. V λ -matici $A(\lambda)$ jsou pouze tři nenulové subdeterminanty druhého řádu:

$$\lambda^2(\lambda - 1)(\lambda - 2), \quad \lambda(\lambda - 1)^2(\lambda - 2), \quad \lambda(\lambda - 1)(\lambda - 2)^2.$$

Odtud $a_2(\lambda) = \lambda(\lambda - 1)(\lambda - 2)$. Invariantní polynomy λ -matice $A(\lambda)$ jsou tedy

$$e_1(\lambda) = 1, \quad e_2(\lambda) = \lambda(\lambda - 1)(\lambda - 2), \quad e_3(\lambda) = \lambda(\lambda - 1)(\lambda - 2).$$

Tím je určen i kanonický tvar λ -matice $A(\lambda)$.

Pomocí elementárních úprav se kanonický tvar λ -matice $A(\lambda)$ nalezne poměrně obtížně. K prvnímu řádku přičteme druhý a třetí řádek. Potom odečteme první sloupec od druhého a třetího. Dostaneme λ -matici

$$\begin{pmatrix} \lambda^2 - \lambda & -\lambda & -2\lambda + 2 \\ 0 & \lambda^2 - 2\lambda & 0 \\ 0 & 0 & \lambda^2 - 3\lambda + 2 \end{pmatrix}.$$

Nyní odečteme dvojnásobek druhého sloupce od třetího. Potom přehodíme první a třetí sloupec. Dostaneme λ -matici

$$\begin{pmatrix} 2 & -\lambda & \lambda^2 - \lambda \\ -2\lambda^2 + 4\lambda & \lambda^2 - 2\lambda & 0 \\ \lambda^2 - 3\lambda + 2 & 0 & 0 \end{pmatrix}.$$

Ke druhému sloupci přičteme $\frac{1}{2}\lambda$ -násobek prvního sloupce a ke třetímu sloupci $\frac{1}{2}(\lambda - \lambda^2)$ -násobek prvního sloupce. Potom přičteme vhodné násobky prvního řádku ke druhému a třetímu řádku. Dostaneme λ -matici

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -\lambda^3 + 3\lambda^2 - 2\lambda & \lambda^4 - 3\lambda^3 + 2\lambda^2 \\ 0 & \frac{1}{2}(\lambda^3 - 3\lambda^2 + 2\lambda) & \frac{1}{2}(-\lambda^4 + 4\lambda^3 - 5\lambda^2 + 2\lambda) \end{pmatrix}.$$

První řádek vynásobíme jednou polovinou a třetí řádek dvěma. Potom přičteme druhý řádek ke třetímu řádku, pak přičteme λ -násobek druhého sloupce ke třetímu, nakonec druhý řádek vynásobíme číslem -1 . Kanonickým tvarem λ -matice $A(\lambda)$ je tedy λ -matice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda(\lambda - 1)(\lambda - 2) & 0 \\ 0 & 0 & \lambda(\lambda - 1)(\lambda - 2) \end{pmatrix}.$$

(iii) Vypočteme kanonický tvar λ -matice $A(\lambda)$ nad tělesem \mathbb{Z}_3 , kde

$$A(\lambda) = \begin{pmatrix} \lambda^2 + 1 & 2\lambda & 1 \\ 0 & \lambda^2 + \lambda & \lambda^2 + 2\lambda + 1 \\ \lambda + 2 & 0 & \lambda \end{pmatrix}.$$

Opět uvedeme obě možnosti výpočtu, abychom měli možnost srovnání.

a) Přehodíme první a třetí sloupec. Přičteme λ -násobek, resp. $(2\lambda^2 + 2)$ -násobek prvního sloupce ke druhému, resp. třetímu sloupci. Ke druhému, resp. třetímu řádku přičteme $(2\lambda^2 + \lambda + 2)$ -násobek, resp. 2λ -násobek prvního řádku. Dostaneme λ -matici

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda^3 + 2\lambda & 2\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 2 \\ 0 & \lambda^2 & 2\lambda^3 + 2 \end{pmatrix}.$$

Ke třetímu sloupci přičteme λ -násobek druhého sloupce. Přehodíme druhý a třetí řádek a potom druhý a třetí sloupec. Dostaneme λ -matici

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & \lambda^2 \\ 0 & \lambda^3 + \lambda + 2 & \lambda^3 + 2\lambda \end{pmatrix}.$$

Ke třetímu sloupci přičteme λ^2 -násobek druhého, potom přičteme ke třetímu řádku $(\lambda^3 + \lambda + 2)$ -násobek druhého řádku. Druhý řádek znásobíme prvkem 2 a dostáváme kanonický tvar λ -matice $A(\lambda)$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda(\lambda^4 + 2\lambda^2 + 2\lambda + 2) \end{pmatrix}.$$

Invariantní polynomy λ -matice $A(\lambda)$ tedy jsou:

$$e_1(\lambda) = 1, \quad e_2(\lambda) = 1, \quad e_3(\lambda) = \lambda(\lambda^4 + 2\lambda^2 + 2\lambda + 2) = \lambda(\lambda + 1)^2(\lambda^2 + \lambda + 2).$$

b) Zřejmě je $a_1(\lambda) = 1$. Vypočteme $\det A(\lambda)$:

$$\det A(\lambda) = \lambda(\lambda + 1) \begin{vmatrix} \lambda^2 + 1 & 2 & 1 \\ 0 & 1 & \lambda + 1 \\ \lambda + 2 & 0 & \lambda \end{vmatrix} =$$

$$= \lambda(\lambda + 1)[\lambda(\lambda^2 + 1) + 2(\lambda + 1)(\lambda + 2) + 2(\lambda + 2)] = \lambda(\lambda + 1)(\lambda^3 + 2\lambda^2 + 2).$$

Tedy

$$a_3(\lambda) = \lambda(\lambda + 1)(\lambda^3 + 2\lambda^2 + 2) = \lambda(\lambda + 1)^2(\lambda^2 + \lambda + 2).$$

Ke zjištění $a_2(\lambda)$ stačí v tomto případě vypočítat pouze dva subdeterminanty řádu 2:

$$\det A_{21}(\lambda) = 2\lambda^2,$$

$$\det A_{12}(\lambda) = -(\lambda + 2)(\lambda^2 + 2\lambda + 1).$$

Protože jsou tyto subdeterminanty nesoudělné, je $a_2(\lambda) = 1$. Odtud

$$e_1(\lambda) = 1, \quad e_2(\lambda) = 1, \quad e_3(\lambda) = \lambda(\lambda + 1)^2(\lambda^2 + \lambda + 2);$$

známe tedy kanonický tvar λ -matice $A(\lambda)$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda(\lambda + 1)^2(\lambda^2 + \lambda + 2) \end{pmatrix}$$

(iv) Zjistíme, zda jsou nad tělesem komplexních čísel ekvivalentní λ -matice

$$A(\lambda) = \begin{pmatrix} \lambda + i & 0 & \lambda + 1 \\ 0 & \lambda + i & 0 \\ 0 & 0 & \lambda(\lambda + i) \end{pmatrix},$$

$$B(\lambda) = \begin{pmatrix} 2\lambda + 2i & \lambda + i & \lambda + 1 \\ \lambda + i & 0 & \lambda^2 + \lambda i + \lambda + 1 \\ \lambda + i & \lambda + i & \lambda^2 + \lambda i \end{pmatrix}.$$

Nejprve najdeme normované největší společné dělitele všech subdeterminantů řádu 1, 2, 3 λ -matice $A(\lambda)$ a její invariantní polynomy.

Zřejmě je $a_1(\lambda) = 1$, $a_3(\lambda) = \lambda(\lambda+i)^3$. V matici $A(\lambda)$ jsou pouze čtyři nenulové subdeterminanty druhého řádu:

$$\begin{aligned} \det A_{11}(\lambda) &= \lambda(\lambda+i)^2, & \det A_{33}(\lambda) &= (\lambda+i)^2, \\ \det A_{22}(\lambda) &= \lambda(\lambda+i)^2, & \det A_{31}(\lambda) &= -(\lambda+i)(\lambda+1). \end{aligned}$$

Je tedy $a_2(\lambda) = \lambda+i$. Matice $A(\lambda)$ má následující invariantní polynomy:

$$e_1(\lambda) = 1, \quad e_2(\lambda) = \lambda+i, \quad e_3(\lambda) = \lambda(\lambda+i)^2.$$

Nyní najdeme kanonický tvar λ -matice $B(\lambda)$. K prvnímu, resp. třetímu sloupci přičteme (-2) -násobek, resp. (-1) -násobek druhého sloupce. Třetí sloupec znásobíme číslem $(1-i)^{-1} = \frac{1}{2}(1+i)$ a potom přičteme $(-\lambda-i)$ -násobek třetího sloupce ke druhému. Vhodné násobky prvního řádku přičteme ke druhému a třetímu řádku. Dostáváme λ -matici

$$\begin{pmatrix} 0 & 0 & 1 \\ \lambda+i & (\lambda^2 + \lambda i + \lambda + 1)\frac{1}{2}(1+i)(-\lambda-i) & 0 \\ -\lambda-i & \lambda+i + (\lambda^2 + \lambda i - \lambda - i)\frac{1}{2}(1+i)(-\lambda-i) & 0 \end{pmatrix}.$$

Druhý řádek přičteme ke třetímu, potom přehodíme první a třetí sloupec. Druhý sloupec znásobíme číslem $(i-1)$. Dostáváme λ -matici

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & (\lambda^2 + \lambda i + \lambda + 1)(\lambda+i) & \lambda+i \\ 0 & 2(\lambda^2 + \lambda i)(\lambda+i) & 0 \end{pmatrix}.$$

Ke druhému sloupci přičteme $(-\lambda^2 - \lambda i - \lambda - 1)$ -násobek třetího sloupce. Třetí řádek vynásobíme číslem $\frac{1}{2}$ a přehodíme druhý a třetí sloupec. Dostáváme kanonický tvar λ -matice $B(\lambda)$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda+i & 0 \\ 0 & 0 & \lambda(\lambda+i)^2 \end{pmatrix}.$$

Podle důsledku 16.14 jsou λ -matice $A(\lambda)$ a $B(\lambda)$ ekvivalentní. Polynomiální matice $A(\lambda)$ a $B(\lambda)$ však nejsou ekvivalentní s λ -maticí

$$C(\lambda) = \begin{pmatrix} \lambda+i & 0 & 0 \\ 0 & \lambda(\lambda+i) & 0 \\ 0 & 0 & \lambda \end{pmatrix},$$

neboť tato λ -matice má invariantní polynomy

$$1, \quad \lambda(\lambda+i), \quad \lambda(\lambda+i).$$

Nechť $A(\lambda)$ je λ -matice řádu n nad tělesem T , která má hodnot r . Nechť $e_1(\lambda), \dots, e_n(\lambda)$ jsou její invariantní polynomy; tedy $e_{r+1}(\lambda) = \dots = e_n(\lambda) = 0$. Invariantní polynomy $e_1(\lambda), \dots, e_r(\lambda)$ nyní rozložíme v součin mocnin normovaných polynomů, které jsou v $T[\lambda]$ ireducibilní. Vzhledem k tomu, že pro každé $i = 1, \dots, r-1$ dělí polynom $e_i(\lambda)$ polynom $e_{i+1}(\lambda)$, vyskytují se v rozkladu polynomu $e_{i+1}(\lambda)$ všechny ireducibilní polynomy, které jsou v rozkladu polynomu $e_i(\lambda)$, a to alespoň v takových mocninách, v jakých jsou obsaženy v rozkladu polynomu $e_i(\lambda)$.

Poznamenejme, že jestliže je např. $e_i(\lambda) = 1$, potom je polynom $e_i(\lambda)$ chápán jako prázdný součin ireducibilních polynomů. Uvědomme si ještě, že rozklad invariantních polynomů na mocniny ireducibilních polynomů podstatně závisí na vlastnostech uvažovaného tělesa, případně na tom, nad jakým tělesem se rozklad provádí (viz dále příklady 16.17).

16.16. Definice. Nechť $A(\lambda)$ je λ -matice řádu n nad tělesem T , která má hodnot r . *Souborem elementárních polynomů* λ -matice $A(\lambda)$ budeme rozumět soubor všech polynomů, které vzniknou rozkladem invariantních polynomů $e_1(\lambda), \dots, e_r(\lambda)$ λ -matice $A(\lambda)$ na mocniny navzájem různých normovaných polynomů, které jsou ireducibilní v $T[\lambda]$.

Poznamenejme, že v souboru elementárních polynomů λ -matice $A(\lambda)$ se může tentýž polynom vyskytnout vícekrát (viz dále příklady 16.17).

Soubor elementárních polynomů λ -matice $A(\lambda)$ zapisujeme obvykle do tabulky, ve které jsou v každém řádku seřazeny všechny mocniny téhož ireducibilního polynomu, a to od největší k nejmenší. Řádky této tabulky nejsou obecně stejně dlouhé. Uvědomíme-li si, že soubor elementárních polynomů λ -matice $A(\lambda)$ vznikl rozkladem jejích invariantních polynomů $e_1(\lambda), \dots, e_r(\lambda)$, které se postupně navzájem dělí, je jasné, že první sloupec uvažované tabulky získáme rozkladem polynomu $e_r(\lambda)$, druhý sloupec rozkladem polynomu $e_{r-1}(\lambda)$ atd.

16.17. Příklady.

(i) Reálná λ -matice $A(\lambda)$ z příkladů 16.8 a 16.10 má invariantní polynomy

$$e_1(\lambda) = \lambda, \quad e_2(\lambda) = \lambda(\lambda + 1), \quad e_3(\lambda) = \lambda^2(\lambda + 1).$$

Soubor elementárních polynomů této λ -matice zapíšeme do tabulky:

$$\begin{array}{ccc} \lambda^2 & \lambda & \lambda \\ \lambda + 1 & \lambda + 1 & \end{array}$$

První sloupec tabulky vznikl rozkladem polynomu $e_3(\lambda)$, druhý rozkladem polynomu $e_2(\lambda)$, třetí rozkladem polynomu $e_1(\lambda)$. Soubor elementárních polynomů λ -matice $A(\lambda)$ je stejný, ať uvažujeme λ -matici $A(\lambda)$ nad tělesem racionálních, reálných či komplexních čísel.

(ii) Soubor elementárních polynomů λ -matice $A(\lambda)$ z příkladu 16.15(ii) zapíšeme do následující tabulky:

$$\begin{array}{cc} \lambda & \lambda \\ \lambda - 1 & \lambda - 1 \\ \lambda - 2 & \lambda - 2 \end{array}$$

Invariantní polynomy $e_3(\lambda)$, resp. $e_2(\lambda)$ jsou součiny prvního, resp. druhého sloupce tabulky, dále je $e_1(\lambda) = 1$ (třetí sloupec tabulky je prázdný).

(iii) Soubor elementárních polynomů kanonické λ -matice

$$A(\lambda) = \begin{pmatrix} \lambda^2 + 1 & 0 & 0 \\ 0 & \lambda(\lambda^2 + 1) & 0 \\ 0 & 0 & \lambda^2(\lambda^2 + 1)(\lambda^2 - 3) \end{pmatrix}$$

závisí podstatně na tom, nad jakým tělesem tuto λ -matici uvažujeme. Nad tělesem racionálních čísel dostáváme tuto tabulku elementárních polynomů:

$$\begin{array}{ccc} \lambda^2 & \lambda & \\ \lambda^2 + 1 & \lambda^2 + 1 & \lambda^2 + 1 \\ \lambda^2 - 3 & & \end{array}$$

Nad tělesem reálných čísel bude tabulka jiná:

$$\begin{array}{ccc} \lambda^2 & \lambda & \\ \lambda^2 + 1 & \lambda^2 + 1 & \lambda^2 + 1 \\ \lambda - \sqrt{3} & & \\ \lambda + \sqrt{3} & & \end{array}$$

Nad tělesem komplexních čísel bude takováto:

$$\begin{array}{ccc} \lambda^2 & \lambda & \\ \lambda + i & \lambda + i & \lambda + i \\ \lambda - i & \lambda - i & \lambda - i \\ \lambda - \sqrt{3} & & \\ \lambda + \sqrt{3} & & \end{array}$$

(iv) Reálné λ -matice

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda^2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^2 \end{pmatrix}$$

nejsou ekvivalentní, ale mají stejný soubor elementárních polynomů:

$$\{ \lambda^2, \lambda \}.$$

Uvažované λ -matice mají stejný řád, ale různou hodnotu.

(v) Tabulka elementárních polynomů λ -matice $A(\lambda)$ z příkladu 16.15(iii) je:

$$\begin{array}{c} \lambda \\ (\lambda + 1)^2 \\ \lambda^2 + \lambda + 2 \end{array}$$

(vi) Tabulka elementárních polynomů λ -matice $A(\lambda)$ (a tedy i λ -matice $B(\lambda)$) z příkladu 16.15(iv) je:

$$\begin{array}{c} (\lambda + i)^2 \quad \lambda + i \\ \lambda \end{array}$$

Každá λ -matice určuje své invariantní polynomy a ty určují soubor elementárních polynomů (s přihlédnutím k tomu, nad jakým tělesem pracujeme). Z předchozího výkladu o uspořádání souboru elementárních polynomů do tabulky vyplývá, že ze souboru elementárních polynomů umíme vytvořit invariantní polynomy, známe-li navíc řád n a hodnotu r výchozí λ -matice $A(\lambda)$. Polynomy $e_r(\lambda)$, $e_{r-1}(\lambda)$, \dots , $e_1(\lambda)$ jsou součiny po řadě prvního, druhého, \dots , r -tého sloupce tabulky (je-li tento sloupec prázdný, je příslušný invariantní polynom roven 1); dále klademe $e_{r+1}(\lambda) = \dots = e_n(\lambda) = 0$. Platí tedy následující tvrzení.

16.18. Věta.

- (i) Řád λ -matice $A(\lambda)$, její hodnota a soubor elementárních polynomů určují její invariantní polynomy.
- (ii) Dvě λ -matice téhož řádu jsou ekvivalentní právě tehdy, když mají stejnou hodnotu a stejný soubor elementárních polynomů.

Důkaz. Tvrzení (i) vyplynulo z předchozí úvahy, tvrzení (ii) je důsledkem tvrzení (i) a důsledku 16.14. \square

16.19. Příklad.

(i) Ze souboru elementárních polynomů

$$\{ \lambda^2, (\lambda + 1)^3, \lambda, (\lambda^2 + 1)^2, \lambda^3, \lambda^2 + 3, \lambda + 1, \lambda + 1, (\lambda^2 + 1)^2, \lambda \}$$

reálné polynomiální matice $A(\lambda)$ řádu 8 a hodnoty 5 určíme její invariantní polynomy. Nejprve sestavíme elementární polynomy do tabulky:

$$\begin{array}{cccc} \lambda^3 & \lambda^2 & \lambda & \lambda \\ (\lambda + 1)^3 & \lambda + 1 & \lambda + 1 & \\ (\lambda^2 + 1)^2 & (\lambda^2 + 1)^2 & & \\ \lambda^2 + 3 & & & \end{array}$$

Nyní je

$$\begin{aligned} e_8(\lambda) &= e_7(\lambda) = e_6(\lambda) = 0, \\ e_5(\lambda) &= \lambda^3(\lambda+1)^3(\lambda^2+1)^2(\lambda^2+3), \\ e_4(\lambda) &= \lambda^2(\lambda+1)(\lambda^2+1)^2, \\ e_3(\lambda) &= \lambda(\lambda+1), \\ e_2(\lambda) &= \lambda, \\ e_1(\lambda) &= 1. \end{aligned}$$

Pokud by λ -matice $A(\lambda)$ měla řád 4 a hodnotu rovněž 4, bylo by

$$\begin{aligned} e_4(\lambda) &= \lambda^3(\lambda+1)^3(\lambda^2+1)^2(\lambda^2+3), \\ e_3(\lambda) &= \lambda^2(\lambda+1)(\lambda^2+1)^2, \\ e_2(\lambda) &= \lambda(\lambda+1), \\ e_1(\lambda) &= \lambda. \end{aligned}$$

λ -matice s výše uvedeným souborem elementárních polynomů nemůže však mít např. řád 6 a hodnotu 3, řád 3 apod.

(ii) Soubor polynomů

$$\{ \lambda^2, \lambda, \lambda, \lambda+1, \lambda+1 \}$$

nemůže být souborem elementárních polynomů λ -matice $A(\lambda)$ řádu 4 hodnoti 2. Hodnota totiž nemůže být menší než počet prvků nejdelšího řádku tabulky elementárních polynomů. Uvedený soubor může být souborem elementárních polynomů λ -matice řádu 6 a hodnoti 4 apod.

V následujících odstavcích se ještě vrátíme k vyjádření polynomiálních matic maticovými polynomy, které jsme zavedli hned za definicí 16.1 (viz též příklad 16.2).

16.20. Poznámka. Nechť $A(\lambda)$ a $B(\lambda)$ jsou λ -matice téhož řádu nad tělesem T . Pišme

$$\begin{aligned} A(\lambda) &= A_0\lambda^r + A_1\lambda^{r-1} + \cdots + A_{r-1}\lambda + A_r, \\ B(\lambda) &= B_0\lambda^s + B_1\lambda^{s-1} + \cdots + B_{s-1}\lambda + B_s, \end{aligned}$$

kde $r = \deg A(\lambda)$ a $s = \deg B(\lambda)$, tj. A_0 a B_0 jsou nenulové matice; předpokládejme, že je např. $r \geq s$. Snadno se ověří, že

$$A(\lambda) + B(\lambda) = A_0\lambda^r + \dots + A_{r-s-1}\lambda^{s+1} + \\ + (A_{r-s} + B_0)\lambda^s + \dots + (A_{r-1} + B_{s-1})\lambda + A_r + B_s ,$$

$$A(\lambda) \cdot B(\lambda) = A_0B_0\lambda^{r+s} + (A_0B_1 + A_1B_0)\lambda^{r+s-1} + \dots + \\ + (A_{r-1}B_s + A_rB_{s-1})\lambda + A_rB_s .$$

Součet a součin λ -matic $A(\lambda)$ a $B(\lambda)$ tedy můžeme počítat jako součet a součin odpovídajících maticových polynomů. Platí zde obdobné vztahy jako pro operace s polynomy z $T[\lambda]$. Zřejmě je

$$\deg(A(\lambda) + B(\lambda)) \leq \max(\deg A(\lambda), \deg B(\lambda)) ;$$

ostrá nerovnost nastane pouze v případě, že mají maticové polynomy stejný stupeň a jejich vedoucí koeficienty jsou opačné matice ($r = s$ a $A_0 = -B_0$). Dále je

$$\deg(A(\lambda) \cdot B(\lambda)) \leq \deg A(\lambda) + \deg B(\lambda) ;$$

ostrá nerovnost nastane, když součin A_0B_0 vedoucích koeficientů obou maticových polynomů je nulová matice.

V následujícím odstavci se budeme zabývat dělením maticových polynomů. Vzhledem k tomu, že násobení matic není komutativní, musíme rozlišovat *dělení zleva* a *dělení zprava*. Formulaci následujícího výsledku o dělení maticových polynomů i jeho důkaz získáme jednoduchým přepisem odpovídající partie o polynomech nad okruhem.

16.21. Věta. *Nechť $A(\lambda)$ a $B(\lambda)$ jsou λ -matice stejného řádu nad tělesem T . Jestliže je vedoucí koeficient maticového polynomu $B(\lambda)$ regulární matice, potom platí:*

- (i) *Existuje právě jediná λ -matice $Q(\lambda)$ a právě jediná λ -matice $R(\lambda)$ nad tělesem T , pro které*

$$A(\lambda) = B(\lambda) \cdot Q(\lambda) + R(\lambda)$$

a buď $R(\lambda) = O$ nebo $\deg R(\lambda) < \deg B(\lambda)$.

- (ii) *Existuje právě jediná λ -matice $Q'(\lambda)$ a právě jediná λ -matice $R'(\lambda)$ nad tělesem T , pro které*

$$A(\lambda) = Q'(\lambda) \cdot B(\lambda) + R'(\lambda)$$

a buď $R'(\lambda) = O$ nebo $\deg R'(\lambda) < \deg B(\lambda)$.

Důkaz. Dokážeme tvrzení (i); tvrzení (ii) se dokáže obdobně.

Nejprve dokážeme existenci λ -matic $Q(\lambda)$ a $R(\lambda)$ s uvedenými vlastnostmi. Označme $\deg A(\lambda) = k$, $\deg B(\lambda) = m$; nechť A_0 a B_0 jsou vedoucí koeficienty maticových polynomů $A(\lambda)$ a $B(\lambda)$. Budeme postupovat indukcí podle $n = k - m$. Je-li $n < 0$, tj. $k < m$, položíme $Q(\lambda) = O$ a $R(\lambda) = A(\lambda)$; je tedy

$$A(\lambda) = B(\lambda) \cdot O + A(\lambda) .$$

Předpokládejme nyní, že $n \geq 0$ (tj. $k \geq m$) a že pro všechna celá čísla menší než n dokazované tvrzení platí. Maticový polynom

$$C(\lambda) = A(\lambda) - B(\lambda) \cdot (B_0^{-1} A_0 \lambda^{k-m}) \quad (1)$$

má zřejmě stupeň nejvýše $k - 1$ a proto je

$$\deg C(\lambda) - \deg B(\lambda) \leq k - 1 - m < n .$$

Podle indukčního předpokladu existují takové λ -matice $P(\lambda)$ a $R(\lambda)$, že

$$C(\lambda) = B(\lambda) \cdot P(\lambda) + R(\lambda) , \quad (2)$$

kde buď $R(\lambda) = O$ nebo $\deg R(\lambda) < \deg B(\lambda)$. Dosadíme-li do vztahu (2) za $C(\lambda)$ z rovnosti (1), dostáváme rovnost

$$A(\lambda) = B(\lambda) \cdot (B_0^{-1} A_0 \lambda^{k-m} + P(\lambda)) + R(\lambda) .$$

Nyní stačí položit $Q(\lambda) = B_0^{-1} A_0 \lambda^{k-m} + P(\lambda)$.

Nyní dokážeme, že λ -matice $Q(\lambda)$ a $R(\lambda)$ s výše uvedenými vlastnostmi jsou λ -maticemi $A(\lambda)$ a $B(\lambda)$ určeny jednoznačně. Předpokládejme, že

$$A(\lambda) = B(\lambda) \cdot Q(\lambda) + R(\lambda) = B(\lambda) \cdot Q_1(\lambda) + R_1(\lambda)$$

je dvojný vyjádření λ -matice $A(\lambda)$ výše uvedeného typu. Je tedy

$$B(\lambda) \cdot (Q(\lambda) - Q_1(\lambda)) = R_1(\lambda) - R(\lambda) . \quad (3)$$

Jestliže $Q(\lambda) \neq Q_1(\lambda)$, potom je

$$\deg [B(\lambda) \cdot (Q(\lambda) - Q_1(\lambda))] \geq \deg B(\lambda) ,$$

neboť vedoucí koeficient maticového polynomu $B(\lambda)$ je regulární matice. Docházíme tak ke sporu, neboť polynom $R_1(\lambda) - R(\lambda)$ na druhé straně rovnosti (3) je buď nulový, nebo má menší stupeň než polynom $B(\lambda)$. Je tedy $Q(\lambda) = Q_1(\lambda)$ a z rovnosti (3) pak vyplývá rovnost $R(\lambda) = R_1(\lambda)$. \square

Povšimněme si, že jsme v obou částech důkazu využili předpoklad o regularitě vedoucího koeficientu B_0 maticového polynomu $B(\lambda)$.

Na závěr uvedeme ještě jedno početní lemma, které využijeme v následujícím paragrafu. Týká se speciálního případu dělení maticových polynomů, kdy je dělitel prvního stupně a jeho vedoucím koeficientem je jednotková matice. Při takovémto dělení nás často zajímá zbytek; jeho stupeň je menší než stupeň dělitele a je to tedy „obyčejná“ matice nad tělesem T , ve které se už neurčitá λ nevyskytuje.

16.22. Lemma. *Nechť $B(\lambda)$ je λ -matice nad tělesem T , která je vyjádřena jako maticový polynom stupně k v tvaru*

$$B(\lambda) = B_0\lambda^k + B_1\lambda^{k-1} + \cdots + B_{k-1}\lambda + B_k .$$

(i) *Jestliže $B(\lambda) = (\lambda E - A) \cdot Q(\lambda) + R$, potom*

$$R = A^k B_0 + A^{k-1} B_1 + \cdots + AB_{k-1} + B_k ,$$

tj. zbytek R při dělení λ -matice $B(\lambda)$ λ -maticí $\lambda E - A$ zleva dostaneme „dosazením zleva“ matice A do maticového polynomu $B(\lambda)$.

(ii) *Jestliže $B(\lambda) = Q'(\lambda) \cdot (\lambda E - A) + R'$, potom*

$$R' = B_0 A^k + B_1 A^{k-1} + \cdots + B_{k-1} A + B_k ,$$

tj. zbytek R' při dělení λ -matice $B(\lambda)$ λ -maticí $\lambda E - A$ zprava dostaneme „dosazením zprava“ matice A do maticového polynomu $B(\lambda)$.

Důkaz. Dokážeme tvrzení (i); tvrzení (ii) se dokáže obdobně. Pišme

$$Q(\lambda) = Q_0\lambda^{k-1} + Q_1\lambda^{k-2} + \cdots + Q_{k-2}\lambda + Q_{k-1} ;$$

maticový polynom $Q(\lambda)$ má stupeň $k - 1$, neboť λ -matice $(\lambda E - A) \cdot Q(\lambda)$ má stupeň k . Po vynásobení maticových polynomů $(\lambda E - A)$ a $Q(\lambda)$ a porovnání koeficientů v rovnosti

$$B(\lambda) = (\lambda E - A) \cdot Q(\lambda) + R$$

dostáváme následující vztahy:

$$B_0 = Q_0 ,$$

$$B_1 = Q_1 - AQ_0 ,$$

$$B_2 = Q_2 - AQ_1 ,$$

.....

$$B_{k-1} = Q_{k-1} - AQ_{k-2} ,$$

$$B_k = R - AQ_{k-1} .$$

Vynásobíme-li tyto rovnosti po řadě maticemi $A^k, A^{k-1}, \dots, A, E$ zleva a sečteme-li je, dostaneme výše uvedené vyjádření matice R . \square

Na závěr tohoto paragrafu zavedeme ještě pojem unimodulární λ -matice a dokážeme několik jednoduchých tvrzení.

16.23. Definice. λ -matice $A(\lambda)$ se nazývá *unimodulární*, jestliže je ekvivalentní s jednotkovou maticí.

16.24. Věta. *Nechť $A(\lambda)$ je λ -matice nad tělesem T . Následující tvrzení jsou ekvivalentní:*

- (i) λ -matice $A(\lambda)$ je unimodulární.
- (ii) λ -matice $A(\lambda)$ je součinem elementárních transformačních λ -matic.
- (iii) Determinant λ -matice $A(\lambda)$ je nenulovým prvkem tělesa T .
- (iv) K λ -matici $A(\lambda)$ existuje inverzní λ -matice.

Důkaz. Nechť $A(\lambda)$ je λ -matice řádu n . Jestliže je $A(\lambda)$ unimodulární, je podle definice 16.23

$$A(\lambda) = X(\lambda) \cdot E \cdot Y(\lambda),$$

kde $X(\lambda)$ a $Y(\lambda)$ jsou součiny elementárních transformačních λ -matic; z tvrzení (i) tedy vyplývá tvrzení (ii). Platí-li tvrzení (ii), platí podle věty o násobení determinantů i tvrzení (iii). Jestliže platí tvrzení (iii), pak jsou podle důsledku 16.14 λ -matice $A(\lambda)$ a E ekvivalentní, neboť mají stejnou posloupnost normovaných největších společných dělitelů všech subdeterminantů řádu $i = 1, \dots, n$. Tvrzení (iii) a (iv) jsou ekvivalentní podle věty 14.18 (resp. důsledku 14.19). \square

Z věty 14.14 o násobení determinantů ihned vyplývá, že součin unimodulárních λ -matic je opět unimodulární λ -matice a že inverzní λ -maticí k unimodulární λ -matici je opět unimodulární λ -matice. Každá regulární matice nad tělesem T je unimodulární.

16.25. Věta. *Dvě λ -matice $A(\lambda)$ a $B(\lambda)$ nad tělesem T jsou ekvivalentní právě tehdy, když existují unimodulární λ -matice $X(\lambda)$ a $Y(\lambda)$, pro které je*

$$A(\lambda) = X(\lambda) \cdot B(\lambda) \cdot Y(\lambda).$$

Důkaz. Tvrzení věty ihned vyplývá z definice 16.5 a věty 16.24. \square

16.26. Příklad. Uvažujme λ -matici

$$A(\lambda) = \begin{pmatrix} \lambda & \lambda^3 + 5 \\ \lambda^2 - \lambda - 4 & \lambda^4 - \lambda^3 - 4\lambda^2 + 5\lambda - 5 \end{pmatrix}$$

nad tělesem reálných čísel.

Zřejmě je

$$\det A(\lambda) = \lambda(\lambda^4 - \lambda^3 - 4\lambda^2 + 5\lambda - 5) - (\lambda^3 + 5)(\lambda^2 - \lambda - 4) = 20.$$

Podle věty 16.24 je λ -matice $A(\lambda)$ unimodulární. Inverzní λ -matici $A(\lambda)^{-1}$ můžeme najít podle věty 14.18 (resp. příkladu 14.20(ii)):

$$A(\lambda)^{-1} = \frac{1}{20} \cdot \begin{pmatrix} \lambda^4 - \lambda^3 - 4\lambda^2 + 5\lambda - 5 & -\lambda^3 - 5 \\ -\lambda^2 + \lambda + 4 & \lambda \end{pmatrix}$$

17. CHARAKTERISTICKÝ A MINIMÁLNÍ POLYNOM, VLASTNÍ ČÍSLA A VLASTNÍ VEKTORY

17.1. Definice. Nechť A je čtvercová matice nad tělesem T . *Charakteristickou maticí* matice A budeme rozumět λ -matici $\lambda E - A$ a *charakteristickým polynomem* matice A determinant její charakteristické matice, tj. $\det(\lambda E - A)$. Kořeny charakteristického polynomu matice A se nazývají *vlastní čísla* matice A . *Násobností* vlastního čísla budeme rozumět jeho násobnost jako kořene charakteristického polynomu. *Spektrém matice* A budeme nazývat soubor utvořený z vlastních čísel matice A ; každé vlastní číslo se v něm vyskytuje právě tolikrát, kolik činí jeho násobnost.

Charakteristickou maticí matice A jsme zavedli jako maticový polynom prvního stupně; jeho vedoucím koeficientem je jednotková matice a absolutním členem matice $-A$ (měli bychom vlastně psát $E\lambda - A$ jako v předchozím paragrafu, např. v 16.2, to však není zvykem). Je-li $A = (a_{ij})$ matice řádu n , je

$$\lambda E - A = \begin{pmatrix} \lambda - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ -a_{n1} & -a_{n2} & \dots & \lambda - a_{nn} \end{pmatrix}.$$

Stanovení vlastních čísel podstatně závisí na tělese T , nad kterým pracujeme; vlastními čísly matice A jsou podle definice právě ty kořeny charakteristického polynomu, které leží v tělese T . Přejdeme-li k jinému tělesu, může se spektrum matice změnit.

Poznamenejme, že někdy se charakteristickou maticí matice A rozumí λ -matice $A - \lambda E$; pokud bychom této definici užili, změnil by se další výklad jen nepodstatně.

17.2. Příklady.

(i) Uvažujme matici

$$A = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 0 & -2 \\ 2 & 0 & -1 \end{pmatrix}.$$

Její charakteristickou maticí je λ -matice

$$\lambda E - A = \begin{pmatrix} \lambda - 1 & 0 & 1 \\ 1 & \lambda & 2 \\ -2 & 0 & \lambda + 1 \end{pmatrix}$$

a jejím charakteristickým polynomem polynom

$$\det(\lambda E - A) = \lambda(\lambda - 1)(\lambda + 1) + 2\lambda = \lambda(\lambda^2 + 1).$$

Nad tělesem racionálních nebo reálných čísel má matice A jediné vlastní číslo $\lambda_1 = 0$ (násobnosti jedna) a spektrum $\{0\}$. Nad tělesem komplexních čísel má matice A tři vlastní čísla $\lambda_1 = 0$, $\lambda_2 = i$, $\lambda_3 = -i$ násobnosti jedna a spektrum $\{0, i, -i\}$.

(ii) Charakteristický polynom horní (dolní) trojúhelníkové matice $A = (a_{ij})$ řádu n je roven

$$(\lambda - a_{11})(\lambda - a_{22}) \dots (\lambda - a_{nn}) ,$$

vlastními čísly matice A jsou prvky a_{11}, \dots, a_{nn} .

17.3. Věta. *Nechť A je čtvercová matice řádu n nad tělesem T .*

- (i) *Charakteristický polynom matice A má stupeň n , je normovaný, jeho absolutní člen je roven $(-1)^n \det A$ a koeficient u λ^{n-1} je roven $-\operatorname{tr} A$.*
- (ii) *Jestliže je charakteristický polynom matice A rozložitelný v $T[\lambda]$ na lineární faktory (je-li např. těleso T algebraicky uzavřené), potom je stopa $\operatorname{tr} A$ matice A součtem a determinant $\det A$ matice A součinem všech prvků spektra matice A .*

Důkaz. Vzhledem k tomu, že v λ -matici $\lambda E - A$ se neurčitá λ vyskytuje právě n -krát, nemůže mít charakteristický polynom matice A větší stupeň než n . Píšeme $A = (a_{ij})$ a

$$\det(\lambda E - A) = c_0 \lambda^n + c_1 \lambda^{n-1} + \dots + c_n .$$

(i) Z definice determinantu vyplývá, že členy s n -tou a $(n-1)$ -ní mocninou neurčité λ můžeme dostat pouze ze součinnu prvků diagonály matice $\lambda E - A$, tj. ze součinnu

$$(\lambda - a_{11})(\lambda - a_{22}) \dots (\lambda - a_{nn}) .$$

Tedy

$$c_0 = 1 \quad \text{a} \quad c_1 = -(a_{11} + a_{22} + \dots + a_{nn}) = -\operatorname{tr} A .$$

Položíme-li $\lambda = 0$, vyplývá z výše uvedeného zápisu charakteristického polynomu rovnost

$$c_n = \det(-A) = (-1)^n \det A .$$

(ii) Je-li

$$\det(\lambda E - A) = (\lambda - \lambda_1)(\lambda - \lambda_2) \dots (\lambda - \lambda_n) ,$$

kde $\lambda_1, \lambda_2, \dots, \lambda_n \in T$ jsou vlastní čísla, která nemusí být navzájem různá, je zřejmé

$$c_1 = -(\lambda_1 + \lambda_2 + \dots + \lambda_n) \quad \text{a} \quad c_n = (-1)^n \lambda_1 \lambda_2 \dots \lambda_n .$$

Odtud

$$\operatorname{tr} A = \sum_{i=1}^n \lambda_i \quad \text{a} \quad \det A = \prod_{i=1}^n \lambda_i .$$

Jestliže je těleso T algebraicky uzavřené, je charakteristický polynom každé matice rozložitelný na lineární faktory a předchozí dvě rovnosti platí pro jakoukoli matici A nad T řádu n . \square

Viděli jsme, že stupeň charakteristického polynomu $\det(\lambda E - A)$ matice A je roven řádu matice A . Proto je charakteristická matice $\lambda E - A$ každé matice A regulární (viz definice 14.22). Protože je $c_n = (-1)^n \det A$, je matice A regulární právě tehdy, když má její charakteristický polynom nenulový absolutní člen; matice je tedy singulární právě tehdy, je-li 0 jejím vlastním číslem.

17.4. Poznámka. Předchozí větu můžeme snadno zobecnit. Musíme však zavést pojem *hlavní subdeterminant* čtvercové matice. Je to determinant matice, která vznikne vynecháním řádků a sloupců se stejnými indexy; hlavní úhlopříčka této dílčí matice je částí hlavní úhlopříčky výchozí matice.

První tvrzení předchozí věty zobecníme takto:

Jestliže A je matice řádu n a $c_0\lambda^n + c_1\lambda^{n-1} + \dots + c_n$ její charakteristický polynom, potom je $c_0 = 1$ a pro každé $i = 1, \dots, n$ je $c_i = (-1)^i K_i$, kde K_i je součet všech hlavních subdeterminantů řádu i matice A .

Důkaz tohoto tvrzení můžeme provést tak, že vypočteme charakteristický polynom matice A podle lemmatu 14.6. Každý sloupec determinantu $\det(\lambda E - A)$ si představíme jako součet dvou sloupců: záporně vzatého sloupce matice A a sloupce s jediným λ a samými nulami. Determinant $\det(\lambda E - A)$ se takto rozloží na součet 2^n determinantů. V jednom z nich jsou na diagonále prvky λ a všude jinde nuly, ve druhém není žádné λ — tyto determinanty jsou rovny λ^n a $(-1)^n \det A$. Každý ze zbývajících $2^n - 2$ determinantů se dá postupně rozvést podle sloupců, ve kterých stojí λ ; výsledkem je vždy nějaký hlavní subdeterminant řádu i matice A násobený $(-1)^i \lambda^{n-i}$. Sdružíme-li nyní jednotlivé sčítance podle toho, v jaké mocnině se v nich λ vyskytuje, získáme výše uvedená vyjádření koeficientů c_1, \dots, c_{n-1} .

Rovněž druhé tvrzení věty 17.3 můžeme zobecnit.

Jestliže je charakteristický polynom matice A rozložitelný v $T[\lambda]$ na lineární faktory, tj.

$$\lambda^n + c_1\lambda^{n-1} + \dots + c_n = (\lambda - \lambda_1)(\lambda - \lambda_2) \dots (\lambda - \lambda_n),$$

potom je

$$c_1 = - \sum_{i=1}^n \lambda_i, \quad c_2 = \sum_{\substack{i,j=1,\dots,n \\ i \neq j}} \lambda_i \lambda_j, \quad \dots,$$

$$c_{n-1} = (-1)^{n-1} \sum_{i=1}^n \lambda_1 \dots \lambda_{i-1} \lambda_{i+1} \dots \lambda_n, \quad c_n = (-1)^n \prod_{i=1}^n \lambda_i.$$

Toto tvrzení dokážeme roznásobením lineárních faktorů na pravé straně výše uvedené rovnosti a porovnáním odpovídajících koeficientů.

17.5. Příklady.

(i) V příkladu 17.2(i) je $\det(\lambda E - A) = \lambda^3 + \lambda$, tedy

$$c_0 = 1, \quad c_1 = -\operatorname{tr} A = 0, \quad c_2 = 1, \quad c_3 = -\det A = 0;$$

přitom je c_2 součtem všech hlavních subdeterminantů druhého řádu, tj.

$$c_2 = \begin{vmatrix} 0 & -2 \\ 0 & -1 \end{vmatrix} + \begin{vmatrix} 1 & -1 \\ 2 & -1 \end{vmatrix} + \begin{vmatrix} 1 & 0 \\ -1 & 0 \end{vmatrix} = 1.$$

Matice A je singulární, proto je $c_3 = 0$. Chápeme-li matici A nad tělesem komplexních čísel, je

$$\begin{aligned} c_1 &= 0 = (-1) \cdot (0 + i + (-i)), \\ c_2 &= 1 = (-1)^2 \cdot (0 \cdot i + 0 \cdot (-i) + i \cdot (-i)), \\ c_3 &= 0 = (-1)^3 \cdot 0 \cdot i \cdot (-i). \end{aligned}$$

(ii) Charakteristickou maticí reálné matice

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

je λ -matice

$$\lambda E - A = \begin{pmatrix} \lambda - 3 & -1 & 1 \\ 0 & \lambda - 2 & 0 \\ -1 & -1 & \lambda - 1 \end{pmatrix}$$

a charakteristickým polynomem matice A je polynom

$$\det(\lambda E - A) = (\lambda - 3)(\lambda - 2)(\lambda - 1) + (\lambda - 2) = (\lambda - 2)^3 = \lambda^3 - 6\lambda^2 + 12\lambda - 8.$$

Matice A má nad tělesem reálných (racionálních, komplexních) čísel jediné vlastní číslo 2 násobnosti 3; spektrum matice A je $\{2, 2, 2\}$. Koefficienty charakteristického polynomu jsou:

$$\begin{aligned} c_0 &= +1, \\ c_1 &= -6 = -\operatorname{tr} A = -(2 + 2 + 2), \\ c_2 &= +12 = \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} + \begin{vmatrix} 3 & -1 \\ 1 & 1 \end{vmatrix} + \begin{vmatrix} 3 & 1 \\ 0 & 2 \end{vmatrix} = 2 \cdot 2 + 2 \cdot 2 + 2 \cdot 2, \\ c_3 &= -8 = -\det A = -2 \cdot 2 \cdot 2. \end{aligned}$$

Matice A je regulární, neboť je $c_3 \neq 0$.

(iii) Charakteristickou maticí reálné matice

$$A = \begin{pmatrix} -2 & -2 & -1 \\ 0 & -1 & 0 \\ 2 & -1 & 0 \end{pmatrix}$$

je λ -matice

$$\lambda E - A = \begin{pmatrix} \lambda + 2 & 2 & 1 \\ 0 & \lambda + 1 & 0 \\ -2 & 1 & \lambda \end{pmatrix}$$

a charakteristickým polynomem matice A je polynom

$$\det(\lambda E - A) = (\lambda + 1)(\lambda^2 + 2\lambda + 2) = \lambda^3 + 3\lambda^2 + 4\lambda + 2 .$$

Matice A má nad tělesem reálných (racionálních) čísel spektrum $\{-1\}$, nad tělesem komplexních čísel má spektrum $\{-1, -1+i, -1-i\}$. Koeficienty charakteristického polynomu jsou:

$$\begin{aligned} c_0 &= 1 , \\ c_1 &= 3 = -\operatorname{tr} A = -[-1 + (-1+i) + (-1-i)] , \\ c_2 &= 4 = \begin{vmatrix} -1 & 0 \\ -1 & 0 \end{vmatrix} + \begin{vmatrix} -2 & -1 \\ 2 & 0 \end{vmatrix} + \begin{vmatrix} -2 & -2 \\ 0 & -1 \end{vmatrix} = \\ &= (-1) \cdot (-1+i) + (-1) \cdot (-1-i) + (-1+i) \cdot (-1-i) , \\ c_3 &= 2 = -\det A = -(-1) \cdot (-1+i) \cdot (-1-i) . \end{aligned}$$

Matice A je regulární, neboť je $c_3 \neq 0$.

17.6. Věta. *Nechť A je čtvercová matice nad tělesem T . Charakteristický polynom matice A je roven součtinu všech invariantních polynomů její charakteristické matice $\lambda E - A$.*

Důkaz. V předchozím paragrafu jsme dokázali, že ekvivalentním λ -maticím řádu n přísluší též posloupnost normovaných největších společných dělitelů všech jejich subdeterminantů řádu $i = 1, 2, \dots, n$ (viz 16.11). Užijeme-li toto tvrzení pro n , dostáváme, že determinant λ -matice $\lambda E - A$ je roven determinantu kanonického tvaru této λ -matice, tj. součtinu všech invariantních polynomů λ -matice $\lambda E - A$. \square

17.7. Věta. *Charakteristický polynom horní (dolní) trojúhelníkové blokové matice je roven součtinu charakteristických polynomů všech jejích bloků na diagonále.*

Důkaz. Jestliže je matice A horní trojúhelníková bloková, je taková i její charakteristická matice. Charakteristický polynom matice A je pak podle věty 14.9 roven součtinu determinantů všech bloků na diagonále matice $\lambda E - A$, tj. součtinu charakteristických polynomů všech bloků stojících na diagonále matice A . \square

17.8. Definice. Nechť A je čtvercová matice nad tělesem T a

$$g(\lambda) = a_0\lambda^k + a_1\lambda^{k-1} + \cdots + a_{k-1}\lambda + a_k$$

nenulový polynom z oboru integrity $T[\lambda]$. *Hodnotou polynomu $g(\lambda)$ v matici A budeme rozumět matici*

$$g(A) = a_0A^k + a_1A^{k-1} + \cdots + a_{k-1}A + a_kE ;$$

budeme též hovořit o *dosazení matice A do polynomu $g(\lambda)$* . Jestliže $g(A) = O$, pak říkáme, že matice A je *kořenem polynomu $g(\lambda)$* a že $g(\lambda)$ je *anulujícím polynomem matice A* . Nulový polynom považujeme rovněž za anulující polynom matice A .

17.9. Věta. *Ke každé matici existuje nenulový anulující polynom.*

Důkaz. Nechť A je matice řádu n nad tělesem T . Matice A je prvkem vektorového prostoru $T^{n \times n}$, který má dimenzi n^2 . Matice

$$A^{n^2}, \quad A^{n^2-1}, \quad \dots, \quad A^2, \quad A, \quad E,$$

kterých je n^2+1 , jsou tedy lineárně závislé. Proto existují prvky $a_0, a_1, \dots, a_{n^2} \in T$, které nejsou všechny rovny nule, pro které je

$$a_0A^{n^2} + a_1A^{n^2-1} + \cdots + a_{n^2-2}A^2 + a_{n^2-1}A + a_{n^2}E = O .$$

Polynom

$$g(\lambda) = a_0\lambda^{n^2} + a_1\lambda^{n^2-1} + \cdots + a_{n^2-2}\lambda^2 + a_{n^2-1}\lambda + a_{n^2}$$

je tedy nenulovým anulujícím polynomem matice A . \square

S dosazováním matic do polynomů se pracuje snadno.

Jestliže je $g(\lambda) = r(\lambda) + s(\lambda)$, pak je $g(A) = r(A) + s(A)$.

Jestliže je $g(\lambda) = r(\lambda) \cdot s(\lambda)$, pak je $g(A) = r(A) \cdot s(A)$.

Odtud vyplývá, že množina I všech anulujících polynomů dané matice A je tzv. *ideálem* oboru integrity $T[\lambda]$, tj. součet dvou anulujících polynomů matice A je anulujícím polynomem matice A , opačný polynom k anulujícímu polynomu matice A je anulujícím polynomem matice A a součin anulujícího polynomu matice A s libovolným polynomem z $T[\lambda]$ je anulujícím polynomem matice A . Protože je $T[\lambda]$ *oborem integrity hlavních ideálů*, je ideál I generován jediným polynomem; takovýto polynom je vice, jen jediný z nich je však normovaný. Označme tento polynom $m(\lambda)$. Je tedy

$$I = m(\lambda) \cdot T[\lambda] = \{ m(\lambda) \cdot p(\lambda); p(\lambda) \in T[\lambda] \} .$$

Poznamenejme, že každý násobek polynomu $m(\lambda)$ prvkem $c \in T$, kde $c \neq 0$ a $c \neq 1$, také generuje ideál I ; polynom $c \cdot m(\lambda)$ však není normovaný.

Pokud se nebudeme odvolávat na znalosti z obecné algebry, můžeme všechny tyto skutečnosti snadno zjistit pomocí věty o dělení polynomů se zbytkem. V množině I všech anulujících polynomů matice A vezmeme polynom $m(\lambda)$ nejmenšího možného stupně, který je normovaný, a ukážeme, že ostatní polynomy z množiny I jsou jeho násobky. Nechť $a(\lambda) \in I$ a

$$a(\lambda) = m(\lambda) \cdot q(\lambda) + r(\lambda) ,$$

kde $r(\lambda) = 0$ nebo $\deg r(\lambda) < \deg m(\lambda)$. Potom je

$$a(A) = m(A) \cdot q(A) + r(A) ;$$

odtud $r(A) = O$, neboť $a(\lambda)$ i $m(\lambda)$ jsou anulující polynomy matice A . Polynom $r(\lambda)$ je tedy anulujícím polynomem matice A ; protože nemůže mít menší stupeň než polynom $m(\lambda)$, musí být nulový. Polynom $a(\lambda)$ je tedy násobkem polynomu $m(\lambda)$.

Na základě předchozích úvah můžeme vyslovit tuto definici.

17.10. Definice. Nechť A je čtvercová matice nad tělesem T . *Minimálním polynomem* matice A budeme rozumět anulující polynom matice A nejmenšího možného stupně, který je navíc normovaný.

Z předchozích úvah vyplývá, že každá čtvercová matice řádu n má právě jediný minimální polynom a že stupeň tohoto polynomu je nejvýše roven n^2 . Brzy uvidíme, že stupeň minimálního polynomu matice A nemůže být větší než její řád (viz 17.12(ii)).

17.11. Věta. *Nechť A je čtvercová matice nad tělesem T . Minimální polynom matice A je roven poslednímu invariantnímu polynomu její charakteristické matice $\lambda E - A$.*

Důkaz. Předpokládejme, že matice A má řád n . Označme $d_{n-1}(\lambda)$ normovaný největší společný dělitel všech subdeterminantů řádu $n - 1$ charakteristické matice $\lambda E - A$ matice A a $e_n(\lambda)$ poslední, tj. n -tý invariantní polynom této λ -matice. Podle definice 16.9 je

$$e_n(\lambda) = \frac{\det(\lambda E - A)}{d_{n-1}(\lambda)} ,$$

tj.

$$\det(\lambda E - A) = e_n(\lambda) \cdot d_{n-1}(\lambda) . \tag{1}$$

Adjungovaná matice $(\lambda E - A)_{\text{rec}}$ k matici $\lambda E - A$ je sestavena právě ze všech subdeterminantů řádu $n - 1$ matice $\lambda E - A$ (s příslušnými znaménky). Vytknutí

největšího společného dělitele $d_{n-1}(\lambda)$ prvků matice $(\lambda E - A)_{\text{rec}}$ zachytíme v rovnosti

$$(\lambda E - A)_{\text{rec}} = d_{n-1}(\lambda) \cdot C(\lambda) ; \quad (2)$$

největší společný dělitel všech prvků λ -matice $C(\lambda)$ je tedy 1. Podle věty 14.17 je

$$(\lambda E - A) \cdot (\lambda E - A)_{\text{rec}} = \det(\lambda E - A) \cdot E . \quad (3)$$

Dosazením (1) a (2) do (3) dostaneme rovnost

$$(\lambda E - A) \cdot d_{n-1}(\lambda) \cdot C(\lambda) = e_n(\lambda) \cdot d_{n-1}(\lambda) \cdot E .$$

Po zkrácení nenulovým polynomem $d_{n-1}(\lambda)$ vychází

$$(\lambda E - A) \cdot C(\lambda) = e_n(\lambda) \cdot E . \quad (4)$$

Pišme

$$e_n(\lambda) = a_0 \lambda^k + a_1 \lambda^{k-1} + \dots + a_k ;$$

je tedy

$$e_n(\lambda) \cdot E = a_0 E \lambda^k + a_1 E \lambda^{k-1} + \dots + a_k E . \quad (5)$$

Polynomiální matice $e_n(\lambda) \cdot E$, která je vyjádřena maticovým polynomem (5), je podle (4) beze zbytku dělitelná zleva λ -maticí $\lambda E - A$. Podle lemmatu 16.22(i) však zbytek O při tomto dělení dostaneme dosazením matice A za neurčitou λ do maticového polynomu $e_n(\lambda)$ zapsaného v (5). Tedy

$$a_0 A^k + a_1 A^{k-1} + \dots + a_k E = O ,$$

tj. $e_n(A) = O$, neboli $e_n(\lambda)$ je anulujícím polynomem matice A .

Označme $m(\lambda)$ minimální polynom matice A ; polynom $e_n(\lambda)$ musí být násobkem polynomu $m(\lambda)$, tj.

$$e_n(\lambda) = m(\lambda) \cdot q(\lambda) , \quad (6)$$

kde polynom $q(\lambda)$ je normovaný, neboť $e_n(\lambda)$ i $m(\lambda)$ jsou normované.

Podle věty 16.21 existuje λ -matice $Q(\lambda)$ a matice R , pro které

$$m(\lambda) \cdot E = (\lambda E - A) \cdot Q(\lambda) + R . \quad (7)$$

Podle lemmatu 16.22(i) však zbytek R získáme dosazením matice A do maticového polynomu $m(\lambda) \cdot E$. Jestliže je

$$m(\lambda) = b_0 \lambda^s + b_1 \lambda^{s-1} + \dots + b_s ,$$

je

$$m(\lambda) \cdot E = b_0 E \lambda^s + b_1 E \lambda^{s-1} + \dots + b_s E$$

a tedy

$$R = b_0 A^s + b_1 A^{s-1} + \dots + b_s E = m(A) = O ,$$

neboť $m(\lambda)$ je minimální polynom matice A .

Z rovnosti (7) tedy plyne rovnost

$$m(\lambda) \cdot E = (\lambda E - A) \cdot Q(\lambda) . \quad (8)$$

Z rovností (4), (6) a (8) vyplývá:

$$(\lambda E - A) \cdot C(\lambda) = m(\lambda) \cdot q(\lambda) \cdot E = (\lambda E - A) \cdot q(\lambda) \cdot Q(\lambda) .$$

Po zkrácení λ -maticí $\lambda E - A$ zleva (využíváme vlastně větu 16.21 — jednoznačnost dělení maticových polynomů) dostáváme rovnost

$$C(\lambda) = q(\lambda) \cdot Q(\lambda) .$$

Protože je však největší společný dělitel prvků λ -matice $C(\lambda)$ roven 1 a protože je polynom $q(\lambda)$ normovaný, je $q(\lambda) = 1$; z rovnosti (6) tedy vyplývá, že minimální polynom $m(\lambda)$ matice A je roven poslednímu invariantnímu polynomu $e_n(\lambda)$ charakteristické matice $\lambda E - A$. \square

Zjistili jsme tedy, že minimální polynom dané matice A je roven *poslednímu* invariantnímu polynomu a že charakteristický polynom matice A je roven *součinu všech* invariantních polynomů její charakteristické matice $\lambda E - A$ (viz 17.6). Z těchto dvou důležitých výsledků vyplývají následující zjištění.

17.12. Důsledky.

- (i) *Charakteristický polynom každé matice je násobkem jejího minimálního polynomu.*
- (ii) *Stupeň minimálního polynomu každé matice je nejvýše roven jejímu řádu.*
- (iii) *Každý ireducibilní polynom, který dělí charakteristický polynom dané matice, dělí i její minimální polynom.*
- (iv) *Charakteristický i minimální polynom dané matice mají v uvažovaném tělese stejné kořeny; jejich násobnosti (jako kořenů charakteristického, resp. minimálního polynomu) však mohou být různé.*

Důkaz. Nechť A je čtvercová matice nad tělesem T a $e_1(\lambda), \dots, e_n(\lambda)$ invariantní polynomy její charakteristické matice $\lambda E - A$. Všechna čtyři tvrzení vyplývají z toho, že charakteristický polynom matice A je $e_1(\lambda)e_2(\lambda)\dots e_n(\lambda)$ a její minimální polynom je $e_n(\lambda)$. U tvrzení (iii) a (iv) je třeba ještě využít faktu, že polynomy $e_1(\lambda), \dots, e_n(\lambda)$ se navzájem dělí (viz 16.6 a 16.12). \square

Modifikací důsledku 17.12(i) je následující velmi známé tvrzení; uvádíme ho ve dvou ekvivalentních vyjádřeních.

17.13. Cayleyova–Hamiltonova věta.

- (i) *Charakteristický polynom každé matice je jejím anulujícím polynomem.*
 (ii) *Každá matice je kořenem svého charakteristického polynomu.* \square

Charakteristický polynom dané matice A vypočteme jako determinant její charakteristické matice. Minimální polynom matice A můžeme někdy hledat pomocí převedení charakteristické matice $\lambda E - A$ na kanonický tvar (jako její poslední invariantní polynom). Zpravidla je však výhodnější — alespoň u matic malých řádů — najít charakteristický polynom a využít tvrzení 17.12(iii).

17.14. Příklady.

(i) Minimální polynom matice A z příkladu 17.2(i), resp. 17.5(i) je podle tvrzení 17.12(iii) roven jejímu charakteristickému polynomu. Rovněž minimální polynom matice A z příkladu 17.5(iii) je roven jejímu charakteristickému polynomu.

(ii) Charakteristický polynom matice A z příkladu 17.5(ii) je $(\lambda - 2)^3$. Podle důsledku 17.12(i) jsou pro minimální polynom tyto možnosti: $\lambda - 2$, $(\lambda - 2)^2$, $(\lambda - 2)^3$. Polynom $\lambda - 2$ však zřejmě není anulujícím polynomem matice A . Dosadíme matici A do polynomu $(\lambda - 2)^2$:

$$(A - 2E)^2 = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & -1 \end{pmatrix}^2 = O$$

Minimálním polynomem matice A je tedy polynom $(\lambda - 2)^2$.

(iii) Charakteristický polynom reálné matice

$$B = \begin{pmatrix} 1 & 2 & -2 \\ -1 & 0 & 2 \\ -2 & 2 & 1 \end{pmatrix}$$

je

$$\begin{aligned} \det(\lambda E - B) &= \begin{vmatrix} \lambda - 1 & -2 & 2 \\ 1 & \lambda & -2 \\ 2 & -2 & \lambda - 1 \end{vmatrix} = \lambda^3 - 2\lambda^2 - 5\lambda + 6 = \\ &= (\lambda - 1)(\lambda + 2)(\lambda - 3). \end{aligned}$$

Spektrum matice B je $\{1, -2, 3\}$; nezávisí na tom, zda matici uvažujeme nad tělesem racionálních, reálných nebo komplexních čísel. Dále je $\operatorname{tr} B = 2$, $\det B = -6$. Minimální polynom je roven charakteristickému (viz 17.12(iii), resp. (iv)).

(iv) Charakteristický polynom matice

$$C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

nad tělesem \mathbb{Z}_5 je

$$\det(\lambda E - C) = \begin{vmatrix} \lambda + 4 & 3 & 2 & 1 \\ 0 & \lambda + 4 & 1 & 0 \\ 0 & 0 & \lambda + 4 & 0 \\ 0 & 4 & 3 & \lambda + 4 \end{vmatrix} = (\lambda + 4)^4.$$

Matice C má vlastní číslo 1 násobnosti 4, spektrum matice C je $\{1, 1, 1, 1\}$. Snadno ověříme, že matice $C + 4E$, $(C + 4E)^2$, $(C + 4E)^3$ jsou nenulové, takže minimální polynom je roven charakteristickému.

17.15. Věta. *Minimální polynom diagonální blokové matice je roven nejmenšímu společnému násobku minimálních polynomů všech jejích bloků na diagonále.*

Důkaz. Nechť A je diagonální bloková matice s bloky A_1, A_2, \dots, A_s na diagonále. Snadno se uváží, že k -tá mocnina matice A ($k = 1, 2, \dots$) je diagonální bloková matice s bloky $A_1^k, A_2^k, \dots, A_s^k$ na diagonále. Odtud vyplývá, že je-li $f(\lambda)$ polynom, pak $f(A)$ je diagonální bloková matice s bloky $f(A_1), f(A_2), \dots, f(A_s)$ na diagonále. Minimální polynom $m(\lambda)$ matice A je tedy normovaný polynom nejmenšího možného stupně, pro který je $m(A_1) = O$, $m(A_2) = O$, \dots , $m(A_s) = O$, tj. $m(\lambda)$ je nejmenší společný násobek minimálních polynomů matic A_1, A_2, \dots, A_s . \square

17.16. Příklady.

(i) Minimální polynom diagonální matice $A = (a_{ij})$ řádu n má podle věty 17.15 tvar

$$(\lambda - b_1)(\lambda - b_2) \dots (\lambda - b_k),$$

kde prvky b_1, \dots, b_k jsou navzájem různé a pro každé $i = 1, \dots, n$ je

$$a_{ii} \in \{b_1, \dots, b_k\}.$$

Např. minimální polynom reálné diagonální matice desátého řádu, která má na diagonále po řadě prvky 1, 1, 2, 3, 1, 3, 2, 4, 2, 1, je roven $(\lambda - 1)(\lambda - 2)(\lambda - 3)(\lambda - 4)$.

(ii) Minimální polynom reálné matice

$$A = \begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

je nejmenším společným násobkem minimálních polynomů matic

$$\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix},$$

tj. polynomů $(\lambda - 1)(\lambda - 2)$ a $(\lambda - 2)^2$. Minimálním polynomem matice A je tedy polynom $(\lambda - 1)(\lambda - 2)^2$.

Nechť A je čtvercová matice řádu n nad tělesem T . Prvek $a \in T$ je vlastním číslem matice A (tj. a je kořenem charakteristického polynomu $\det(\lambda E - A)$ matice A) právě tehdy, když $\det(aE - A) = 0$, tj. když je matice $aE - A$ singulární. To však nastane právě tehdy, když homogenní soustava lineárních rovnic s maticí $aE - A$ má netriviální řešení, tj. existuje nenulový vektor $x \in T^n$, pro který

$$(aE - A) \cdot x^T = 0, \quad \text{neboli} \quad A \cdot x^T = a \cdot x^T.$$

17.17. Definice. Nechť A je čtvercová matice řádu n nad tělesem T a $a \in T$ její vlastní číslo. *Vlastním vektorem* matice A , který přísluší vlastnímu číslu a , budeme rozumět každý nenulový vektor $x \in T^n$, pro který $A \cdot x^T = a \cdot x^T$.

Jestliže $a \in T$ není vlastní číslo matice A , potom rovnost $A \cdot x^T = a \cdot x^T$ platí jen pro $x = 0$; tento fakt jsme ukázali již před definicí 17.17.

Všechny vlastní vektory příslušející témuž vlastnímu číslu $a \in T$ matice A spolu s nulovým vektorem tvoří podprostor prostoru T^n ; jde o podprostor všech řešení homogenní soustavy lineárních rovnic s maticí $aE - A$.

O vlastních číslech a vlastních vektorech je možno dokázat řadu zajímavých tvrzení.

17.18. Věta. *Nechť A, B jsou čtvercové matice téhož řádu nad tělesem T .*

- (i) *Jestliže a je vlastní číslo matice A a x příslušný vlastní vektor, potom pro každé přirozené číslo k je a^k vlastní číslo matice A^k a x je příslušný vlastní vektor.*
- (ii) *Nechť A je regulární matice. Číslo $a \in T$ je vlastním číslem matice A právě tehdy, když je číslo a^{-1} vlastním číslem matice A^{-1} . Vektor x je vlastním vektorem matice A příslušným k vlastnímu číslu a právě tehdy, když je vlastním vektorem matice A^{-1} příslušným k vlastnímu číslu a^{-1} .*
- (iii) *Matice AB a BA mají stejná vlastní čísla.*

Důkaz. (i) Jestliže je

$$A \cdot x^T = a \cdot x^T,$$

potom je zřejmé

$$A^2 \cdot x^T = A \cdot a \cdot x^T = a \cdot A \cdot x^T = a^2 \cdot x^T$$

a tedy i

$$A^k \cdot x^T = a^k \cdot x^T ,$$

jak se snadno dokáže indukcí.

(ii) Rovnost

$$A \cdot x^T = a \cdot x^T$$

platí právě tehdy, když

$$a^{-1} \cdot x^T = A^{-1} \cdot x^T .$$

(iii) Jestliže a je vlastní číslo matice AB a x příslušný vlastní vektor, tj.

$$AB \cdot x^T = a \cdot x^T ,$$

potom je

$$B \cdot AB \cdot x^T = B \cdot a \cdot x^T ,$$

neboli

$$BA \cdot B \cdot x^T = a \cdot B \cdot x^T ;$$

tedy a je vlastním číslem matice BA ; vektor y určený vztahem $y^T = B \cdot x^T$ je příslušným vlastním vektorem. (Pokud je $y^T = B \cdot x^T = 0$, není y vlastním vektorem. Potom je však matice B singulární, ze vztahu $AB \cdot x^T = a \cdot x^T$ vyplývá $a = 0$, a to je vlastní číslo singulární matice BA .) \square

17.19. Příklad. Reálná matice

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 2 & 4 \end{pmatrix}$$

má charakteristický polynom

$$\det(\lambda E - A) = (\lambda - 2)^2(\lambda - 3) = \lambda^3 - 7\lambda^2 + 16\lambda - 12 .$$

Vlastní vektory příslušné k vlastnímu číslu 2, resp. 3 jsou všechna nenulová řešení homogenní soustavy lineárních rovnic s maticí

$$2E - A = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & 1 \\ 0 & -2 & -2 \end{pmatrix} , \quad \text{resp.} \quad 3E - A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 2 & 1 \\ 0 & -2 & -1 \end{pmatrix} ,$$

tj. všechny nenulové vektory podprostoru

$$[(1, 0, 0)] , \quad \text{resp.} \quad [(1, 1, -2)] .$$

Minimální polynom matice A je roven jejímu charakteristickému polynomu. Matice

$$A^3 = \begin{pmatrix} 8 & 5 & -7 \\ 0 & -11 & -19 \\ 0 & 38 & 46 \end{pmatrix}$$

má charakteristický polynom $\det(\lambda E - A^3) = (\lambda - 8)^2(\lambda - 27)$. Vlastní vektory příslušné k vlastnímu číslu 8, resp. 27 jsou všechny nenulové vektory podprostoru

$$[(1, 0, 0)] , \quad \text{resp.} \quad [(1, 1, -2)] .$$

Inverzní maticí k matici A je matice

$$A^{-1} = \frac{1}{12} \begin{pmatrix} 6 & -4 & -1 \\ 0 & 8 & 2 \\ 0 & -4 & 2 \end{pmatrix} .$$

Její vlastní čísla jsou $\frac{1}{2}$ a $\frac{1}{3}$, příslušné vlastní vektory jsou všechny nenulové vektory podprostorů

$$[(1, 0, 0)] , \quad \text{resp.} \quad [(1, 1, -2)] .$$

Pro matici A je

$$A^3 - 7A^2 + 16A - 12E = O , \quad \text{neboli} \quad A^3 = 7A^2 - 16A + 12E .$$

Z tohoto vztahu lze postupně získat vyjádření dalších mocnin matice A , např.

$$A^4 = 7A^3 - 16A^2 + 12A = 33A^2 - 100A + 84E ,$$

nebo (po vynásobení maticí A^{-1}) rovnost

$$A^{-1} = \frac{1}{12}(A^2 - 7A + 16E) ,$$

odtud

$$A^{-2} = \frac{1}{12}(A - 7E + 16A^{-1}) = \frac{1}{144}(16A^2 - 100A + 172E) .$$

Každá mocnina matice A je tedy lineární kombinací matic A^2 , A , E .

Velmi důležitý výsledek o vlastních číslech je zformulován v následující větě.

17.20. Věta. *Všechna vlastní čísla hermitovské (reálné symetrické) matice jsou reálná.*

Důkaz. Vzhledem k tomu, že každá reálná symetrická matice je hermitovská, stačí tvrzení dokázat pro hermitovské matice.

Nechť A je hermitovská matice řádu n , tj. $\overline{A}^T = A$, nechť $a \in \mathbb{C}$ je vlastní číslo matice A a $x = (x_1, \dots, x_n) \in \mathbb{C}^n$ příslušný vlastní vektor. Je tedy

$$A \cdot x^T = a \cdot x^T$$

a odtud

$$\overline{x} \cdot A \cdot x^T = \overline{x} \cdot a \cdot x^T = a \cdot (|x_1|^2 + \dots + |x_n|^2). \quad (9)$$

Transponujeme-li a komplexně sdružíme obě strany této rovnosti, dostaneme rovnost

$$\overline{\overline{x} \cdot A \cdot x^T} = \overline{a \cdot (|x_1|^2 + \dots + |x_n|^2)^T},$$

tj.

$$\overline{x} \cdot A \cdot x^T = \overline{a} \cdot (|x_1|^2 + \dots + |x_n|^2), \quad (10)$$

neboť matice A je hermitovská a $|x_1|^2 + \dots + |x_n|^2$ je reálné číslo. Ze vztahů (9) a (10) vyplývá rovnost

$$a \cdot (|x_1|^2 + \dots + |x_n|^2) = \overline{a} \cdot (|x_1|^2 + \dots + |x_n|^2), \quad \text{tj.} \quad a = \overline{a},$$

ze které plyne, že a je reálné číslo. \square

17.21. Příklady.

(i) Uvažujme hermitovskou matici

$$A = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}.$$

Charakteristickým polynomem matice A je polynom

$$\det(\lambda E - A) = \lambda^2 - 1 = (\lambda - 1)(\lambda + 1).$$

Vlastní vektory příslušné k vlastnímu číslu 1, resp. -1 získáme řešením homogenní soustavy lineárních rovnic s maticí

$$E - A = \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}, \quad \text{resp.} \quad -E - A = \begin{pmatrix} -1 & -i \\ i & -1 \end{pmatrix}.$$

Vlastními vektory matice A , které přísluší vlastnímu číslu 1, resp. -1 jsou všechny nenulové vektory podprostoru

$$[(i, 1)], \quad \text{resp.} \quad [(-i, 1)].$$

(ii) Reálná symetrická matice

$$B = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$$

má charakteristický polynom

$$\det(\lambda E - B) = \lambda^2 - 4\lambda - 1,$$

vlastní čísla $2 + \sqrt{5}$ a $2 - \sqrt{5}$; příslušné vlastní vektory jsou všechna nenulová řešení homogenní soustavy lineárních rovnic s maticí

$$\begin{pmatrix} 1 + \sqrt{5} & -2 \\ -2 & -1 + \sqrt{5} \end{pmatrix}, \quad \text{resp.} \quad \begin{pmatrix} 1 - \sqrt{5} & -2 \\ -2 & -1 - \sqrt{5} \end{pmatrix},$$

neboli všechny nenulové vektory podprostorů

$$[(2, 1 + \sqrt{5})], \quad \text{resp.} \quad [(2, 1 - \sqrt{5})].$$

17.22. Věta. *Nechť A je matice řádu n nad tělesem T . Jsou-li X_1, \dots, X_k lineárně nezávislé množiny vlastních vektorů příslušných po řadě k navzájem různým vlastním číslům a_1, \dots, a_k matice A , je množina $X = X_1 \cup \dots \cup X_k$ lineárně nezávislá.*

Důkaz. V úvodu důkazu poznamenejme, že každou lineární kombinaci vektorů množiny X můžeme vyjádřit jako součet $x_1 + \dots + x_k$, kde pro každé $i = 1, \dots, k$ je $x_i \in [X_i]$. Přitom je buď x_i vlastní vektor příslušný k vlastnímu číslu a_i , nebo je $x_i = o$ (všechny vlastní vektory příslušné k těmto vlastním číslům tvoří totiž spolu s nulovým vektorem podprostor prostoru T^n).

Stačí tedy dokázat, že vlastní vektory x_1, \dots, x_k příslušné k navzájem různým vlastním číslům a_1, \dots, a_k jsou lineárně nezávislé. Důkaz provedeme indukcí podle k .

Pro $k = 1$ není co dokazovat. Předpokládejme, že tvrzení platí pro $k - 1$ a že

$$c_1 x_1 + \dots + c_k x_k = o, \tag{11}$$

kde x_1, \dots, x_k jsou vlastní vektory příslušné k navzájem různým vlastním číslům a_1, \dots, a_k . Nyní je

$$A \cdot (c_1 x_1 + \dots + c_k x_k)^T = o^T$$

a odtud

$$c_1 a_1 x_1 + \dots + c_k a_k x_k = o.$$

Ze vztahu (11) však dostáváme rovnost

$$c_1 a_k x_1 + \dots + c_k a_k x_k = o.$$

Z předchozích dvou rovností vyplývá vztah

$$c_1 (a_1 - a_k) x_1 + \dots + c_{k-1} (a_{k-1} - a_k) x_{k-1} = o.$$

Podle indukčního předpokladu jsou vektory x_1, \dots, x_{k-1} lineárně nezávislé; protože jsou vlastní čísla a_1, \dots, a_k navzájem různá, je nutně $c_1 = \dots = c_{k-1} = 0$ a tedy i $c_k = 0$. Vektory x_1, \dots, x_k jsou tedy lineárně nezávislé. \square

18. PODOBNOST, JORDANŮV KANONICKÝ TVAR

18.1. Definice. Nechtě A, B jsou čtvercové matice téhož řádu nad tělesem T . Budeme říkat, že matice A, B jsou *podobné*, jestliže existuje regulární matice C nad tělesem T , taková, že

$$A = C^{-1}BC .$$

Poznamenejme, že je lhostejné, zda v definici 18.1 píšeme inverzní matici vpravo nebo vlevo; matice A vznikne vynásobením matice B zleva a zprava navzájem inverzními maticemi.

Snadno se ověří, že relace podobnosti je *ekvivalence*, je totiž reflexivní, symetrická a tranzitivní. Množina $T^{n \times n}$ všech čtvercových matic řádu n nad tělesem T se tedy rozpadne na disjunktní třídy navzájem podobných matic. Třídy obsahující jednotkovou matici, resp. nulovou matici, resp. jakoukoli skalární matici jsou zřejmě jednoprvkové. Podobnost matic prvního řádu přejde v „obyčejnou rovnost“ matic (násobení matic prvního řádu je komutativní, proto je rovnost $A = C^{-1}BC$ ekvivalentní s rovností $A = B$); všechny třídy podobnosti v $T^{1 \times 1}$ jsou tedy jednoprvkové.

Podle věty 11.11 se můžeme na podobné matice z $T^{n \times n}$ dívat jako na matice téhož endomorfismu nějakého n -rozměrného vektorového prostoru (např. T^n) vytvořené vzhledem k různým bázím.

Podobně jako v 16. paragrafu o polynomiálních maticích se budeme snažit nalézt v každé třídě navzájem podobných matic jakousi matici, která by celou tuto třídu reprezentovala a přitom měla poměrně jednoduchou strukturu. Nejprve však dokážeme nutnou a postačující podmínku pro podobnost matic; již toto kritérium ukáže význam předchozí partie o polynomiálních maticích.

18.2. Kritérium podobnosti matic. *Matice A a B jsou podobné právě tehdy, když jsou jejich charakteristické matice $\lambda E - A$ a $\lambda E - B$ ekvivalentní.*

Důkaz. Jsou-li matice A a B podobné, existuje regulární matice C , taková, že $A = C^{-1}BC$. Je tedy

$$C^{-1} \cdot (\lambda E - B) \cdot C = \lambda C^{-1}EC - C^{-1}BC = \lambda E - A .$$

Podle věty 12.21 je každá regulární matice součinem elementárních transformačních matic; charakteristické matice $\lambda E - A$ a $\lambda E - B$ jsou tedy ekvivalentní.

Předpokládejme naopak, že λ -matice $\lambda E - A$ a $\lambda E - B$ jsou ekvivalentní. Je tedy

$$\lambda E - A = X(\lambda) \cdot (\lambda E - B) \cdot Y(\lambda) , \quad (1)$$

kde $X(\lambda)$ a $Y(\lambda)$ jsou součiny elementárních transformačních λ -matic. Podle věty 16.21 o dělení polynomiálních matic existují λ -matice $Q_1(\lambda)$ a $Q_2(\lambda)$ a matice R_1 a R_2 takové, že platí:

$$X(\lambda) = (\lambda E - A) \cdot Q_1(\lambda) + R_1 , \quad (2)$$

$$Y(\lambda) = Q_2(\lambda) \cdot (\lambda E - A) + R_2 .$$

V následujícím postupu ukážeme, že vztah (1) bude platit i tehdy, nahradíme-li v něm λ -matice $X(\lambda)$ a $Y(\lambda)$ maticemi R_1 a R_2 , tj. *zbytky při dělení* λ -matic $X(\lambda)$ a $Y(\lambda)$ charakteristickou maticí $\lambda E - A$ zleva a zprava.

Budeme tedy počítat součin $R_1(\lambda E - B)R_2$; ze vztahů (2) dosadíme za R_1 a R_2 a získaný součin roznásobíme:

$$\begin{aligned} R_1 \cdot (\lambda E - B) \cdot R_2 &= \\ &= [X(\lambda) - (\lambda E - A) \cdot Q_1(\lambda)] \cdot (\lambda E - B) \cdot [Y(\lambda) - Q_2(\lambda) \cdot (\lambda E - A)] = \\ &= X(\lambda) \cdot (\lambda E - B) \cdot Y(\lambda) - X(\lambda) \cdot (\lambda E - B) \cdot Q_2(\lambda) \cdot (\lambda E - A) - \\ &\quad - (\lambda E - A) \cdot Q_1(\lambda) \cdot (\lambda E - B) \cdot Y(\lambda) + \\ &\quad + (\lambda E - A) \cdot Q_1(\lambda) \cdot (\lambda E - B) \cdot Q_2(\lambda) \cdot (\lambda E - A) \end{aligned}$$

V další úpravě užijeme třikrát rovnost (1); přihlédneme též k tomu, že λ -matice $X(\lambda)$ a $Y(\lambda)$ jsou invertibilní (neboť jsou to součiny elementárních transformačních λ -matic):

$$\begin{aligned} R_1 \cdot (\lambda E - B) \cdot R_2 &= (\lambda E - A) - (\lambda E - A) \cdot Y(\lambda)^{-1} \cdot Q_2(\lambda) \cdot (\lambda E - A) - \\ &\quad - (\lambda E - A) \cdot Q_1(\lambda) \cdot X(\lambda)^{-1} \cdot (\lambda E - A) + \\ &\quad + (\lambda E - A) \cdot Q_1(\lambda) \cdot (\lambda E - B) \cdot Q_2(\lambda) \cdot (\lambda E - A) \end{aligned}$$

Po dvojnásobím vytknutí docházíme k rovnosti

$$R_1 \cdot (\lambda E - B) \cdot R_2 = (\lambda E - A) \cdot [E - C(\lambda) \cdot (\lambda E - A)] , \quad (3)$$

kde

$$C(\lambda) = Y(\lambda)^{-1} \cdot Q_2(\lambda) - Q_1(\lambda) \cdot X(\lambda)^{-1} + Q_1(\lambda) \cdot (\lambda E - B) \cdot Q_2(\lambda) .$$

Stupeň λ -matice $R_1(\lambda E - B)R_2$ stojící v rovnosti (3) vlevo je nejvýše 1. Kdyby byla λ -matice $C(\lambda)$ nenulová, měla by λ -matice stojící v rovnosti (3) vpravo stupeň alespoň 2. Matice $C(\lambda)$ tedy musí být nulová. Z tohoto zjištění a z rovnosti (3) nyní vyplývá rovnost

$$R_1 \cdot (\lambda E - B) \cdot R_2 = \lambda E - A ,$$

ktehou jsme chtěli dokázat. Porovnáním koeficientů maticových polynomů na levé a pravé straně této rovnosti dostáváme tyto vztahy:

$$\begin{aligned} R_1 R_2 &= E && \text{neboli} && R_1 &= R_2^{-1} , \\ R_1 B R_2 &= A && \text{neboli} && A &= R_2^{-1} B R_2 . \end{aligned}$$

Matice A a B jsou tedy podobné. \square

18.3. Metody zjištění podobnosti matic.

Předchozí výsledek dává jasný návod ke zjištění podobnosti matic. Máme-li zjistit, zda jsou matice A a B podobné, najdeme kanonické tvary jejich charakteristických matic a porovnáme je. Jsou-li stejné, pak jsou matice A a B podobné, nejsou-li stejné, pak matice A a B podobné nejsou.

Předpokládejme však, že je naším úkolem zjistit, zda jsou matice A, B řádu n podobné a v kladném případě najít nějakou regulární matici C , pomocí které se podobnost realizuje. Nyní ukážeme dvě možnosti řešení tohoto problému.

(i) Rovnost $A = C^{-1}BC$ je ekvivalentní s rovností $CA = BC$, pokud C je regulární matice. Chápejme prvky matice C jako neznámé. Maticová rovnost $CA = BC$ přejde po provedeném násobení v soustavu n^2 lineárních rovnic o n^2 neznámých. Při řešení této soustavy musíme mít na paměti, že hledaná matice C musí být regulární; nemusíme však najít všechna řešení, tj. všechny regulární matice C , pro které platí rovnost $CA = BC$, stačí najít řešení jediné.

(ii) Charakteristické matice $\lambda E - A$ a $\lambda E - B$ převedeme řádkovými a sloupcovými elementárními úpravami na kanonické tvary $K_1(\lambda)$ a $K_2(\lambda)$ a zachytíme provedené řádkové úpravy:

$$(\lambda E - A | E) \rightsquigarrow (K_1(\lambda) | X_1(\lambda)) ,$$

$$(\lambda E - B | E) \rightsquigarrow (K_2(\lambda) | X_2(\lambda)) ,$$

tj.

$$X_1(\lambda) \cdot (\lambda E - A) \cdot Y_1(\lambda) = K_1(\lambda) ,$$

$$X_2(\lambda) \cdot (\lambda E - B) \cdot Y_2(\lambda) = K_2(\lambda) .$$

Je-li $K_1(\lambda) = K_2(\lambda)$, jsou matice A a B podobné a můžeme hledat regulární matici C , pro kterou $A = C^{-1}BC$. Z rovností (4) vyplývá rovnost

$$\lambda E - A = X_1(\lambda)^{-1} \cdot X_2(\lambda) \cdot (\lambda E - B) \cdot Y_2(\lambda) \cdot Y_1(\lambda)^{-1} .$$

Polynomiální matici $X_1(\lambda)^{-1}X_2(\lambda)$ najdeme, když přejdeme řádkovými elementárními úpravami od matice

$$(X_1(\lambda) | X_2(\lambda)) \quad \text{k matici} \quad (E | X_1(\lambda)^{-1}X_2(\lambda)) .$$

Podle důkazu věty 18.2 víme, že matice C^{-1} je zbytkem při dělení λ -matice $X_1(\lambda)^{-1}X_2(\lambda)$ λ -maticí $\lambda E - A$ zleva:

$$X_1(\lambda)^{-1} \cdot X_2(\lambda) = (\lambda E - A) \cdot Q(\lambda) + C^{-1}$$

Podle lemmatu 16.22 získáme matici C^{-1} dosazením matice A do maticového polynomu $X_1(\lambda)^{-1}X_2(\lambda)$ za neurčitou λ , a to zleva.

Další možnosti postupu při hledání transformační matice poznáme později.

Z kritéria podobnosti 18.2 a vět 16.14 a 16.18 ihned vyplývá následující důsledek.

18.4. Důsledek. *Pro čtvercové matice A, B téhož řádu nad tělesem T jsou následující tvrzení ekvivalentní.*

- (i) *Matice A, B jsou podobné.*
- (ii) *Charakteristické matice $\lambda E - A$ a $\lambda E - B$ mají stejnou posloupnost invariantních polynomů.*
- (iii) *Charakteristické matice $\lambda E - A$ a $\lambda E - B$ mají stejný soubor elementárních polynomů. \square*

Ještě než uvedeme příklady podobných matic, zformulujeme další jednoduchý důsledek věty 18.2.

18.5. Důsledek. *Podobné matice mají stejnou hodnotu, charakteristický a minimální polynom, stopu, determinant i spektrum.*

Důkaz. Předpokládejme, že matice A a B jsou podobné. Podle důsledku 18.4 mají jejich charakteristické matice $\lambda E - A$ a $\lambda E - B$ stejné invariantní polynomy. Matice A a B mají tedy podle vět 17.6 a 17.11 stejný charakteristický a minimální polynom. Mají proto i stejné spektrum a podle 17.3 i stopu a determinant. Vzhledem k 12.6 a definici podobnosti mají matice A a B i stejnou hodnotu. \square

Později uvidíme, že rovnost charakteristických a minimálních polynomů dvou matic není postačující podmínkou pro jejich podobnost (viz 18.13(ii)).

18.6. Příklad. Zjistíme, zda reálné matice

$$A = \begin{pmatrix} -2 & 1 \\ 0 & 3 \end{pmatrix} \quad \text{a} \quad B = \begin{pmatrix} -10 & -4 \\ 26 & 11 \end{pmatrix}$$

jsou podobné.

Charakteristické polynomy matic A a B jsou

$$\begin{vmatrix} \lambda + 2 & -1 \\ 0 & \lambda - 3 \end{vmatrix} = (\lambda + 2)(\lambda - 3),$$

$$\begin{vmatrix} \lambda + 10 & 4 \\ -26 & \lambda - 11 \end{vmatrix} = (\lambda + 10)(\lambda - 11) + 104 = (\lambda + 2)(\lambda - 3).$$

Obě λ -matice $\lambda E - A$ a $\lambda E - B$ mají tedy stejné invariantní polynomy

$$e_1(\lambda) = 1, \quad e_2(\lambda) = (\lambda + 2)(\lambda - 3).$$

Matice A a B jsou proto podobné; existuje regulární matice C , pro kterou je $A = C^{-1}BC$. Pišme

$$C = \begin{pmatrix} x & y \\ z & t \end{pmatrix} .$$

Ze vztahu $CA = BC$ dostáváme soustavu čtyř rovnic o čtyřech neznámých:

$$\begin{aligned} -2x &= -10x - 4z , \\ x + 3y &= -10y - 4t , \\ -2z &= 26x + 11z , \\ z + 3t &= 26y + 11t . \end{aligned}$$

Po jednoduchých úpravách se tato soustava redukuje na soustavu dvou rovnic:

$$\begin{aligned} x + 13y + 4t &= 0 , \\ 2x + z &= 0 . \end{aligned}$$

Čísla x, y, z, t musíme navíc nalézt tak, aby hledaná matice C byla regulární. Volba $x = -1, y = 1, z = 2, t = -3$ vyhovuje požadavkům. Pro matici

$$C = \begin{pmatrix} -1 & 1 \\ 2 & -3 \end{pmatrix} \quad \text{a} \quad C^{-1} = \begin{pmatrix} -3 & -1 \\ -2 & -1 \end{pmatrix}$$

je tedy $A = C^{-1}BC$, jak se snadno prověří.

Vyřešme zadaný příklad jiným způsobem. Charakteristické matice $\lambda E - A$ a $\lambda E - B$ převedeme na kanonický tvar a zachytíme příslušné řádkové elementární úpravy:

$$\begin{aligned} & \left(\begin{array}{cc|cc} \lambda + 2 & -1 & 1 & 0 \\ 0 & \lambda - 3 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} -1 & \lambda + 2 & 1 & 0 \\ \lambda - 3 & 0 & 0 & 1 \end{array} \right) \rightsquigarrow \\ & \rightsquigarrow \left(\begin{array}{cc|cc} -1 & \lambda + 2 & 1 & 0 \\ 0 & (\lambda + 2)(\lambda - 3) & \lambda - 3 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & (\lambda + 2)(\lambda - 3) & \lambda - 3 & 1 \end{array} \right) , \\ & \left(\begin{array}{cc|cc} \lambda + 10 & 4 & 1 & 0 \\ -26 & \lambda - 11 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 4 & \lambda + 10 & 1 & 0 \\ 4(\lambda - 11) & -104 & 0 & 4 \end{array} \right) \rightsquigarrow \\ & \rightsquigarrow \left(\begin{array}{cc|cc} 4 & \lambda + 10 & 1 & 0 \\ 0 & -\lambda^2 + \lambda + 6 & 11 - \lambda & 4 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & (\lambda + 2)(\lambda - 3) & \lambda - 11 & -4 \end{array} \right) . \end{aligned}$$

Matice A a B jsou tedy podobné. Nyní budeme hledat příslušnou transformační matici (viz 18.3(ii)):

$$\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ \lambda - 3 & 1 & \lambda - 11 & -4 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & -8 & -4 \end{array} \right)$$

Našli jsme tedy matici

$$C^{-1} = \begin{pmatrix} 1 & 0 \\ -8 & -4 \end{pmatrix},$$

pro kterou je $A = C^{-1}BC$.

Transformační matice, pomocí níž se realizuje podobnost matic A a B , není určena jednoznačně, jak jsme viděli v příkladu 18.6.

18.7. Příklady.

(i) Reálné matice

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad \text{a} \quad B = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

nejsou podobné; mají různou stopu, různé charakteristické polynomy:

$$\det(\lambda E - A) = (\lambda - 2)(\lambda - 3)^2, \quad \det(\lambda E - B) = (\lambda - 2)^2(\lambda - 3).$$

Minimální polynomy těchto matic jsou však stejné; jde o polynom $(\lambda - 2)(\lambda - 3)$ (viz 17.15, resp. 17.16). Kanonický tvar charakteristické matice $\lambda E - A$, resp. $\lambda E - B$ je

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda - 3 & 0 \\ 0 & 0 & (\lambda - 2)(\lambda - 3) \end{pmatrix}, \quad \text{resp.} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda - 2 & 0 \\ 0 & 0 & (\lambda - 2)(\lambda - 3) \end{pmatrix}.$$

(ii) Reálné matice

$$A = \begin{pmatrix} 3 & 1 & 1 \\ 2 & 4 & 2 \\ 1 & 1 & 3 \end{pmatrix} \quad \text{a} \quad B = \begin{pmatrix} 1 & -4 & -1 \\ 1 & 6 & 1 \\ 1 & 4 & 3 \end{pmatrix}$$

jsou podobné. Polynom

$$(\lambda - 2)^2(\lambda - 6), \quad \text{resp.} \quad (\lambda - 2)(\lambda - 6)$$

je jejich charakteristickým, resp. minimálním polynomem, soubor

$$\{ \lambda - 2, \lambda - 2, \lambda - 6 \}$$

je souborem elementárních polynomů jejich charakteristických matic.

Povšimněme si, že matice B vznikla z matice A pomocí dvou dvojic „navzájem inverzních“ elementárních úprav: vynásobení druhého sloupce dvěma a vydělení druhého řádku dvěma, přičtení dvojnásobku prvního sloupce ke druhému a odečtení dvojnásobku druhého řádku od prvního. Rovnost $B = C^{-1}AC$ tedy platí např. pro matici C , která je součinem matic

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{tj.} \quad C = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

18.8. Definice. Čtvercová matice tvaru

$$\begin{pmatrix} a & 0 & \dots & 0 & 0 \\ 1 & a & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & a \end{pmatrix}$$

se nazývá *Jordanova buňka* (na diagonále je prvek a , na rovnoběžné linii pod diagonálou jsou jedničky). Diagonální bloková matice, jejíž bloky na diagonále jsou Jordanovy buňky, se nazývá *Jordanova matice*.

Jordanova matice se někdy definuje ekvivalentním způsobem jako matice tvaru

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 & 0 \\ e_1 & a_2 & 0 & \dots & 0 & 0 \\ 0 & e_2 & a_3 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & e_{n-1} & a_n \end{pmatrix},$$

která splňuje tyto dvě podmínky: pro každé $i = 1, \dots, n - 1$ je

- (i) $e_i = 0$ nebo $e_i = 1$;
- (ii) jestliže $e_i = 1$, potom $a_i = a_{i+1}$.

Jordanovu buňku řádu n dostaneme v případě, kdy $e_1 = e_2 = \dots = e_{n-1} = 1$.

Poznamenejme, že nulová i jednotková matice jsou Jordanovy matice, každá diagonální matice je rovněž Jordanova; její buňky mají řád 1.

18.9. Věta. *Nechť J je Jordanova buňka řádu k , která má na hlavní diagonále prvek a . Potom je polynom $(\lambda - a)^k$ charakteristickým i minimálním polynomem matice J .*

Důkaz. Charakteristickou maticí Jordanovy buňky J je λ -matice

$$\lambda E - J = \begin{pmatrix} \lambda - a & 0 & 0 & \dots & 0 & 0 \\ -1 & \lambda - a & 0 & \dots & 0 & 0 \\ 0 & -1 & \lambda - a & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -1 & \lambda - a \end{pmatrix}.$$

Subdeterminant této λ -matice, který vznikne vynecháním prvního řádku a posledního sloupce, je roven $(-1)^{k-1}$. Posloupnost normovaných největších společných dělitelů všech subdeterminantů řádu $i = 1, \dots, k$ matice J je proto

$$a_1(\lambda) = \dots = a_{k-1}(\lambda) = 1, \quad a_k(\lambda) = (\lambda - a)^k.$$

Stejně vypadá posloupnost invariantních polynomů λ -matice $\lambda E - J$ (viz 16.9); tvrzení věty je tedy dokázáno (viz 17.6 a 17.11). \square

18.10. Věta. *Mějme Jordanovu matici J , která je sestavena z Jordanových buněk J_1, J_2, \dots, J_s . Jestliže tyto Jordanovy buňky mají řádky k_1, k_2, \dots, k_s a na jejich diagonálách jsou po řadě prvky b_1, b_2, \dots, b_s , potom soubor elementárních polynomů charakteristické matice $\lambda E - J$ je*

$$\{ (\lambda - b_1)^{k_1}, (\lambda - b_2)^{k_2}, \dots, (\lambda - b_s)^{k_s} \}.$$

Důkaz. Nechť n je řád matice J . Charakteristická matice $\lambda E - J$ je diagonální bloková matice, na její diagonále jsou bloky

$$\lambda E - J_1, \quad \lambda E - J_2, \quad \dots, \quad \lambda E - J_s.$$

Tyto bloky je možno převést řádkovými a sloupcovými elementárními úpravami (pracujeme však s řádky a sloupci λ -matice $\lambda E - J$) na kanonické λ -matice. Podle předchozí věty tak od λ -matice $\lambda E - J$ dojdeme elementárními úpravami k diagonální λ -matici $B(\lambda)$, která má na diagonále kromě jedniček polynomy

$$(\lambda - b_1)^{k_1}, (\lambda - b_2)^{k_2}, \dots, (\lambda - b_s)^{k_s}. \quad (6)$$

Pomocí metody normovaných největších společných dělitelů všech subdeterminantů řádu $i = 1, 2, \dots, n$ nyní najdeme invariantní polynomy λ -matice $\lambda E - J$.

Prvky b_1, b_2, \dots, b_s nemusí být různé. Polynomy (6) proto srovnáme do tabulky podobným způsobem, jako elementární polynomy (viz 16.16 a 16.17): do jednotlivých řádků zapíšeme všechny polynomy z (6), které mají stejný kořen, a to tak, aby jejich stupně tvořily nerostoucí posloupnost.

Posloupnost $a_1(\lambda), a_2(\lambda), \dots, a_n(\lambda)$ normovaných největších společných dělitelů λ -matice $B(\lambda)$ se nyní určí takto: polynom $a_n(\lambda)$ je součinem všech polynomů utvořené tabulky, polynom $a_{n-1}(\lambda)$ je součinem všech polynomů tabulky, které nestojí v prvním sloupci, polynom $a_{n-2}(\lambda)$ je součinem všech polynomů tabulky, které nestojí ani v prvním ani v druhém sloupci atd; po vyčerpání všech sloupců tabulky jsou zbylé polynomy $a_i(\lambda)$ rovny jedničce (prázdné součiny).

Invariantní polynomy charakteristické matice $\lambda E - J$ dostaneme tedy takto (viz 16.9): $e_n(\lambda)$ je součinem polynomů prvního sloupce tabulky, $e_{n-1}(\lambda)$ je součinem polynomů druhého sloupce tabulky atd. Má-li tabulka i sloupců, je $e_{n-i}(\lambda) = 1, \dots, e_1(\lambda) = 1$ (prázdné součiny). Soubor elementárních polynomů charakteristické

matice $\lambda E - J$ vznikne rozkladem invariantních polynomů na mocniny ireducibilních polynomů; souborem elementárních polynomů charakteristické matice $\lambda E - J$ je tedy soubor (6). \square

Věta 18.10 popisuje *vzájemně jednoznačnou korespondenci* mezi buňkami Jordanovy matice J a elementárními polynomy její charakteristické matice $\lambda E - J$. Každé buňce J_i odpovídá jeden elementární polynom $(\lambda - b_i)^{k_i}$, kde k_i je řád této buňky a b_i je prvek, který v ní stojí na diagonále. Je-li dána Jordanova matice J , dovedeme tedy ihned zapsat soubor elementárních polynomů její charakteristické matice $\lambda E - J$ (i kanonický tvar této λ -matice). Známe-li naopak soubor elementárních polynomů charakteristické matice $\lambda E - J$ Jordanovy matice J , známe všechny buňky matice J .

18.11. Příklady.

(i) Matice

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

nad tělesem \mathbb{Z}_5 je Jordanova buňka čtvrtého řádu. Polynom

$$(\lambda - 3)^4 = (\lambda + 2)^4$$

je jejím charakteristickým i minimálním polynomem (viz 18.9). Kanonickým tvarem její charakteristické matice je λ -matice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & (\lambda + 2)^4 \end{pmatrix};$$

její soubor elementárních polynomů je $\{(\lambda + 2)^4\}$.

(ii) Reálná matice

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 \end{pmatrix}$$

je Jordanova matice šestého řádu sestavená ze čtyř buněk řádu 1, 1, 2, 2. Souborem elementárních polynomů její charakteristické matice je soubor

$$\{ \lambda - 2, \lambda - 2, (\lambda - 2)^2, (\lambda - 3)^2 \},$$

jejími invariantními polynomy jsou polynomy

$$e_1(\lambda) = e_2(\lambda) = e_3(\lambda) = 1 ,$$

$$e_4(\lambda) = \lambda - 2 , \quad e_5(\lambda) = \lambda - 2 , \quad e_6(\lambda) = (\lambda - 2)^2(\lambda - 3)^2 .$$

(iii) Jestliže

$$\{ \lambda - 1 , (\lambda - 1)^2 , (\lambda - 1)^3 , (\lambda - 2)^2 \}$$

je soubor elementárních polynomů charakteristické matice $\lambda E - J$ Jordanovy matice J , potom je matice J sestavena z těchto Jordanových buněk:

$$(1) , \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} , \quad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} , \quad \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} .$$

Invariantní polynomy λ -matice $\lambda E - J$ jsou

$$e_1(\lambda) = \dots = e_5(\lambda) = 1 ,$$

$$e_6(\lambda) = \lambda - 1 , \quad e_7(\lambda) = (\lambda - 1)^2 , \quad e_8(\lambda) = (\lambda - 1)^3(\lambda - 2)^2 .$$

18.12. Důsledky.

- (i) *Dvě Jordanovy matice jsou podobné právě tehdy, mají-li stejný soubor Jordanových buněk, tj. liší-li se pouze pořadím Jordanových buněk na diagonále.*
- (ii) *Jestliže je Jordanova matice podobná diagonální matici, potom je sama diagonální.*
- (iii) *Dvě diagonální matice jsou podobné právě tehdy, když se liší pouze pořadím prvků na diagonále.*

Důkaz. Dvě Jordanovy matice J_1 a J_2 jsou podobné právě tehdy, když mají jejich charakteristické matice stejný soubor elementárních polynomů (viz 18.4). Soubor elementárních polynomů však podle věty 18.10 určuje buňky matic J_1 a J_2 , tj. matice J_1 a J_2 jsou podobné, jsou-li utvořeny ze stejného souboru Jordanových buněk.

Tvrzení (ii) a (iii) jsou jednoduchými důsledky tvrzení (i); stačí si uvědomit, že diagonální matice je Jordanova matice, jejíž všechny buňky jsou prvního řádu. \square

18.13. Příklad.

(i) Reálné diagonální matice

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

jsou podobné (viz 18.12(iii)).

(ii) Reálné matice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{a} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

nejdou podobné, neboť to jsou Jordanovy matice vytvořené z různých souborů Jordanových buněk (viz 18.12(i)). První má dvě buňky druhého řádu, druhá má dvě buňky prvního řádu a jednu buňku druhého řádu. Uvědomme si, že tyto dvě matice mají stejný charakteristický i minimální polynom, a sice $(\lambda - 1)^4$, resp. $(\lambda - 1)^2$ — viz 18.9, 17.7 a 17.15, stejné spektrum a stejnou hodnotu. Srovnáme tento příklad s důsledkem 18.5.

18.14. Definice. Nechť A je čtvercová matice nad tělesem T . Jestliže existuje Jordanova matice J nad tělesem T , taková, že matice A a J jsou podobné, potom říkáme, že matice A má nad tělesem T *Jordanův kanonický tvar* J .

18.15. Věta. Pro čtvercovou matici A nad tělesem T jsou následující tvrzení ekvivalentní:

- (i) Matice A má nad tělesem T *Jordanův kanonický tvar*.
- (ii) Všechny elementární polynomy charakteristické matice $\lambda E - A$ jsou mocninami lineárních polynomů (nad T).
- (iii) Všechny invariantní polynomy charakteristické matice $\lambda E - A$ jsou v $T[\lambda]$ rozložitelné na lineární faktory.
- (iv) Minimální polynom matice A je v $T[\lambda]$ rozložitelný na lineární faktory.
- (v) Charakteristický polynom matice A je v $T[\lambda]$ rozložitelný na lineární faktory.

Důkaz. Matice A má nad tělesem T *Jordanův kanonický tvar* právě tehdy, když soubor elementárních polynomů její charakteristické matice $\lambda E - A$ je souborem elementárních polynomů charakteristické matice $\lambda E - J$ nějaké Jordanovy matice J nad tělesem T (viz 18.4). To však nastane podle 18.10 právě tehdy, když jsou všechny elementární polynomy mocninami lineárních polynomů. Tvrzení (i) a (ii) jsou tedy ekvivalentní. Vzhledem k předchozím výsledkům (16.6, 16.12, 16.16, 17.6, 17.11) jsou navzájem ekvivalentní i tvrzení (ii)–(v). \square

18.16. Důsledek. Nad algebraicky uzavřeným tělesem má každá matice *Jordanův kanonický tvar*. \square

Poznamenejme, že jestliže matice A nad tělesem T *Jordanův kanonický tvar* nemá, potom má *Jordanův kanonický tvar* nad nějakým nadtělesem T' tělesa T ; stačí si uvědomit, že každé těleso je podtělesem nějakého algebraicky uzavřeného tělesa.

Některé reálné matice nemají Jordanův kanonický tvar nad tělesem reálných čísel, ale mají Jordanův kanonický tvar nad tělesem komplexních čísel (viz příklad 18.18(iii)). Některé matice nemají Jordanův kanonický tvar nad tělesem racionálních čísel, ale mají Jordanův kanonický tvar nad tělesem reálných čísel (viz příklad 18.18(iv)).

Matice A může být podobná i několika navzájem různým Jordanovým maticím; všechny jsou však navzájem podobné a liší se tedy jen pořadím Jordanových buněk na diagonále (viz 18.12(i)). Pokud tedy Jordanův kanonický tvar dané matice existuje, je určen jednoznačně až na pořadí Jordanových buněk na diagonále.

Připomeňme ještě jednou, že podobnost matic řádu n nad tělesem T je ekvivalencí na množině $T^{n \times n}$. Při této ekvivalenci se množina $T^{n \times n}$ rozpadne na třídy navzájem podobných matic, v některých třídách jsou Jordanovy matice; jestliže je těleso T algebraicky uzavřené, potom jsou Jordanovy matice ve všech třídách tohoto rozkladu. Jordanovy matice ležící v téže třídě se liší pouze pořadím buněk na diagonále.

18.17. Metoda nalezení Jordanova kanonického tvaru.

Nechť je dána čtvercová matice A nad tělesem T . Chceme-li nalézt Jordanův kanonický tvar matice A , najdeme soubor elementárních polynomů charakteristické matice $\lambda E - A$ a zjistíme, zda jsou všechny elementární polynomy mocninami lineárních polynomů, tj. zda matice A má nad tělesem T Jordanův kanonický tvar (viz 18.15). Podle věty 18.10 nyní zapíšeme Jordanovu matici J , jejíž charakteristická matice $\lambda E - J$ má stejný soubor elementárních polynomů jako charakteristická matice $\lambda E - A$; Jordanovy buňky odpovídající jednotlivým elementárním polynomům (viz 18.10) sestavíme do matice J v libovolném pořadí.

18.18. Příklady.

(i) Charakteristický polynom matice

$$A = \begin{pmatrix} 1 & 2 & -2 \\ -1 & 0 & 2 \\ -2 & 2 & 1 \end{pmatrix}$$

nad tělesem racionálních čísel je $(\lambda - 1)(\lambda + 2)(\lambda - 3)$. Soubor elementárních polynomů λ -matice $\lambda E - A$ je tedy

$$\{ \lambda - 1, \lambda + 2, \lambda - 3 \},$$

tj. Jordanovým kanonickým tvarem matice A je diagonální matice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

(ii) Reálná matice

$$B = \begin{pmatrix} 3 & 1 & -1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

má charakteristický polynom $(\lambda - 2)^3$ a minimální polynom $(\lambda - 2)^2$. Soubor elementárních polynomů λ -matice $\lambda E - B$ je tedy

$$\{(\lambda - 2)^2, \lambda - 2\}$$

a Jordanův kanonický tvar matice B nad tělesem reálných čísel je

$$\begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

(iii) Reálná matice

$$C = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 0 & -2 \\ 2 & 0 & -1 \end{pmatrix}$$

má charakteristický polynom $\lambda(\lambda^2 + 1)$. Nad tělesem reálných (resp. racionálních) čísel tedy matice C nemá Jordanův kanonický tvar. Nad tělesem komplexních čísel má λ -matice $\lambda E - C$ soubor elementárních polynomů

$$\{\lambda, \lambda + i, \lambda - i\}$$

a matice C má nad tělesem komplexních čísel Jordanův kanonický tvar

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & i \end{pmatrix}.$$

Srovnajte tento příklad s příklady (i) a (ii), ve kterých mají matice A, B Jordanův kanonický tvar nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(iv) Reálná matice

$$A = \begin{pmatrix} 0 & 0 & -3 \\ 0 & 1 & -1 \\ 0 & -1 & -1 \end{pmatrix}$$

má charakteristický polynom $\lambda(\lambda^2 - 2)$. Nad tělesem racionálních čísel tedy matice A nemá Jordanův kanonický tvar. Nad tělesem \mathbb{R} , resp. \mathbb{C} má matice A Jordanův kanonický tvar

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & \sqrt{2} & 0 \\ 0 & 0 & -\sqrt{2} \end{pmatrix}.$$

(v) Matice

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

nad tělesem \mathbb{Z}_5 má charakteristický i minimální polynom $(\lambda + 4)^4$, jejím Jordanovým kanonickým tvarem je tedy Jordanova buňka

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

18.19. Definice. Nechť A je čtvercová matice nad tělesem T . Řekneme, že matice A je nad tělesem T *diagonalizovatelná*, je-li podobná nějaké diagonální matici D nad tělesem T .

18.20. Věta. Pro čtvercovou matici A nad tělesem T jsou následující tvrzení ekvivalentní:

- (i) Matice A je nad tělesem T diagonalizovatelná.
- (ii) Všechny elementární polynomy charakteristické matice $\lambda E - A$ nad tělesem T jsou prvního stupně.
- (iii) Všechny invariantní polynomy charakteristické matice $\lambda E - A$ jsou v $T[\lambda]$ rozložitelné na lineární faktory a mají jen jednoduché kořeny.
- (iv) Minimální polynom matice A je v $T[\lambda]$ rozložitelný na lineární faktory a má pouze jednoduché kořeny.

Důkaz. Matice A je diagonalizovatelná právě tehdy, když má Jordanův kanonický tvar J , jehož všechny buňky jsou prvního řádu. To nastane právě tehdy, když jsou všechny elementární polynomy matice $\lambda E - A$ prvního stupně (viz 18.10). Tím je dokázána ekvivalence tvrzení (i) a (ii). Podle předchozích výsledků (16.6, 16.12, 16.16, 17.11) jsou navzájem ekvivalentní i tvrzení (ii)—(iv). \square

18.21. Metoda zjištění diagonalizovatelnosti matice.

Nechť je dána čtvercová matice A nad tělesem T . Vypočteme charakteristický polynom matice A a rozložíme ho v $T[\lambda]$ na mocniny navzájem různých lineárních faktorů (pokud to není možné, pak matice A nemá nad tělesem T Jordanův kanonický tvar a není tedy diagonalizovatelná). Pišme

$$\det(\lambda E - A) = (\lambda - a_1)^{n_1} (\lambda - a_2)^{n_2} \dots (\lambda - a_s)^{n_s},$$

kde prvky $a_1, a_2, \dots, a_s \in T$ jsou navzájem různé. Položme

$$f(\lambda) = (\lambda - a_1)(\lambda - a_2) \dots (\lambda - a_s).$$

Podle věty 18.20 je matice A diagonalizovatelná právě tehdy, když je $f(\lambda)$ minimálním polynomem matice A , tj. právě když je $f(A) = O$.

18.22. Příklady.

(i) Matice A z příkladu 18.18(i) je nad tělesem \mathbb{Q} (resp. \mathbb{R} , \mathbb{C}) diagonalizovatelná, reálná matice B z příkladu 18.18(ii) nad tělesem \mathbb{R} (resp. \mathbb{Q} , \mathbb{C}) diagonalizovatelná není (ale má nad \mathbb{Q} , \mathbb{R} , \mathbb{C} Jordanův kanonický tvar), reálná matice C z příkladu 18.18(iii) nad tělesem \mathbb{Q} , resp. \mathbb{R} diagonalizovatelná není (nemá nad \mathbb{R} Jordanův kanonický tvar), je však diagonalizovatelná nad tělesem komplexních čísel \mathbb{C} . Matice A z příkladu 18.18(iv) není diagonalizovatelná nad \mathbb{Q} (nemá nad \mathbb{Q} Jordanův kanonický tvar), je však diagonalizovatelná nad \mathbb{R} a nad \mathbb{C} . Matice A nad tělesem \mathbb{Z}_5 z příkladu 18.18(v) diagonalizovatelná není, ale má Jordanův kanonický tvar.

(ii) Reálná matice

$$A = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 2 & -1 \\ -1 & 1 & 4 \end{pmatrix}$$

má charakteristický polynom $(\lambda - 1)(\lambda - 3)^2$. Polynom $(\lambda - 1)(\lambda - 3)$ je anulujícím a tedy minimálním polynomem matice A , neboť

$$(A - E)(A - 3E) = \begin{pmatrix} 0 & 2 & 2 \\ 1 & 1 & -1 \\ -1 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} -2 & 2 & 2 \\ 1 & -1 & -1 \\ -1 & 1 & 1 \end{pmatrix} = O.$$

Matice A je tedy diagonalizovatelná, je podobná diagonální matici

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

kteřá je rovněž Jordanovým kanonickým tvarem matice A .

O podobnosti a podobných maticích je možno dokázat řadu zajímavých tvrzení.

18.23. Věta. *Nechť A , B jsou čtvercové matice téhož řádu nad tělesem T .*

- (i) *Navzájem transponované matice jsou podobné.*
- (ii) *Jsou-li matice A a B podobné, jsou podobné i matice A^T a B^T , matice A^{-1} a B^{-1} (pokud existují) a pro každé přirozené číslo k i matice A^k a B^k .*
- (iii) *Jestliže je alespoň jedna z matic A , B regulární, jsou matice AB a BA podobné.*
- (iv) *Nechť A a B jsou podobné matice, $A = C^{-1}BC$. Jestliže je x vlastní vektor matice A příslušný k vlastnímu číslu a , potom je vektor y určený vztahem $y^T = C \cdot x^T$ vlastním vektorem matice B příslušným k vlastnímu číslu a .*

Důkaz.

(i) Nechť A je čtvercová matice řádu n . Uvažujme charakteristické matice $\lambda E - A$ a $\lambda E - A^T$ matic A a A^T . Vzhledem k tomu, že jsou tyto λ -matice navzájem transponované, mají stejnou posloupnost normovaných největších společných dělitelů

všech subdeterminantů řádu $i = 1, \dots, n$ a tedy i stejný kanonický tvar. Proto jsou λ -matice $\lambda E - A$ a $\lambda E - A^T$ ekvivalentní a matice A a A^T podle věty 18.2 podobné.

(ii) Jsou-li matice A a B podobné, je $A = C^{-1}BC$. Transponováním, resp. inverzováním, resp. mocněním získáme rovnost

$$A^T = C^T B^T (C^T)^{-1}, \quad A^{-1} = C^{-1} B^{-1} C, \quad A^k = C^{-1} B^k C.$$

(iii) Je-li matice B , resp. A regulární, je

$$AB = B^{-1} \cdot BA \cdot B, \quad \text{resp.} \quad BA = A^{-1} \cdot AB \cdot A.$$

Nejsou-li matice A a B regulární, nemusí být matice AB a BA podobné; jednoduchý příklad získáme, položíme-li

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

(iv) Jestliže je $A \cdot x^T = a \cdot x^T$, potom je

$$B \cdot C \cdot x^T = C \cdot A \cdot x^T = C \cdot a \cdot x^T = a \cdot C \cdot x^T;$$

označíme-li $y^T = C \cdot x^T$, je

$$B \cdot y^T = a \cdot y^T. \quad \square$$

18.24. Nalezení transformační matice.

Nechť A je matice řádu n nad tělesem T a $J = C^{-1}AC$ Jordanův kanonický tvar matice A . Matice A je maticí nějakého endomorfismu f prostoru $V = T^n$ vzhledem ke kanonické bázi tohoto prostoru, matice C je maticí přechodu od nějaké báze $N = \{v_1, \dots, v_n\}$ ke kanonické bázi prostoru V , matice J je maticí endomorfismu f vzhledem k bázi N (viz 11.11).

$$\begin{array}{ccccccc} & & \overbrace{\hspace{10em}}^f & & & & \\ T^n & \xleftarrow{1} & T^n & \xleftarrow{f} & T^n & \xleftarrow{1} & T^n \\ N & & \text{k.b.} & & \text{k.b.} & & N \\ & & \underbrace{C^{-1}} & & \underbrace{A} & & \underbrace{C} \\ & & \underbrace{\hspace{10em}}_{J = C^{-1}AC} & & & & \end{array}$$

Protože má Jordanova matice poměrně jednoduchý tvar, dá se jednoduše zapsat i vztah mezi vektory v_1, \dots, v_n báze N a jejich obrazy $f(v_1), \dots, f(v_n)$. Je-li např.

$$J = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix},$$

je

$$\begin{aligned} f(v_1) &= 2v_1 + v_2, & \text{tj.} & (f - 2 \cdot 1_V)(v_1) = v_2, \\ f(v_2) &= 2v_2 + v_3, & \text{tj.} & (f - 2 \cdot 1_V)(v_2) = v_3, \\ f(v_3) &= 2v_3, & \text{tj.} & (f - 2 \cdot 1_V)(v_3) = o, \\ f(v_4) &= 3v_4 + v_5, & \text{tj.} & (f - 3 \cdot 1_V)(v_4) = v_5, \\ f(v_5) &= 3v_5, & \text{tj.} & (f - 3 \cdot 1_V)(v_5) = o. \end{aligned}$$

Přepis do maticového tvaru vede k následujícím vztahům

$$\begin{aligned} (A - 2E) \cdot v_1^T &= v_2^T, \\ (A - 2E) \cdot v_2^T &= v_3^T, \\ (A - 2E) \cdot v_3^T &= o^T, \\ (A - 3E) \cdot v_4^T &= v_5^T, \\ (A - 3E) \cdot v_5^T &= o^T. \end{aligned}$$

Vektory v_1, \dots, v_n tedy postupně získáme jako řešení homogenních, resp. nehomogenních soustav lineárních rovnic. Vektory v_3 a v_5 jsou vlastní vektory příslušné k vlastním číslům 2, 3; získáme je z příslušných homogenních soustav. Vektor v_2 , resp. v_4 získáme jako řešení soustavy rovnic s maticí $A - 2E$, resp. $A - 3E$ a pravou stranou v_3^T , resp. v_5^T . Vektor v_1 získáme jako řešení soustavy rovnic s maticí $A - 2E$ a pravou stranou v_2^T . Známe-li vektory v_1, \dots, v_n , známe i matici C ; v jejích sloupcích jsou totiž právě vektory v_1, \dots, v_n .

Uvědomme si, že počet lineárně nezávislých vlastních vektorů příslušných ke všem navzájem různým vlastním číslům matice A (viz 17.22) je roven počtu buněk jejího Jordanova kanonického tvaru J . Matice řádu n je tedy diagonalizovatelná, právě když má n lineárně nezávislých vlastních vektorů.

Vypočteme-li vlastní čísla a vlastní vektory matice A , můžeme výše naznačeným způsobem nalézt Jordanův kanonický tvar J matice A i příslušnou transformační matici C .

Konkrétní postup ukážeme na následujících příkladech.

18.25. Příklady.

(i) Reálná matice

$$A = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$$

má charakteristický polynom $\lambda(\lambda+3)^2$. Vlastními vektory příslušnými k vlastnímu číslu 0, resp. -3 jsou všechny nenulové vektory podprostoru

$$[(1, 1, 1)] , \quad \text{resp.} \quad [(1, -1, 0), (1, 0, -1)] .$$

Protože jsme našli tři lineárně nezávislé vlastní vektory, má Jordanův kanonický tvar $J = C^{-1}AC$ tři buňky. Je tedy

$$J = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -3 \end{pmatrix} \quad \text{a} \quad C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} .$$

(ii) Matice

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

nad tělesem \mathbb{Z}_3 má charakteristický polynom $(\lambda - 1)^2(\lambda - 2)$. Vlastními vektory příslušnými k vlastnímu číslu 1, resp. 2 jsou všechny nenulové vektory podprostoru

$$[(1, 0, 0)] , \quad \text{resp.} \quad [(2, 1, 1)] .$$

Protože jsme našli dva lineárně nezávislé vlastní vektory, má Jordanův kanonický tvar $J = C^{-1}AC$ dvě buňky. Je tedy

$$J = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} .$$

Zatím jsme našli vektory $v_2 = (1, 0, 0)$, $v_3 = (2, 1, 1)$; vektor v_1 vypočteme jako řešení soustavy lineárních rovnic s maticí $A - E$ a pravou stranou v_2^T :

$$\left(\begin{array}{ccc|c} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{array} \right)$$

Řešením je např. vektor $v_1 = (0, 1, 0)$; tedy

$$C = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} .$$

(iii) Matice

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

nad tělesem \mathbb{Z}_5 má charakteristický polynom $(\lambda - 1)^3$. Vlastními vektory příslušnými k vlastnímu číslu 1 jsou všechny nenulové vektory podprostoru

$$[(1, 0, 0)] .$$

Protože jsme našli jen jeden lineárně nezávislý vlastní vektor, má Jordanův kanonický tvar $J = C^{-1}AC$ jedinou buňku. Je tedy

$$J = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} .$$

Zatím jsme našli jen vektor $v_3 = (1, 0, 0)$; vektor v_2 vypočteme jako řešení soustavy lineárních rovnic s maticí $A - E$ a pravou stranou v_3^T :

$$\left(\begin{array}{ccc|c} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

Řešením je např. vektor $v_2 = (0, 1, 0)$; vektor v_1 nyní vypočteme jako řešení soustavy lineárních rovnic s maticí $A - E$ a pravou stranou v_2^T :

$$\left(\begin{array}{ccc|c} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

Řešením je např. vektor $v_1 = (0, 4, 1)$; tedy

$$C = \begin{pmatrix} 0 & 0 & 1 \\ 4 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} .$$

(iv) Reálná matice

$$A = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 3 & 0 & 3 & -3 \\ 4 & -1 & 3 & -3 \end{pmatrix}$$

má charakteristický polynom λ^4 . Vlastními vektory příslušnými k vlastnímu číslu 0 jsou všechny nenulové vektory podprostoru

$$[(1, 1, 0, 1), (0, 0, 1, 1)] .$$

Protože jsme našli dva lineárně nezávislé vlastní vektory, má Jordanův kanonický tvar $J = C^{-1}AC$ dvě buňky. Protože je minimální polynom matice A roven λ^2 , je

$$J = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Zatím jsme našli vektory $v_2 = (1, 1, 0, 1)$ a $v_4 = (0, 0, 1, 1)$; vektory v_1 a v_3 vypočteme jako řešení soustavy lineárních rovnic s maticí A a pravou stranou v_2^T a v_4^T :

$$\left(\begin{array}{cccc|c|c} 1 & -1 & 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 0 & 1 & 0 \\ 3 & 0 & 3 & -3 & 0 & 1 \\ 4 & -1 & 3 & -3 & 1 & 1 \end{array} \right).$$

Řešeními jsou např. vektory $v_1 = (0, -1, 0, 0)$ a $v_3 = (0, 0, 0, -\frac{1}{3})$; vhodnější volbou budou vektory $3v_3$ a $3v_4$; tedy

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 1 & -1 & 3 \end{pmatrix}.$$

(v) Reálná matice

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

má charakteristický polynom $(\lambda - 2)^3$. Vlastními vektory příslušnými k vlastnímu číslu 2 jsou všechny nenulové vektory podprostoru

$$[(1, -1, 0), (2, -1, 1)].$$

Protože jsme našli dva lineárně nezávislé vlastní vektory, má Jordanův kanonický tvar $J = C^{-1}AC$ dvě buňky. Je tedy

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Pokud bychom vektory $(1, -1, 0)$, $(2, -1, 1)$ označili v_2, v_3 resp. v_3, v_2 , nepodařilo by se nám najít vektor v_1 , který by byl řešením soustavy lineárních rovnic s maticí $A - 2E$ a pravou stranou v_2^T . Jako pravou stranu této soustavy je třeba vzít vhodnou lineární kombinaci výše uvedených vlastních vektorů, např. vektor

$v_2 = (1, 0, 1)$ (a jako vektor v_3 kterýkoli vlastní vektor, který není násobkem vektoru v_2):

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 1 \end{array} \right)$$

Řešením je např. vektor $v_1 = (1, 0, 0)$; tedy

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

(vi) Reálná matice

$$A = \begin{pmatrix} 0 & -4 & 0 \\ 1 & -4 & 0 \\ 1 & -2 & -2 \end{pmatrix}$$

má charakteristický polynom $(\lambda + 2)^3$. Vlastními vektory příslušnými k vlastnímu číslu -2 jsou všechny nenulové vektory podprostoru

$$[(0, 0, 1), (2, 1, 0)].$$

Protože jsme našli dva lineárně nezávislé vlastní vektory, má Jordanův kanonický tvar $J = C^{-1}AC$ dvě buňky. Je tedy

$$J = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 1 & -2 \end{pmatrix}.$$

Pokud bychom vektory $(0, 0, 1)$, $(2, 1, 0)$ označili v_1, v_3 , resp. v_3, v_1 , nepodařilo by se nám najít vektor v_2 , který by byl řešením soustavy lineárních rovnic s maticí $A+2E$ a pravou stranou v_3^T . Jako pravou stranu této soustavy je třeba vzít vhodnou lineární kombinaci výše uvedených vlastních vektorů, např. vektor $v_3 = (2, 1, 1)$ (a jako vektor v_1 kterýkoli vlastní vektor, který není násobkem vektoru v_3):

$$\left(\begin{array}{ccc|c} 2 & -4 & 0 & 2 \\ 1 & -2 & 0 & 1 \\ 1 & -2 & 0 & 1 \end{array} \right)$$

Řešením je např. vektor $v_2 = (1, 0, 0)$; tedy

$$C = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

(vii) Reálná matice

$$A = \begin{pmatrix} 3 & -4 & 0 & 0 \\ 4 & -5 & -2 & 4 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 2 & -1 \end{pmatrix}$$

má charakteristický polynom $(\lambda + 1)^2(\lambda - 1)^2$. Vlastními vektory příslušnými k vlastnímu číslu -1 , resp. 1 jsou všechny nenulové vektory podprostoru

$$[(1, 1, 0, 0)] \quad \text{resp.} \quad [(-2, -1, 1, 1)] .$$

Jordanův kanonický tvar $J = C^{-1}AC$ má dvě buňky,

$$J = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix} .$$

Položíme $v_2 = (-2, -1, 1, 1)$ a $v_4 = (1, 1, 0, 0)$ a jako v předchozích příkladech vypočteme zbylé vektory v_1, v_3 a dojdeme k matici

$$C = \begin{pmatrix} 3 & -2 & \frac{1}{4} & 1 \\ 2 & -1 & 0 & 1 \\ \frac{1}{2} & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} .$$

Paragraf ukončíme stručnou informací o dalších kanonických tvarech matic.

18.26. Definice. Necht $f(\lambda) \in T[\lambda]$ je normovaný polynom stupně $n \geq 1$,

$$f(\lambda) = \lambda^n + c_1\lambda^{n-1} + \dots + c_{n-1}\lambda + c_n .$$

Doprovodnou maticí polynomu $f(\lambda)$ budeme rozumět matici

$$D = \begin{pmatrix} 0 & 0 & \dots & 0 & -c_n \\ 1 & 0 & \dots & 0 & -c_{n-1} \\ 0 & 1 & \dots & 0 & -c_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & -c_1 \end{pmatrix} ;$$

je-li $n = 1$, je doprovodnou maticí polynomu $f(\lambda) = \lambda + c_1$ matice $(-c_1)$.

Poznamenejme, že jsme v příkladu 15.4 počítali determinant matice, která se jen nepodstatně liší od výše definované doprovodné matice.

18.27. Lemma. *Nechť D je doprovoďná matice polynomu $f(\lambda) \in T[\lambda]$. Potom charakteristickým i minimálním polynomem matice D je polynom $f(\lambda)$.*

Důkaz. Nechť $f(\lambda) = \lambda^n + c_1\lambda^{n-1} + \dots + c_{n-1}\lambda + c_n$. Označme symboly $a_{n-1}(\lambda)$, resp. $a_n(\lambda)$ normované největší společné dělitele všech subdeterminantů řádu $n-1$, resp. n λ -matice

$$\lambda E - D = \begin{pmatrix} \lambda & 0 & \dots & 0 & c_n \\ -1 & \lambda & \dots & 0 & c_{n-1} \\ 0 & -1 & \dots & 0 & c_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 & \lambda + c_1 \end{pmatrix}.$$

Subdeterminant λ -matice $\lambda E - D$, který vznikne vyškrtnutím prvního řádku a posledního sloupce, je roven $(-1)^{n-1}$; proto je $a_{n-1}(\lambda) = 1$. Přičteme-li postupně λ -násobek posledního řádku λ -matice $\lambda E - D$ k předposlednímu, λ -násobek předposledního řádku k $(n-2)$ -hému, ... a λ -násobek druhého řádku k prvnímu, získáme v pravém horním rohu vzniklé λ -matice polynom $f(\lambda)$. Rozvojem podle prvního řádku zjistíme, že

$$\det(\lambda E - D) = (-1)^{n+1} \cdot f(\lambda) \cdot (-1)^{n-1} = f(\lambda), \quad \text{tj.} \quad a_n(\lambda) = f(\lambda).$$

Invariantními polynomy λ -matice $\lambda E - D$ jsou tedy polynomy

$$e_1(\lambda) = \dots = e_{n-1}(\lambda) = 1, \quad e_n(\lambda) = f(\lambda).$$

Podle vět 17.6 a 17.11 je polynom $f(\lambda)$ charakteristickým i minimálním polynomem matice D . \square

18.28. Věta. *Každá matice A je podobná diagonální blokové matici D , jejíž bloky na diagonále jsou doprovoďnými maticemi netriviálních invariantních polynomů charakteristické matice $\lambda E - A$ matice A .*

Důkaz. Předpokládejme, že

$$e_1(\lambda) = \dots = e_{k-1}(\lambda) = 1, \quad e_k(\lambda) \neq 1, \dots, e_n(\lambda)$$

jsou invariantní polynomy λ -matice $\lambda E - A$. Nechť D je diagonální bloková matice sestavená z doprovoďných matic D_k, \dots, D_n polynomů $e_k(\lambda), \dots, e_n(\lambda)$ jako bloků na diagonále. Vzhledem k tomu, že řády doprovoďných matic D_k, \dots, D_n jsou po řadě rovny stupňům polynomů $e_k(\lambda), \dots, e_n(\lambda)$ a součet těchto stupňů je roven řádu matice A , mají matice A a D stejný řád.

Ukážeme, že jsou matice A a D podobné. Charakteristickou matici $\lambda E - D$ můžeme řádkovými a sloupcovými úpravami převést na diagonální matici, která má na diagonále kromě jedniček pouze polynomy $e_k(\lambda), \dots, e_n(\lambda)$; jednotlivé bloky

$\lambda E - D_i$ je totiž možno podle předchozího lemmatu řádkovými a sloupcovými úpravami převést na kanonické matice

$$\begin{pmatrix} 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 0 & e_i(\lambda) \end{pmatrix}.$$

Prohozením řádků a sloupců seřadíme polynomy $e_k(\lambda), \dots, e_n(\lambda)$ na poslední místa diagonály a získáme kanonický tvar λ -matice $\lambda E - D$, který je stejný jako kanonický tvar λ -matice $\lambda E - A$. Matice A a D jsou proto podobné podle věty 18.2. \square

18.29. Definice. Nechť A je čtvercová matice nad tělesem T . *Prvním racionálním kanonickým tvarem* matice A budeme rozumět blokovou diagonální matici D , která je sestavena z doprovoďných matic netriviálních invariantních polynomů charakteristické matice $\lambda E - A$.

18.30. Věta. *Každá matice A je podobná diagonální blokové matici D , jejíž bloky na diagonále jsou doprovoďnými maticemi elementárních polynomů charakteristické matice $\lambda E - A$ matice A .*

Důkaz. Nechť A je matice řádu n a nechť

$$\{\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)\}$$

je soubor elementárních polynomů λ -matice $\lambda E - A$. Nechť D je diagonální bloková matice sestavená z doprovoďných matic D_1, \dots, D_m elementárních polynomů $\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)$ jako bloků na diagonále. Matice A a D mají stejný řád; v obou případech je roven součtu stupňů polynomů $\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)$.

Ukážeme, že jsou matice A a D podobné. Charakteristickou matici $\lambda E - D$ můžeme řádkovými a sloupcovými úpravami převést na diagonální matici, která má na diagonále kromě jedniček pouze polynomy $\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)$; jednotlivé bloky $\lambda E - D_i$ je totiž možno podle lemmatu 18.27 řádkovými a sloupcovými úpravami převést na kanonické matice

$$\begin{pmatrix} 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 0 & \varepsilon_i(\lambda) \end{pmatrix}.$$

Invariantní polynomy λ -matice $\lambda E - D$ nyní najdeme stejně jako v důkaze věty 18.10. Polynomy $\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)$ srovnáme do tabulky tak, aby v jednotlivých řádcích byly všechny mocniny téhož ireducibilního polynomu a exponenty tvořily nerostoucí posloupnosti. Pomocí metody největších společných dělitelů všech subdeterminantů řádu $i = 1, \dots, n$ zjistíme (stejně jako v 18.10), že

invariantní polynomy λ -matice $\lambda E - D$ jsou součiny jednotlivých sloupců tabulky a že souborem elementárních polynomů λ -matice $\lambda E - D$ je původní soubor

$$\{\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)\}$$

elementárních polynomů λ -matice $\lambda E - A$. Proto jsou λ -matice $\lambda E - A$ a $\lambda E - D$ ekvivalentní (viz 16.18) a matice A a D jsou podobné (viz 18.2). \square

18.31. Definice. Nechť A je čtvercová matice nad tělesem T . *Druhým racionálním kanonickým tvarem* matice A budeme rozumět blokovou diagonální matici D , která je sestavena z doprovodných matic elementárních polynomů charakteristické matice $\lambda E - A$.

18.32. Definice. Nechť $f(\lambda) \in T[\lambda]$ je normovaný ireducibilní polynom stupně k . *Hyperdoprovodnou maticí* polynomu $f(\lambda)^n$, kde $n \geq 1$, budeme rozumět blokovou matici

$$D = \begin{pmatrix} A & O & \dots & O & O \\ M & A & \dots & O & O \\ O & M & \dots & O & O \\ \dots & \dots & \dots & \dots & \dots \\ O & O & \dots & M & A \end{pmatrix}$$

řádu kn , kde A je doprovodnou maticí polynomu $f(\lambda)$ a M je čtvercová matice téhož řádu, která má v pravém horním rohu jedničku a na ostatních místech nuly. Je-li $n = 1$, je hyperdoprovodnou maticí polynomu $f(\lambda)$ jeho doprovodná matice.

Poznamenejme, že hyperdoprovodnou maticí polynomu $(\lambda + a)^n$ je Jordanova buňka řádu n , která má na diagonále prvek $-a$.

18.33. Lemma. *Nechť $f(\lambda) \in T[\lambda]$ je normovaný ireducibilní polynom a D hyperdoprovodná matice polynomu $f(\lambda)^n$, kde $n \geq 1$. Potom charakteristickým i minimálním polynomem matice D je polynom $f(\lambda)^n$.*

Důkaz. Předpokládejme, že polynom $f(\lambda)$ má stupeň k . Charakteristický polynom hyperdoprovodné matice D je podle věty 17.7 roven n -té mocnině charakteristického polynomu doprovodné matice polynomu $f(\lambda)$, tj. $f(\lambda)^n$. Vyškrtnutím prvního řádku a posledního sloupce λ -matice $\lambda E - D$ získáme subdeterminant, který je roven $(-1)^{kn-1}$. Předposlední invariantní polynom λ -matice $\lambda E - D$ je tedy roven 1 a minimální polynom matice D je roven charakteristickému. \square

18.34. Věta. *Každá matice A je podobná diagonální blokové matici D , jejíž bloky na diagonále jsou hyperdoprovodnými maticemi elementárních polynomů charakteristické matice $\lambda E - A$ matice A .*

Důkaz. Nechť

$$\{\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)\}$$

je soubor elementárních polynomů λ -matice $\lambda E - A$. Nechť D je diagonální bloková matice sestavená z hyperdoprovodných matic D_1, \dots, D_m elementárních polynomů

$\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)$. Matice A a D mají stejný řád; v obou případech je roven součtu stupňů polynomů $\varepsilon_1(\lambda), \varepsilon_2(\lambda), \dots, \varepsilon_m(\lambda)$. Stejným způsobem jako v důkazu věty 18.30 nyní ukážeme, že jsou matice A a D podobné. \square

18.35. Definice. Nechť A je čtvercová matice nad tělesem T . *Třetím racionálním kanonickým tvarem* nebo též *Jacobsonovým kanonickým tvarem* matice A budeme rozumět blokovou diagonální matici D , která je sestavena z hyperdoprovodných matic elementárních polynomů charakteristické matice $\lambda E - A$.

Poznamenejme, že je-li těleso T algebraicky uzavřené, potom třetí racionální kanonický tvar každé matice nad tělesem T je stejný jako Jordanův.

18.36. Příklady.

(i) Je dána reálná matice

$$A = \begin{pmatrix} -7 & -12 & 0 & 0 \\ 3 & 5 & 0 & 0 \\ 0 & 1 & -5 & -8 \\ 0 & 0 & 2 & 3 \end{pmatrix}.$$

Pomocí předchozích výsledků zjistíme, že charakteristickým i minimálním polynomm matice A je polynom $(\lambda+1)^4$, takže invariantními polynomy λ -matice $\lambda E - A$ jsou polynomy

$$e_1(\lambda) = e_2(\lambda) = e_3(\lambda) = 1, \quad e_4(\lambda) = (\lambda+1)^4;$$

jediným elementárním polynomm této λ -matice (nad \mathbb{Q}, \mathbb{R} i \mathbb{C}) je polynom

$$(\lambda+1)^4 = \lambda^4 + 4\lambda^3 + 6\lambda^2 + 4\lambda + 1.$$

Prvním i druhým racionálním kanonickým tvarem matice A (nad \mathbb{Q}, \mathbb{R} i \mathbb{C}) je tedy matice

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & -4 \end{pmatrix}.$$

Třetím racionálním kanonickým tvarem (a rovněž Jordanovým kanonickým tvarem) matice A (nad \mathbb{Q}, \mathbb{R} i \mathbb{C}) je matice

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

(ii) Mějme reálnou matici

$$B = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 4 & -2 & -4 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & -4 & 2 & 0 \\ 0 & 0 & 0 & 1 & -1 & 1 \end{pmatrix}.$$

Protože je matice B diagonální bloková, snadno se vypočte její charakteristický i minimální polynom (viz 17.7, 17.11, 17.12(iv) a 17.15) a určí invariantní polynomy charakteristické matice $\lambda E - B$:

$$e_1(\lambda) = e_2(\lambda) = e_3(\lambda) = 1, \quad e_4(\lambda) = \lambda - 2,$$

$$e_5(\lambda) = (\lambda+2)(\lambda-2) = \lambda^2 - 4, \quad e_6(\lambda) = (\lambda+2)(\lambda-2)(\lambda-1) = \lambda^3 - \lambda^2 - 4\lambda + 4.$$

Prvním racionálním kanonickým tvarem matice B (nad \mathbb{Q} , \mathbb{R} i \mathbb{C}) je matice

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 1 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Druhým i třetím racionálním kanonickým tvarem (a rovněž Jordanovým kanonickým tvarem) matice B (nad \mathbb{Q} , \mathbb{R} i \mathbb{C}) je diagonální matice

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(iii) Reálná matice

$$C = \begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & -3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & -5 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & -1 & 1 & -1 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & -4 \end{pmatrix}$$

je diagonální bloková se třemi bloky na diagonále. Proto se charakteristický i minimální polynom matice C a invariantní polynomy její charakteristické matice $\lambda E - C$ vypočítají pomocí vět 16.9, 17.7, 17.11 a 17.15:

$$\begin{aligned} e_1(\lambda) &= e_2(\lambda) = e_3(\lambda) = e_4(\lambda) = e_5(\lambda) = e_6(\lambda) = 1, \\ e_7(\lambda) &= (\lambda + 2)(\lambda^2 + 2\lambda - 1) = \lambda^3 + 4\lambda^2 + 3\lambda - 2 = \\ &= (\lambda + 2)(\lambda + 1 - \sqrt{2})(\lambda + 1 + \sqrt{2}), \\ e_8(\lambda) &= (\lambda + 2)(\lambda^2 + 2\lambda - 1)^2 = (\lambda + 2)(\lambda^4 + 4\lambda^3 + 2\lambda^2 - 4\lambda + 1) = \\ &= \lambda^5 + 6\lambda^4 + 10\lambda^3 - 7\lambda + 2 = \\ &= (\lambda + 2)(\lambda + 1 - \sqrt{2})^2(\lambda + 1 + \sqrt{2})^2 = \\ &= (\lambda + 2)(\lambda^2 + (2 - 2\sqrt{2})\lambda + (3 - 2\sqrt{2}))(\lambda^2 + (2 + 2\sqrt{2})\lambda + (3 + 2\sqrt{2})). \end{aligned}$$

Prvním racionálním kanonickým tvarem matice C (nad \mathbb{Q} , \mathbb{R} i \mathbb{C}) je matice

$$\begin{pmatrix} 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -10 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -6 \end{pmatrix}.$$

Druhým racionálním kanonickým tvarem matice C nad \mathbb{Q} je matice

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -4 \end{pmatrix}.$$

Druhým racionálním kanonickým tvarem matice C nad \mathbb{R} a \mathbb{C} je matice

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 + \sqrt{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 - \sqrt{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -3 + 2\sqrt{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -2 + 2\sqrt{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -3 - 2\sqrt{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 - 2\sqrt{2} \end{pmatrix}.$$

Třetím racionálním kanonickým tvarem matice C nad \mathbb{Q} je matice

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}.$$

Třetím racionálním kanonickým tvarem (a současně Jordanovým kanonickým tvarem) matice C nad \mathbb{R} a \mathbb{C} je matice

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 + \sqrt{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 - \sqrt{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 + \sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 + \sqrt{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 - \sqrt{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 - \sqrt{2} \end{pmatrix}.$$

(iv) Reálná matice

$$A = \begin{pmatrix} 0 & -1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

je diagonální bloková se dvěma bloky na diagonále. Charakteristický i minimální polynom matice A a invariantní polynomy charakteristické matice $\lambda E - A$ se vy počítají s pomocí vět 16.9, 17.7, 17.11 a 17.15:

$$e_1(\lambda) = e_2(\lambda) = e_3(\lambda) = e_4(\lambda) = e_5(\lambda) = 1,$$

$$e_6(\lambda) = e_7(\lambda) = (\lambda^2 + 1) = (\lambda + i)(\lambda - i),$$

$$e_8(\lambda) = (\lambda^2 + 1)^2 = \lambda^4 + 2\lambda^2 + 1 = (\lambda + i)^2(\lambda - i)^2 = (\lambda^2 + 2i\lambda - 1)(\lambda^2 - 2i\lambda - 1).$$

Prvním racionálním kanonickým tvarem matice A nad \mathbb{Q} , \mathbb{R} i \mathbb{C} a současně druhým racionálním kanonickým tvarem matice A nad \mathbb{Q} a \mathbb{R} je matice

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Druhým racionálním kanonickým tvarem matice A nad \mathbb{C} je matice

$$\begin{pmatrix} -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -2i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2i \end{pmatrix}.$$

Třetím racionálním kanonickým tvarem matice A nad \mathbb{Q} a \mathbb{R} je matice

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Třetím racionálním kanonickým tvarem (a současně Jordanovým kanonickým tvarem) matice A nad \mathbb{C} je matice

$$\begin{pmatrix} -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & i \end{pmatrix}.$$

19. WEYROVA TEORIE CHARAKTERISTICKÝCH ČÍSEL

V následujících odstavcích vyložíme efektivní způsob převedení reálné nebo komplexní matice na Jordanův kanonický tvar; tuto metodu publikoval roku 1885 český matematik Eduard Weyr (1852–1903).¹ Weyrovu metodu podáme v moderní řeči vektorových prostorů a homomorfismů.

19.1. Obrazy a jádra. Nechť A je komplexní matice řádu n a nechť f je odpovídající endomorfismus vektorového prostoru $V = \mathbb{C}^n$, tj. matice A je maticí endomorfismu f vzhledem ke kanonické bázi prostoru V . Pro dané komplexní číslo λ je matice $A - \lambda E$ maticí endomorfismu $\varphi = f - \lambda \cdot 1_V$ prostoru V . Číslo λ je vlastním číslem matice A právě tehdy, když je matice $A - \lambda E$ singulární; to nastane právě tehdy, když endomorfismus φ není izomorfismus, neboli $\text{Im } \varphi$ je vlastní částí prostoru V , tj. $V \supset \text{Im } \varphi$.

Předpokládejme, že λ je vlastním číslem matice A . Existuje tedy přirozené číslo $r \geq 1$ takové, že

$$V \supset \text{Im } \varphi \supset \text{Im } \varphi^2 \supset \dots \supset \text{Im } \varphi^{r-1} \supset \text{Im } \varphi^r = \text{Im } \varphi^{r+1} = \dots ,$$

číslo r je tedy nejmenší přirozené číslo, pro které $\text{Im } \varphi^r \cap \text{Ker } \varphi = O$. Vzhledem k tomu, že pro každé $i = 1, 2, \dots$ je podle věty o hodnotě a defektu (pro endomorfismus φ^i)

$$\dim \text{Ker } \varphi^i + \dim \text{Im } \varphi^i = n ,$$

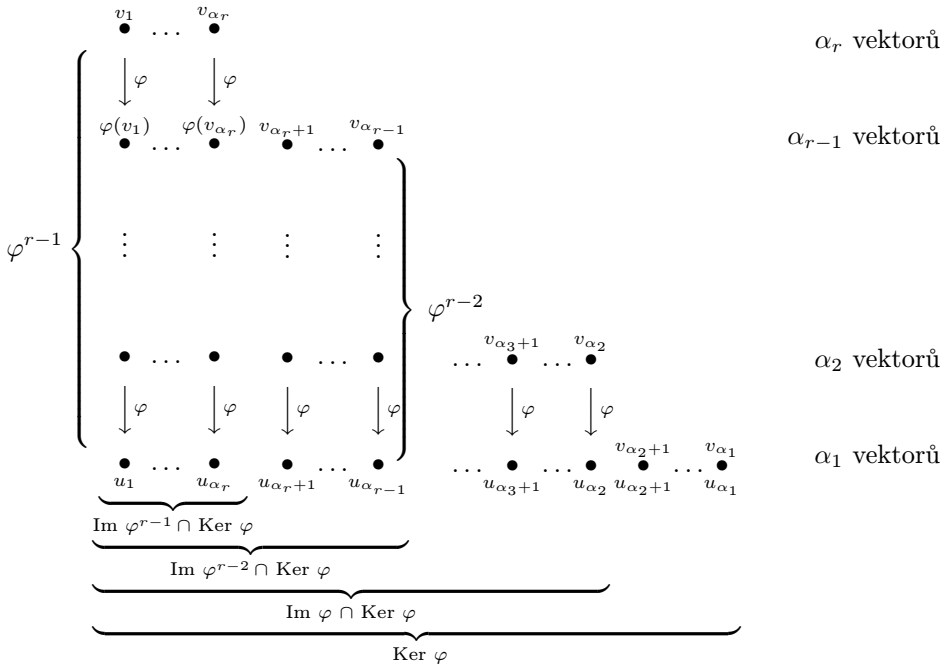
je dále

$$O \subset \text{Ker } \varphi \subset \text{Ker } \varphi^2 \subset \dots \subset \text{Ker } \varphi^{r-1} \subset \text{Ker } \varphi^r = \text{Ker } \varphi^{r+1} = \dots . \quad (1)$$

19.2. Weyrova charakteristická čísla. Weyrovými charakteristickými čísly matice A příslušnými k vlastnímu číslu λ budeme rozumět čísla

$$\begin{aligned} \alpha_1 &= \dim V && - \dim \text{Im } \varphi = \dim \text{Ker } \varphi - \dim O , \\ \alpha_2 &= \dim \text{Im } \varphi && - \dim \text{Im } \varphi^2 = \dim \text{Ker } \varphi^2 - \dim \text{Ker } \varphi , \\ &\dots && \dots \\ \alpha_i &= \dim \text{Im } \varphi^{i-1} - \dim \text{Im } \varphi^i = \dim \text{Ker } \varphi^i - \dim \text{Ker } \varphi^{i-1} , && (2) \\ &\dots && \dots \\ \alpha_r &= \dim \text{Im } \varphi^{r-1} - \dim \text{Im } \varphi^r = \dim \text{Ker } \varphi^r - \dim \text{Ker } \varphi^{r-1} . \end{aligned}$$

¹ O životě a díle Eduarda Weyra se můžeme dočíst v monografii J. Bečvář a kol.: *Eduard Weyr 1852–1903*, Prometheus, Praha 1995, 196 str. a 24 obr. příloh. Lineární algebrы se týkají články *Eduard Weyr, lineární algebra a teorie hyperkomplexních čísel*, str. 91–119, a *Weyrova teorie charakteristických čísel*, str. 121–127. Viz též H. Shapiro: *The Weyr Characteristic*, Amer. Math. Monthly 106(1999), 919–929.



Protože vektory u_1, \dots, u_{α_r} leží v $\text{Im } \varphi^{r-1}$, existují vektory v_1, \dots, v_{α_r} , takové, že $\varphi^{r-1}(v_1) = u_1, \dots, \varphi^{r-1}(v_{\alpha_r}) = u_{\alpha_r}$. Dále existují vektory $v_{\alpha_r+1}, \dots, v_{\alpha_r-1}$, takové, že $\varphi^{r-2}(v_{\alpha_r+1}) = u_{\alpha_r+1}, \dots, \varphi^{r-2}(v_{\alpha_r-1}) = u_{\alpha_r-1}$ atd. Nakonec existují vektory $v_{\alpha_3+1}, \dots, v_{\alpha_2}$, takové, že $\varphi(v_{\alpha_3+1}) = u_{\alpha_3+1}, \dots, \varphi(v_{\alpha_2}) = u_{\alpha_2}$. Pro úplnost položme $v_{\alpha_2+1} = u_{\alpha_2+1}, \dots, v_{\alpha_1} = u_{\alpha_1}$. Množina

$$B = \{v_1, \varphi(v_1), \dots, \varphi^{r-1}(v_1); \dots; v_{\alpha_r}, \varphi(v_{\alpha_r}), \dots, \varphi^{r-1}(v_{\alpha_r}); v_{\alpha_r+1}, \dots, \varphi^{r-2}(v_{\alpha_r+1}); \dots; v_{\alpha_2}, \varphi(v_{\alpha_2}); v_{\alpha_2+1}; \dots; v_{\alpha_1}\} \quad (5)$$

je zřejmě obsažena v $\text{Ker } \varphi^r$ a má $\alpha_1 + \alpha_2 + \dots + \alpha_r$ prvků (viz obrázek — počítáno po vrstvách), tj. tolik, kolik je $\dim \text{Ker } \varphi^r$.

Nyní dokážeme lineární nezávislost množiny B . Předpokládejme, že

$$a_1x_1 + a_2x_2 + \dots + a_kx_k = 0, \quad (6)$$

kde x_1, x_2, \dots, x_k jsou navzájem různé prvky množiny B a koeficienty a_1, a_2, \dots, a_k jsou nenulové. Nechť m je nejmenší přirozené číslo, pro které $\varphi^m(x_i) = 0$ pro každé

$i = 1, \dots, k$ (tedy $m \leq r$, neboť $B \subset \text{Ker } \varphi^r$). Provedeme-li endomorfismus φ^{m-1} na rovnost (6), získáme vyjádření nulového vektoru jako netriviální lineární kombinace lineárně nezávislých vektorů u_1, \dots, u_{α_1} a to je spor. Množina B je tedy lineárně nezávislá a je proto bází podprostoru $\text{Ker } \varphi^r$; uspořádání této báze je uvedeno v (5). Budeme říkat, že B je *Weyrova báze* podprostoru $\text{Ker } \varphi^r$.

19.4. Odpovídající matice. Rozšířme nyní sestrojenou bázi B podprostoru $\text{Ker } \varphi^r$ na bázi B' prostoru V ; bázi B' uspořádejme tak, že nejprve jdou vektory báze B ve výše uvedeném pořadí (5) a teprve potom přidané vektory. Matice endomorfismu φ vzhledem k bázi B' má tvar

$$M = \begin{pmatrix} I & X \\ 0 & Y \end{pmatrix};$$

vzhledem ke konstrukci báze B je I Jordanova matice řádu $\alpha_1 + \alpha_2 + \dots + \alpha_r$ s nulami na diagonále, která má

$$\begin{array}{ll} \alpha_r & \text{buněk řádu } r, \\ \alpha_{r-1} - \alpha_r & \text{buněk řádu } r - 1, \\ \dots\dots\dots & \dots\dots\dots \\ \alpha_1 - \alpha_2 & \text{buněk řádu } 1, \end{array}$$

tj. celkem α_1 buněk. Každá buňka odpovídá jednomu řetízku vektorů z báze B , který končí některým z vektorů u_1, \dots, u_{α_1} . Původní endomorfismus $f = \varphi + \lambda \cdot 1_V$ má tedy vzhledem k bázi B' matici

$$M + \lambda E = \begin{pmatrix} I + \lambda E & X \\ 0 & Y + \lambda E \end{pmatrix},$$

kde $J = I + \lambda E$ je Jordanova matice stejné struktury jako matice I , ale s číslem λ na diagonále. Násobnost s vlastního čísla λ matice A je tedy alespoň $\alpha_1 + \dots + \alpha_r$, takže

$$r \leq \alpha_1 + \dots + \alpha_r \leq s. \quad (7)$$

19.5. Celkový pohled. Předchozí úvahy můžeme provést pro každé vlastní číslo matice A . Protože pracujeme v komplexním oboru, je charakteristický polynom $p(\lambda)$ matice A rozložitelný na lineární faktory,

$$p(\lambda) = (\lambda - \lambda_1)^{s_1} (\lambda - \lambda_2)^{s_2} \dots (\lambda - \lambda_k)^{s_k}; \quad (8)$$

předpokládejme, že vlastní čísla $\lambda_1, \dots, \lambda_k$ jsou navzájem různá.

Pro každé $i = 1, \dots, k$ nechť

$$\alpha_1^i, \alpha_2^i, \dots, \alpha_{r_i}^i$$

jsou Weyrova charakteristická čísla matice A příslušná k vlastnímu číslu λ_i , nechť $\varphi_i = f - \lambda_i \cdot 1_V$. Podle (7) je pro každé $i = 1, \dots, k$

$$r_i \leq \alpha_1^i + \dots + \alpha_{r_i}^i \leq s_i, \quad (9)$$

a tedy podle (1) je

$$\text{Ker } \varphi_i^{r_i} = \text{Ker } \varphi_i^{s_i}. \quad (10)$$

Pro každé $i = 1, \dots, k$ označme symbolem B_i výše zavedenou Weyrovu bázi podprostoru $\text{Ker } \varphi_i^{r_i}$ a symbolem J_i Jordanovu matici řádu $\alpha_1^i + \dots + \alpha_{r_i}^i$ s prvkem λ_i na diagonále; strukturu této Jordanovy matice určují Weyrova charakteristická čísla $\alpha_1^i, \dots, \alpha_{r_i}^i$.

V následujícím textu dokážeme, že sjednocení Weyrovýchází B_i , $i = 1, \dots, k$, tvoří bázi prostoru V a že složení Jordanových matic J_i dává Jordanův kanonický tvar matice A ; nejprve však musíme zavést několik pojmů a dokázat jedno teoretické lemma.

Zatím jsme používali pojmy charakteristický polynom matice, vlastní číslo matice a jeho násobnost apod. Tyto pojmy můžeme přirozeným způsobem přenést na endomorfismy prostorů konečných dimenzí.

Uvažujme endomorfismus vektorového prostoru V nad tělesem T a zvolme nějakou bázi M prostoru V ; nechť A je matice endomorfismu f vzhledem k bázi M . *Anulujícím polynomem, charakteristickým polynomem, minimálním polynomem, vlastním číslem, spektrem* endomorfismu f budeme rozumět po řadě anulující polynom, charakteristický polynom, minimální polynom, vlastní číslo, spektrum matice A . Jestliže je B matice endomorfismu f vzhledem k bázi N , potom jsou matice A , B podobné; definice výše uvedených pojmů tedy nezávisí na volbě báze prostoru V .

Výše uvedené pojmy bychom také mohli definovat přímo. Dosazením endomorfismu f do polynomu

$$p(\lambda) = \lambda^n + a_1 \lambda^{n-1} + \dots + a_{n-1} \lambda + a_n$$

budeme rozumět endomorfismus

$$p(f) = f^n + a_1 f^{n-1} + \dots + a_{n-1} f + a_n 1_V,$$

anulujícím polynomem endomorfismu f budeme rozumět polynom $p(\lambda)$, pro který je endomorfismus $p(f)$ nulový atd. Je zřejmé, že endomorfismus $p(f)$ je nulový právě tehdy, když je matice

$$p(A) = A^n + a_1 A^{n-1} + \dots + a_{n-1} A + a_n E$$

nulová.

Poznamenejme ještě, že pro každé dva polynomy $p(\lambda)$ a $q(\lambda)$ jsou endomorfismy $p(f)$ a $q(f)$ komutující, tj. $p(f)q(f) = q(f)p(f)$.

Podprostor W prostoru V se nazývá *invariantní* vůči endomorfismu f , jestliže je $f(W) \subseteq W$.

19.6. Lemma. *Nechť $p(\lambda)$ je anulující polynom endomorfismu f prostoru V . Jestliže*

$$p(\lambda) = p_1(\lambda)p_2(\lambda) \dots p_k(\lambda)$$

je rozklad polynomu $p(\lambda)$ na navzájem nesoudělné polynomy, potom je

$$V = \text{Ker } p_1(f) \oplus \dots \oplus \text{Ker } p_k(f) \quad (11)$$

direktní rozklad prostoru V na podprostory invariantní vůči endomorfismu f .

Důkaz. Tvrzení dokážeme pro $k = 2$. Protože jsou polynomy $p_1(\lambda)$ a $p_2(\lambda)$ nesoudělné, existují polynomy $q_1(\lambda)$ a $q_2(\lambda)$, takové, že

$$q_1(\lambda) \cdot p_1(\lambda) + q_2(\lambda) \cdot p_2(\lambda) = 1 .$$

Dosadíme-li do této rovnosti za λ endomorfismus f , dostaneme rovnost, která vyjadřuje rozklad identického automorfismu prostoru V na součet dvou endomorfismů:

$$q_1(f)p_1(f) + q_2(f)p_2(f) = 1_V$$

Pro každý vektor $v \in V$ je tedy

$$[q_1(f)p_1(f)](v) + [q_2(f)p_2(f)](v) = v . \quad (12)$$

Protože je $p = p_1p_2$ anulující polynom endomorfismu f , je

$$[p_2(f)q_1(f)p_1(f)](v) = o \quad \text{a} \quad [p_1(f)q_2(f)p_2(f)](v) = o ,$$

takže

$$[q_1(f)p_1(f)](v) \in \text{Ker } p_2(f) \quad \text{a} \quad [q_2(f)p_2(f)](v) \in \text{Ker } p_1(f) .$$

Tedy

$$V = \text{Ker } p_1(f) + \text{Ker } p_2(f) .$$

Jestliže je $v \in \text{Ker } p_1(f) \cap \text{Ker } p_2(f)$, je podle (12) $v = o$ a rovnost (11) je pro $k = 2$ dokázána.

Jestliže $v \in \text{Ker } p_1(f)$, potom

$$[p_1(f)](f(v)) = f[p_1(f)(v)] = f(o) = o ,$$

takže $f(v) \in \text{Ker } p_1(f)$; jestliže $v \in \text{Ker } p_2(f)$, potom

$$[p_2(f)](f(v)) = f[p_2(f)(v)] = f(o) = o ,$$

takže $f(v) \in \text{Ker } p_2(f)$. Jde tedy o direktní rozklad na podprostory, které jsou invariantní vůči f .

Indukcí rozšíříme platnost tvrzení pro libovolné přirozené číslo k (provedení indukce umožňuje invariantnost podprostorů). \square

19.7. Důsledky. Aplikujme nyní předchozí lemma na charakteristický polynom $p(\lambda)$ endomorfismu f prostoru V (tj. na charakteristický polynom matice A), jehož rozklad na navzájem nesoudělné polynomy je uveden v (8). Vzhledem k definici endomorfismů φ_i a rovnostem (10) má direktní rozklad (11) tvar

$$V = \text{Ker } \varphi_1^{r_1} \oplus \cdots \oplus \text{Ker } \varphi_k^{r_k}. \quad (13)$$

Z předchozích úvah vyplývá řada důležitých výsledků:

- (i) *Sjednocení bází B_i podprostorů $\text{Ker } \varphi_i^{r_i}$ je bází prostoru V .*

Toto tvrzení je přímým důsledkem rozkladu (13).

Bázi

$$B = \bigcup_{i=1}^k B_i$$

prostoru V uspořádáme přirozeným způsobem. Nejprve vezmeme vektory báze B_1 , potom vektory báze B_2 atd., nakonec vektory báze B_k ; přitom zachováme výše konstruovaná uspořádání jednotlivých bází B_i . Hovoříme o *Weyrově bází* prostoru V , která přísluší k endomorfismu f .

- (ii) *Násobnost každého vlastního čísla matice A je rovna součtu všech příslušných Weyrových charakteristických čísel, tj.*

$$s_i = \alpha_1^i + \alpha_2^i + \cdots + \alpha_{r_i}^i.$$

Podle (8), (9) a (13) je

$$n = \sum_{i=1}^k s_i \geq \sum_{i=1}^k (\alpha_1^i + \alpha_2^i + \cdots + \alpha_{r_i}^i) = \sum_{i=1}^k \dim \text{Ker } \varphi_i^{r_i} = n.$$

Pro každé $i = 1, \dots, k$ je tedy

$$s_i = \alpha_1^i + \alpha_2^i + \cdots + \alpha_{r_i}^i \geq r_i.$$

- (iii) *Matice endomorfismu f vzhledem k bází B je Jordanovou.*
 (iv) *Jordanův kanonický tvar J matice A je určen vlastními čísly matice A a k nim příslušnými Weyrovými charakteristickými čísly. Transformační matice C , pro kterou je $J = C^{-1}AC$ je určena Weyrovou bází B .*

První části báze B (vektorům z B_1) odpovídá Jordanova matice J_1 řádu s_1 , která má na diagonále vlastní číslo λ_1, \dots , poslední části báze B (vektorům z B_k) odpovídá Jordanova matice J_k řádu s_k , která má na diagonále vlastní číslo λ_k . Maticí endomorfismu f vzhledem k bází B je Jordanova matice J sestavená z bloků

J_1, \dots, J_k ; složení těchto bloků z jednotlivých buněk je určeno příslušnými Weyrovými charakteristickými čísly.

Protože je A maticí endomorfismu f vzhledem ke kanonické bázi a J maticí endomorfismu f vzhledem k bázi B , je

$$J = C^{-1}AC,$$

kde C je matice přechodu od Weyrovy báze B ke kanonické bázi prostoru V ; ve sloupcích matice C jsou tedy přímo vektory báze B . Našli jsme tedy nejen Jordanův kanonický tvar J matice A , ale i transformační matici C , pomocí které se realizuje podobnost matic A a J .

Poznamenejme, že k nalezení Jordanova kanonického tvaru J matice A nemůžeme konstruovat Weyrovu bázi B , neboť matici J umíme napsat ihned, jakmile známe vlastní čísla matice A a k nim příslušná Weyrova charakteristická čísla.

(v) *Polynom*

$$(\lambda - \lambda_1)^{r_1} (\lambda - \lambda_2)^{r_2} \dots (\lambda - \lambda_k)^{r_k}$$

je minimálním polynomem matice A .

Z direktního rozkladu (13) prostoru V vyplývá, že polynom

$$(\lambda - \lambda_1)^{r_1} (\lambda - \lambda_2)^{r_2} \dots (\lambda - \lambda_k)^{r_k}$$

je anulujícím polynomem endomorfismu f . Libovolný vektor $v \in V$ je podle (13) možno zapsat jako součet vektorů $v_i \in \text{Ker } \varphi^{r_i}$, $i = 1, \dots, k$ a každý vektor v_i je anulován endomorfismem

$$\varphi^{r_i} = (f - \lambda_i \cdot 1_V)^{r_i}.$$

Minimální polynom matice A (resp. endomorfismu f) je tedy určen vlastními čísly λ_i matice A a počty r_i k nim příslušných Weyrových charakteristických čísel.

(vi) *Dvě matice jsou podobné právě tehdy, když mají stejná vlastní čísla a stejná Weyrova charakteristická čísla. Vlastní čísla a Weyrova charakteristická čísla tvoří úplnou soustavu invariantů podobnosti matic.*

System

$$\begin{aligned} \lambda_1 &; \alpha_1^1, \dots, \alpha_{r_1}^1; \\ \lambda_2 &; \alpha_1^2, \dots, \alpha_{r_2}^2; \\ &\dots\dots\dots \\ \lambda_k &; \alpha_1^k, \dots, \alpha_{r_k}^k \end{aligned}$$

se někdy nazývá *Weyrova charakteristika* matice A .

V následujících příkladech ukážeme, že předchozí teorii můžeme použít i pro reálné matice; chápeme je jako matice komplexní, vše se však děje v reálném oboru. Rovněž ukážeme dvě možnosti nalezení Weyrovy báze.

19.8. Příklady.

(i) Uvažujme reálnou matici

$$A = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 3 & 0 & 3 & -3 \\ 4 & -1 & 3 & -3 \end{pmatrix}$$

z příkladu 18.25(iv). Standardním způsobem vypočteme, že charakteristickým polynomem matice A je λ^4 , matice A má tedy čtyřnásobné vlastní číslo 0. Označme symbolem f endomorfismus prostoru $V = \mathbb{C}^4$, jehož maticí vzhledem ke kanonické bázi prostoru V je matice A , položme dále $\varphi = f - 0 \cdot 1_V = f$; maticí endomorfismu φ je matice $A - 0 \cdot E = A$. Snadno zjistíme, že $A^2 = O$. Je tedy

$$\lambda = 0, \quad r = 2,$$

$$\alpha_1 = 4 - r(A) = 2, \quad \alpha_2 = r(A) - r(A^2) = 2,$$

$$s = \alpha_1 + \alpha_2 = 4.$$

V Jordanově kanonickém tvaru J matice A jsou tedy dvě ($\alpha_2 = 2$) buňky řádu 2 (a $\alpha_1 - \alpha_2 = 0$ buněk řádu 1), tj.

$$J = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Nyní najdeme Weyrovu bázi B prostoru V . Hledáme vektory v_1, v_2, v_3, v_4 , pro které je

$$\varphi(v_1) = v_2, \quad \varphi(v_2) = o, \quad \varphi(v_3) = v_4, \quad \varphi(v_4) = o;$$

tyto vztahy jsou dány Weyrovými charakteristickými čísly příslušnými k vlastnímu číslu 0, jsou však rovněž ihned vidět z matice J , která je maticí endomorfismu φ vzhledem k bázi $B = \{v_1, v_2, v_3, v_4\}$. Ukážeme dva postupy výpočtu vektorů v_1, v_2, v_3, v_4 .

a) Snadno nalezneme vektory v_2, v_4 , které generují podprostor $\text{Im } \varphi \cap \text{Ker } \varphi$; položíme např.

$$v_2 = (0, 0, 1, 1), \quad v_4 = (1, 1, -1, 0)$$

a najdeme jejich vzory v_1, v_3 při endomorfismu φ . Vektor v_1 , resp. v_3 je řešením soustavy lineárních rovnic s maticí A a pravou stranou v_2 , resp. v_4 . Tedy

$$v_1 = \left(0, 0, \frac{1}{6}, -\frac{1}{6}\right), \quad v_3 = \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{3}\right).$$

Nakonec můžeme zvolit vhodný násobek těchto vektorů a položit

$$B = \{ (0, 0, 1, -1), (0, 0, 6, 6), (3, -3, -3, 2), (6, 6, -6, 0) \}.$$

Jestliže je

$$C = \begin{pmatrix} 0 & 0 & 3 & 6 \\ 0 & 0 & -3 & 6 \\ 1 & 6 & -3 & -6 \\ -1 & 6 & 2 & 0 \end{pmatrix},$$

je $J = C^{-1}AC$.

b) Můžeme zvolit dva lineárně nezávislé vektory, které neleží v $\text{Ker } \varphi$ (ale leží v $\text{Ker } \varphi^2$), např.

$$v_1 = (1, 0, 0, 0), \quad v_3 = (0, 0, 0, 1).$$

Obrazy těchto vektorů při endomorfismu φ jsou

$$v_2 = (1, 1, 3, 4), \quad v_4 = (0, 0, -3, -3);$$

získáme je tak, že vektory v_1, v_3 vynásobíme maticí A zleva. Nyní položíme

$$B = \{ (1, 0, 0, 0), (1, 1, 3, 4), (0, 0, 0, 1), (0, 0, -3, -3) \};$$

pro matici

$$C = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & -3 \\ 0 & 4 & 1 & -3 \end{pmatrix}$$

je $J = C^{-1}AC$.

(ii) Uvažujme reálnou matici

$$A = \begin{pmatrix} -7 & -12 & 0 & 0 \\ 3 & 5 & 0 & 0 \\ 0 & 1 & -5 & -8 \\ 0 & 0 & 2 & 3 \end{pmatrix}$$

z příkladu 18.36(i). Standardním způsobem vypočteme, že charakteristickým polynomem matice A je $(\lambda + 1)^4$, matice A má tedy čtyřnásobné vlastní číslo -1 . Označme symbolem f endomorfismus prostoru $V = \mathbb{C}^4$, jehož maticí vzhledem ke kanonické bázi prostoru V je matice A , položme dále $\varphi = f + 1 \cdot 1_V$; maticí endomorfismu φ je matice $A + E$. Snadno zjistíme, že

$$A + E = \begin{pmatrix} -6 & -12 & 0 & 0 \\ 3 & 6 & 0 & 0 \\ 0 & 1 & -4 & -8 \\ 0 & 0 & 2 & 4 \end{pmatrix}, \quad (A + E)^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix},$$

$$(A + E)^3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -12 & -24 & 0 & 0 \\ 6 & 12 & 0 & 0 \end{pmatrix}, \quad (A + E)^4 = O.$$

Je tedy

$$\lambda = -1, \quad r = 4,$$

$$\begin{aligned} \alpha_1 &= 4 - r(A + E) = 1, & \alpha_2 &= r(A + E) - r(A + E)^2 = 1, \\ \alpha_3 &= r(A + E)^2 - r(A + E)^3 = 1, & \alpha_4 &= r(A + E)^3 - r(A + E)^4 = 1, \end{aligned}$$

$$s = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 4.$$

V Jordanově kanonickém tvaru J matice A je tedy jedna ($\alpha_4 = 1$) buňka řádu 4 (a $\alpha_1 - \alpha_2 = 0$ buněk řádu 1, $\alpha_2 - \alpha_3 = 0$ buněk řádu 2, $\alpha_3 - \alpha_4 = 0$ buněk řádu 3), tj.

$$J = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Nyní najdeme Weyrovu bázi B prostoru V . Hledáme vektory v_1, v_2, v_3, v_4 , pro které je

$$\varphi(v_1) = v_2, \quad \varphi(v_2) = v_3, \quad \varphi(v_3) = v_4, \quad \varphi(v_4) = o;$$

tyto vztahy jsou dány Weyrovými charakteristickými čísly příslušnými k vlastnímu číslu -1 matice A , jsou však rovněž ihned vidět z Jordanovy matice $J + E$, která je maticí endomorfismu φ vzhledem k bázi $B = \{v_1, v_2, v_3, v_4\}$. Opět ukážeme dva způsoby výpočtu vektorů v_1, v_2, v_3, v_4 .

a) Vektor $v_4 \in \text{Im } \varphi^3 \cap \text{Ker } \varphi$ je vlastní vektor matice A (příslušný k vlastnímu číslu -1), tj. v_4 je řešením homogenní soustavy lineárních rovnic s maticí $A + E$. Tedy např.

$$v_4 = (0, 0, -2, 1).$$

Nyní najdeme vzor vektoru v_4 při endomorfismu φ a označíme ho v_3 , najdeme vzor vektoru v_3 při endomorfismu φ a označíme ho v_2 , najdeme vzor vektoru v_2

při endomorfismu φ a označíme ho v_1 . Vektor v_3 je řešením soustavy lineárních rovnic s maticí $A + E$ a pravou stranou v_4 , vektor v_2 je řešením soustavy lineárních rovnic s maticí $A + E$ a pravou stranou v_3 , vektor v_1 je řešením soustavy lineárních rovnic s maticí $A + E$ a pravou stranou v_2 . Tedy

$$v_3 = \left(0, 0, \frac{1}{2}, 0 \right), \quad v_2 = \left(-1, \frac{1}{2}, 0, 0 \right), \quad v_1 = \left(\frac{1}{6}, 0, 0, 0 \right).$$

Nyní můžeme tyto vektory nahradit jejich šestinásobky a položit

$$B = \{ (1, 0, 0, 0), (-6, 3, 0, 0), (0, 0, 3, 0), (0, 0, -12, 6) \}.$$

Snadno se přesvědčíme, že pro matici

$$C = \begin{pmatrix} 1 & -6 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & -12 \\ 0 & 0 & 0 & 6 \end{pmatrix}$$

je $J = C^{-1}AC$.

b) Vektor v_1 zvolíme v doplňku podprostoru $\text{Ker } \varphi^3$ do $\text{Ker } \varphi^4 = V$, např.

$$v_1 = (1, 0, 0, 0).$$

Vektory v_2, v_3, v_4 získáme jako obrazy vektoru v_1 při endomorfismech $\varphi, \varphi^2, \varphi^3$, resp. postupným násobením vektoru v_1 maticí $A + E$ zleva. Tedy

$$v_2 = (-6, 3, 0, 0), \quad v_3 = (0, 0, 3, 0), \quad v_4 = (0, 0, -12, 6).$$

Dostali jsme stejný výsledek jako v předchozím případě. Jinou volbou vektoru v_1 (např. $(0, 1, 0, 0)$, $(1, 1, 0, 0)$ apod.) bychom získali jinou bázi B a jinou transformační matici C .

(iii) Uvažujme reálnou matici

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

z příkladu 18.25(v). Standardním způsobem vypočteme, že charakteristickým polynomem matice A je $(\lambda - 2)^3$, matice A má tedy trojnásobné vlastní číslo 2. Označme symbolem f endomorfismus prostoru $V = \mathbb{C}^3$, jehož maticí vzhledem ke kanonické bázi prostoru V je matice A , položme dále $\varphi = f - 2 \cdot 1_V$; maticí endomorfismu φ je matice $A - 2E$. Snadno zjistíme, že

$$A - 2E = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & -1 \end{pmatrix}, \quad (A - 2E)^2 = O.$$

Je tedy

$$\begin{aligned}\lambda &= 2, & r &= 2, \\ \alpha_1 &= 3 - r(A - 2E) = 2, & \alpha_2 &= r(A - 2E) - r(A - 2E)^2 = 1, \\ s &= \alpha_1 + \alpha_2 = 3.\end{aligned}$$

V Jordanově kanonickém tvaru J matice A je tedy jedna ($\alpha_2 = 1$) buňka řádu 2 a jedna ($\alpha_1 - \alpha_2 = 1$) buňka řádu 1, tj.

$$J = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Nyní najdeme Weyrovu bázi B prostoru V . Hledáme vektory v_1, v_2, v_3 , pro které je

$$\varphi(v_1) = v_2, \quad \varphi(v_2) = o, \quad \varphi(v_3) = o;$$

tyto vztahy jsou dány Weyrovými charakteristickými čísly příslušnými k vlastnímu číslu 2 matice A , jsou však rovněž ihned vidět z Jordanovy matice $J - 2E$, která je maticí endomorfismu φ vzhledem k bázi $B = \{v_1, v_2, v_3\}$. Opět ukážeme dva způsoby výpočtu vektorů v_1, v_2, v_3 .

a) Lineárně nezávislé vektory $v_2 \in \text{Im } \varphi \cap \text{Ker } \varphi$ a $v_3 \in \text{Ker } \varphi$ jsou vlastní vektory matice A (příslušné k vlastnímu číslu 2). Vlastními vektory matice A jsou všechny nenulové vektory podprostoru $[(0, 1, 1), (1, 0, 1)]$. Za vektor v_2 můžeme zvolit pouze násobky vektoru $(1, 0, 1) \in \text{Im } \varphi$; tedy $v_2 = (1, 0, 1)$. Vektor v_1 je řešením soustavy lineárních rovnic s maticí $A - 2E$ a pravou stranou v_2 ; zvolme např. $v_1 = (0, 1, 0)$. Weyrovou bázi je tedy např. báze

$$B = \{ (0, 1, 0), (1, 0, 1), (0, 1, 1) \},$$

které odpovídá transformační matice

$$C = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

b) Zvolíme vektor $v_1 \in \text{Ker } \varphi^2 \setminus \text{Ker } \varphi$, např.

$$v_1 = (1, 0, 0).$$

Vektor $v_2 = \varphi(v_1)$ získáme vynásobením vektoru v_1 maticí $A - 2E$, tj. $v_2 = (1, 0, 1)$. Vektor v_2 leží v $\text{Ker } \varphi$; vektor v_3 musí rovněž ležet v $\text{Ker } \varphi$ a v_2, v_3 musí být lineárně nezávislé. Zvolíme tedy např. $v_3 = (1, -1, 0)$. Odtud

$$B = \{ (1, 0, 0), (1, 0, 1), (1, -1, 0) \};$$

pro matici

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

je $J = C^{-1}AC$.

(iv) Uvažujme reálnou matici

$$A = \begin{pmatrix} 3 & -4 & 0 & 0 \\ 4 & -5 & -2 & 4 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 2 & -1 \end{pmatrix}$$

z příkladu 18.25(vii). Standardním způsobem vypočteme, že charakteristickým polynomem matice A je $(\lambda - 1)^2(\lambda + 1)^2$, matice A má tedy dvojnásobné vlastní číslo 1 a dvojnásobné vlastní číslo -1 . Označme symbolem f endomorfismus prostoru $V = \mathbb{C}^4$, jehož maticí vzhledem ke kanonické bázi prostoru V je matice A , položme dále $\varphi_1 = f - 1 \cdot 1_V$ a $\varphi_2 = f + 1 \cdot 1_V$; maticí endomorfismu φ_1 je matice $A - E$ a maticí endomorfismu φ_2 je matice $A + E$ (vzhledem ke kanonické bázi). Snadno zjistíme, že

$$A - E = \begin{pmatrix} 2 & -4 & 0 & 0 \\ 4 & -6 & -2 & 4 \\ 0 & 0 & 2 & -2 \\ 0 & 0 & 2 & -2 \end{pmatrix}, \quad (A - E)^2 = \begin{pmatrix} -12 & 16 & 8 & -16 \\ -16 & 20 & 16 & -28 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$(A - E)^3 = \begin{pmatrix} 40 & -48 & -48 & 80 \\ 48 & -56 & -64 & 104 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix};$$

$$A + E = \begin{pmatrix} 4 & -4 & 0 & 0 \\ 4 & -4 & -2 & 4 \\ 0 & 0 & 4 & -2 \\ 0 & 0 & 2 & 0 \end{pmatrix}, \quad (A + E)^2 = \begin{pmatrix} 0 & 0 & 8 & -16 \\ 0 & 0 & 8 & -12 \\ 0 & 0 & 12 & -8 \\ 0 & 0 & 8 & -4 \end{pmatrix},$$

$$(A + E)^3 = \begin{pmatrix} 0 & 0 & 0 & -16 \\ 0 & 0 & 8 & -16 \\ 0 & 0 & 32 & -24 \\ 0 & 0 & 24 & -16 \end{pmatrix}.$$

Je tedy

$$\begin{aligned}\lambda_1 &= 1, & r_1 &= 2, \\ \alpha_1^1 &= 4 - r(A - E) = 1, & \alpha_2^1 &= r(A - E) - r(A - E)^2 = 1, \\ s_1 &= \alpha_1^1 + \alpha_2^1 = 2;\end{aligned}$$

$$\begin{aligned}\lambda_2 &= -1, & r_2 &= 2, \\ \alpha_1^2 &= 4 - r(A + E) = 1, & \alpha_2^2 &= r(A + E) - r(A + E)^2 = 1, \\ s_2 &= \alpha_1^2 + \alpha_2^2 = 2.\end{aligned}$$

V Jordanově kanonickém tvaru J matice A je tedy jedna buňka řádu 2, která odpovídá vlastnímu číslu $\lambda_1 = 1$, a jedna buňka řádu 2, která odpovídá vlastnímu číslu $\lambda_2 = -1$. Tedy

$$J = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Nyní najdeme Weyrovu bázi B prostoru V . Hledáme vektory v_1, v_2, v_3, v_4 , pro které je

$$\varphi_1(v_1) = v_2, \quad \varphi_1(v_2) = o, \quad \varphi_2(v_3) = v_4, \quad \varphi_2(v_4) = o;$$

tyto vztahy jsou dány Weyrovými charakteristickými čísly příslušnými k vlastním číslům 1 a -1 . Opět ukážeme dva postupy výpočtu vektorů v_1, v_2, v_3, v_4 .

a) Vektor v_2 je vlastním vektorem matice A (příslušným k vlastnímu číslu 1), tj. vektor v_2 je řešením homogenní soustavy lineárních rovnic s maticí $A - E$. Tedy např.

$$v_2 = (-4, -2, 2, 2).$$

Nyní najdeme vzor vektoru v_2 při endomorfismu φ_1 a označíme ho v_1 , vektor v_1 je řešením soustavy lineárních rovnic s maticí $A - E$ a pravou stranou v_2 . Tedy

$$v_1 = (6, 4, 1, 0).$$

Vektor v_4 je vlastním vektorem matice A (příslušným k vlastnímu číslu -1), tj. vektor v_4 je řešením homogenní soustavy lineárních rovnic s maticí $A + E$. Tedy např.

$$v_4 = (4, 4, 0, 0).$$

Nyní najdeme vzor vektoru v_4 při endomorfismu φ_2 a označíme ho v_3 , vektor v_3 je řešením soustavy lineárních rovnic s maticí $A + E$ a pravou stranou v_4 . Tedy

$$v_3 = (1, 0, 0, 0).$$

Za Weyrovu bázi tedy vezmeme bázi

$$B = \{ (6, 4, 1, 0), (-4, -2, 2, 2), (1, 0, 0, 0), (4, 4, 0, 0) \}.$$

Snadno se přesvědčíme, že pro matici

$$C = \begin{pmatrix} 6 & -4 & 1 & 4 \\ 4 & -2 & 0 & 4 \\ 1 & 2 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}$$

je $J = C^{-1}AC$.

b) Zvolíme vektor $v_1 \in \text{Ker } \varphi_1^2 \setminus \text{Ker } \varphi_1$, např.

$$v_1 = (2, 0, -5, -4).$$

Obrazem tohoto vektoru při endomorfismu φ_1 je vektor

$$v_3 = (4, 2, -2, -2),$$

získáme ho vynásobením vektoru v_1 maticí $A - E$ zleva.

Zvolíme dále vektor $v_3 \in \text{Ker } \varphi_2^2 \setminus \text{Ker } \varphi_2$, např.

$$v_3 = (0, 1, 0, 0).$$

Obrazem tohoto vektoru při endomorfismu φ_2 je vektor

$$v_4 = (-4, -4, 0, 0),$$

získáme ho vynásobením vektoru v_3 maticí $A + E$ zleva. Za Weyrovu bázi tedy můžeme vzít bázi

$$B = \{ (2, 0, -5, -4), (4, 2, -2, -2), (0, 1, 0, 0), (-4, -4, 0, 0) \}.$$

Odpovídající transformační maticí je matice

$$C = \begin{pmatrix} 2 & 4 & 0 & -4 \\ 0 & 2 & 1 & -4 \\ -5 & -2 & 0 & 0 \\ -4 & -2 & 0 & 0 \end{pmatrix}.$$

(v) Uvažujme reálnou matici

$$A = \begin{pmatrix} 0 & -1 & 1 & -1 \\ 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Charakteristickým polynomem matice A je polynom $(\lambda - i)^2(\lambda + i)^2$, matice A má dvojnásobné vlastní číslo i a dvojnásobné vlastní číslo $-i$. Snadno zjistíme, že

$$A - iE = \begin{pmatrix} -i & -1 & 1 & -1 \\ 1 & -i & 1 & -1 \\ 0 & 0 & -i & -1 \\ 0 & 0 & 1 & -i \end{pmatrix}, \quad (A - iE)^2 = \begin{pmatrix} -2 & 2i & -2 - 2i & 2i \\ -2i & -2 & -2i & -2 + 2i \\ 0 & 0 & -2 & 2i \\ 0 & 0 & -2i & -2 \end{pmatrix},$$

$$A + iE = \begin{pmatrix} i & -1 & 1 & -1 \\ 1 & i & 1 & -1 \\ 0 & 0 & i & -1 \\ 0 & 0 & 1 & i \end{pmatrix}, \quad (A + iE)^2 = \begin{pmatrix} -2 & -2i & -2 + 2i & -2i \\ 2i & -2 & 2i & -2 - 2i \\ 0 & 0 & -2 & -2i \\ 0 & 0 & 2i & -2 \end{pmatrix},$$

Tedy

$$\begin{aligned} \lambda_1 &= i, & r_1 &= 2, \\ \alpha_1^1 &= 1, & \alpha_2^1 &= 1, \\ s_1 &= 2; \end{aligned}$$

$$\begin{aligned} \lambda_2 &= -i, & r_2 &= 2, \\ \alpha_1^2 &= 1, & \alpha_2^2 &= 1, \\ s_2 &= 2. \end{aligned}$$

Jordanovým kanonickým tvarem J matice A je

$$J = \begin{pmatrix} i & 0 & 0 & 0 \\ 1 & i & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & 0 & 1 & -i \end{pmatrix}.$$

Nyní najdeme Weyrovu bázi $B = \{v_1, v_2, v_3, v_4\}$. Vektor v_1 má být řešením homogenní soustavy s maticí $(A - iE)^2$, ale nesmí být řešením homogenní soustavy s maticí $A - iE$; vektor v_2 dostaneme vynásobením vektoru v_1 maticí $A - iE$.

Vektor v_3 má být řešením homogenní soustavy s maticí $(A + iE)^2$, ale nesmí být řešením homogenní soustavy s maticí $A + iE$; vektor v_4 dostaneme vynásobením vektoru v_3 maticí $A + iE$.

Tedy

$$B = \{ (1, 0, i, 1), (-1, i, 0, 0), (1, 0, -i, 1), (-1, -i, 0, 0) \}.$$

Pro matici

$$C = \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & i & 0 & -i \\ i & 0 & -i & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

je $J = C^{-1}AC$.

Řešení soustavy lineárních diferenciálních rovnic $z' = Jz$, jejíž matice J je Jordanova, snadno určíme. Tato soustava se rozpadne na menší soustavy, které odpovídají jednotlivým Jordanovým buňkám, a ty se snadno vyřeší. Např. soustava

$$\begin{aligned} z'_1 &= rz_1 \quad , \\ z'_2 &= z_1 + rz_2 \quad , \\ z'_3 &= z_2 + rz_3 \quad , \\ z'_4 &= z_3 + rz_4 \quad , \end{aligned}$$

která odpovídá Jordanově buňce

$$\begin{pmatrix} r & 0 & 0 & 0 \\ 1 & r & 0 & 0 \\ 0 & 1 & r & 0 \\ 0 & 0 & 1 & r \end{pmatrix} ,$$

má řešení

$$\begin{aligned} z_1 &= a \cdot e^{rx} \quad , \\ z_2 &= (ax + b) \cdot e^{rx} \quad , \\ z_3 &= \left(\frac{1}{2}ax^2 + bx + c \right) \cdot e^{rx} \quad , \\ z_4 &= \left(\frac{1}{6}ax^3 + \frac{1}{2}bx^2 + cx + d \right) \cdot e^{rx} \quad , \end{aligned}$$

kde konstanty $a, b, c, d \in \mathbb{R}$ můžeme volit libovolně. Řešení soustavy $z' = Jz$ získáme jako souhrn řešení jednotlivých menších soustav odpovídajících jednotlivým Jordanovým buňkám; konstanty, které jsou v dílčích řešeních, je přitom třeba volit nezávisle na sobě. Řešení původní soustavy $y' = Ay$ pak snadno získáme z řešení soustavy $z' = Jz$ pomocí vztahu $z^T = C^{-1} \cdot y^T$, neboli

$$y^T = C \cdot z^T .$$

20.2. Příklady.

(i) Řešme následující soustavu lineárních diferenciálních rovnic:

$$\begin{aligned} y'_1 &= y_2 \quad , \\ y'_2 &= y_3 \quad , \\ y'_3 &= y_1 - 3y_2 + 3y_3 \quad . \end{aligned}$$

Matici A dané soustavy $y' = Ay$ převedeme na Jordanův kanonický tvar J a najdeme nějakou transformační matici C , pro kterou je $J = C^{-1}AC$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 3 & -1 \\ 2 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 1 \\ 4 & 3 & 1 \end{pmatrix}$$

Nyní vyřešíme soustavu lineárních diferenciálních rovnic $z' = Jz$:

$$\begin{aligned} z'_1 &= z_1, \\ z'_2 &= z_1 + z_2, \\ z'_3 &= z_2 + z_3. \end{aligned}$$

Řešením této soustavy je

$$z_1 = a \cdot e^x, \quad z_2 = (ax + b) \cdot e^x, \quad z_3 = \left(\frac{1}{2}ax^2 + bx + c\right) \cdot e^x.$$

Řešení původní soustavy $y' = Ay$ nyní snadno získáme pomocí matice C ze vztahu $y^T = C \cdot z^T$:

$$\begin{aligned} y_1 &= \left[a \left(\frac{1}{2}x^2 + x + 1 \right) + b(x + 1) + c \right] \cdot e^x, \\ y_2 &= \left[a \left(\frac{1}{2}x^2 + 2x + 2 \right) + b(x + 2) + c \right] \cdot e^x, \\ y_3 &= \left[a \left(\frac{1}{2}x^2 + 3x + 4 \right) + b(x + 3) + c \right] \cdot e^x. \end{aligned}$$

Množinu všech řešení dané soustavy můžeme zapsat jako vektorový prostor

$$\left[\left(\frac{1}{2}x^2 + x + 1, \frac{1}{2}x^2 + 2x + 2, \frac{1}{2}x^2 + 3x + 4 \right) \cdot e^x, (x + 1, x + 2, x + 3) \cdot e^x, (1, 1, 1) \cdot e^x \right];$$

výše uvedené obecné řešení (y_1, y_2, y_3) je lineární kombinací prvků báze tohoto prostoru s koeficienty a, b, c . Báze prostoru všech řešení dané soustavy se nazývá *fundamentální systém*.

(ii) Řešme následující soustavu lineárních diferenciálních rovnic:

$$\begin{aligned} y'_1 &= 3y_1 - y_2, \\ y'_2 &= y_1 + y_2, \\ y'_3 &= 3y_1 + 5y_3 - 3y_4, \\ y'_4 &= 4y_1 - y_2 + 3y_3 - y_4. \end{aligned}$$

Matici A dané soustavy $y' = Ay$ převedeme na Jordanův kanonický tvar J a najdeme nějakou transformační matici C , pro kterou je $J = C^{-1}AC$:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & -1 \\ -\frac{1}{3} & 0 & 0 & \frac{1}{3} \\ 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 3 & 0 & 5 & -3 \\ 4 & -1 & 3 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 3 & 0 & 0 \\ 0 & 3 & 1 & 1 \end{pmatrix}$$

Nyní vyřešíme soustavu lineárních diferenciálních rovnic $z' = Jz$:

$$\begin{aligned} z_1' &= 2z_1, \\ z_2' &= z_1 + 2z_2, \\ z_3' &= 2z_3, \\ z_4' &= z_3 + 2z_4. \end{aligned}$$

Řešením této soustavy je

$$z_1 = a \cdot e^{2x}, \quad z_2 = (ax + b) \cdot e^{2x}, \quad z_3 = c \cdot e^{2x}, \quad z_4 = (cx + d) \cdot e^{2x}.$$

Řešení původní soustavy $y' = Ay$ nyní snadno získáme pomocí matice C ze vztahu $y^T = C \cdot z^T$:

$$\begin{aligned} y_1 &= [c(x+1) + d] \cdot e^{2x}, \\ y_2 &= [cx + d] \cdot e^{2x}, \\ y_3 &= [a(3x+1) + 3b] \cdot e^{2x}, \\ y_4 &= [3ax + 3b + c(x+1) + d] \cdot e^{2x}. \end{aligned}$$

Množinu všech řešení dané soustavy můžeme zapsat jako vektorový prostor

$$\left[(0, 0, 3x+1, 3x) \cdot e^{2x}, (0, 0, 3, 3) \cdot e^{2x}, (x+1, x, 0, x+1) \cdot e^{2x}, (1, 1, 0, 1) \cdot e^{2x} \right];$$

výše uvedené řešení (y_1, y_2, y_3, y_4) je lineární kombinací (s koeficienty a, b, c, d) prvků báze tohoto prostoru, tj. lineární kombinací nalezeného fundamentálního systému.

(iii) Řešte následující soustavu lineárních diferenciálních rovnic:

$$\begin{aligned} y_1' &= -2y_2 + 2y_3, \\ y_2' &= -y_1 + y_2 - y_3 + 2y_4, \\ y_3' &= y_1 + y_2 - y_3 - 2y_4, \\ y_4' &= -y_2 + y_3. \end{aligned}$$

Matici A dané soustavy $y' = Ay$ převedeme na Jordanův kanonický tvar J a najdeme nějakou transformační matici C , pro kterou je $J = C^{-1}AC$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \\ = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 1 \\ 1 & 0 & 0 & -2 \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 & 2 & 0 \\ -1 & 1 & -1 & 2 \\ 1 & 1 & -1 & -2 \\ 0 & -1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & 0 & 4 \\ 1 & 1 & -1 & -2 \\ 1 & 1 & 1 & -2 \\ 0 & -1 & 0 & 2 \end{pmatrix}$$

Nyní vyřešíme soustavu lineárních diferenciálních rovnic $z' = Jz$:

$$\begin{aligned} z'_1 &= 0, \\ z'_2 &= 0, \\ z'_3 &= z_2, \\ z'_4 &= z_3. \end{aligned}$$

Řešením této soustavy jsou funkce

$$z_1 = a, \quad z_2 = b, \quad z_3 = bx + c, \quad z_4 = \frac{1}{2}bx^2 + cx + d.$$

Řešení původní soustavy $y' = Ay$ nyní snadno získáme pomocí matice C ze vztahu $y^T = C \cdot z^T$:

$$\begin{aligned} y_1 &= b(2x^2 - 1) + 4cx + 4d, \\ y_2 &= a + b(-x^2 - x + 1) + c(-2x - 1) - 2d, \\ y_3 &= a + b(-x^2 + x + 1) + c(-2x + 1) - 2d, \\ y_4 &= b(x^2 - 1) + 2cx + 2d. \end{aligned}$$

Množinu všech řešení dané soustavy můžeme vyjádřit jako vektorový prostor

$$\left[(0, 1, 1, 0), (2x^2 - 1, -x^2 - x + 1, -x^2 + x + 1, x^2 - 1), \right. \\ \left. (4x, -2x - 1, -2x + 1, 2x), (4, -2, -2, 2) \right];$$

výše uvedené obecné řešení (y_1, y_2, y_3, y_4) je lineární kombinací prvků báze tohoto prostoru (fundamentálního systému).

(iv) Řešme následující soustavu lineárních diferenciálních rovnic:

$$\begin{aligned}y_1' &= -y_2, \\y_2' &= y_1, \\y_3' &= y_2 - y_4, \\y_4' &= y_3.\end{aligned}$$

Matici A dané soustavy $y' = Ay$ převedeme na Jordanův kanonický tvar J a najdeme nějakou transformační matici C , pro kterou je $J = C^{-1}AC$; protože v reálném oboru Jordanův kanonický tvar matice A neexistuje, budeme pracovat v komplexním oboru:

$$\begin{aligned}& \begin{pmatrix} i & 0 & 0 & 0 \\ 1 & i & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & 0 & 1 & -i \end{pmatrix} = \\&= \frac{1}{4} \begin{pmatrix} -1 & -i & 0 & 0 \\ -i & 0 & -2i & 2 \\ 1 & -i & 0 & 0 \\ -i & 0 & -2i & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 & 2 & 0 \\ 2i & 0 & 2i & 0 \\ 1 & i & -1 & i \\ 0 & 1 & 0 & -1 \end{pmatrix}\end{aligned}$$

Nyní vyřešíme soustavu lineárních diferenciálních rovnic $z' = Jz$:

$$\begin{aligned}z_1' &= iz_1, \\z_2' &= z_1 + iz_2, \\z_3' &= -iz_3, \\z_4' &= z_3 - iz_4.\end{aligned}$$

Řešením této soustavy jsou komplexní funkce

$$z_1 = a \cdot e^{ix}, \quad z_2 = (ax + b) \cdot e^{ix}, \quad z_3 = c \cdot e^{-ix}, \quad z_4 = (cx + d) \cdot e^{-ix}.$$

Obecné řešení $\{(w_1, w_2, w_3, w_4)\}$ původní soustavy $y' = Ay$ získáme pomocí matice C ze vztahu $y^T = C \cdot z^T$:

$$\begin{aligned}w_1 &= -2a \cdot e^{ix} + 2c \cdot e^{-ix}, \\w_2 &= 2i \cdot a \cdot e^{ix} + 2i \cdot c \cdot e^{-ix}, \\w_3 &= a \cdot e^{ix} + i \cdot (ax + b) \cdot e^{ix} - c \cdot e^{-ix} + i \cdot (cx + d) \cdot e^{-ix}, \\w_4 &= (ax + b) \cdot e^{ix} - (cx + d) \cdot e^{-ix}.\end{aligned}$$

Množina všech řešení může být zapsána jako vektorový prostor

$$\left[(-2, 2i, ix + 1, x) \cdot e^{ix}, (0, 0, i, 1) \cdot e^{ix}, (2, 2i, ix - 1, -x) \cdot e^{-ix}, (0, 0, i, -1) \cdot e^{-ix} \right];$$

obecné řešení (w_1, w_2, w_3, w_4) je lineární kombinací prvků báze tohoto prostoru, tj. prvků fundamentálního systému.

Reálná řešení původní soustavy můžeme získat tak, že vytvoříme vhodné násobky součtu prvního a třetího, resp. druhého a čtvrtého prvku předchozího fundamentálního systému a vhodné násobky rozdílu prvního a třetího, resp. druhého a čtvrtého prvku předchozího fundamentálního systému (připomeňme ještě, že $e^{\pm ix} = \cos x \pm i \sin x$). Množina všech reálných řešení tedy může být zapsána v tvaru

$$\left[(-2 \sin x, 2 \cos x, \sin x + x \cos x, x \sin x), (0, 0, \cos x, \sin x), \right. \\ \left. (-2 \cos x, -2 \sin x, \cos x - x \sin x, x \cos x), (0, 0, -\sin x, \cos x) \right].$$

Obecné řešení můžeme zapsat v tvaru:

$$y_1 = -2A \cdot \sin x - 2C \cdot \cos x, \\ y_2 = 2A \cdot \cos x - 2C \cdot \sin x, \\ y_3 = (Ax + B + C) \cdot \cos x - (Cx - A + D) \cdot \sin x, \\ y_4 = (Cx + D) \cdot \cos x + (Ax + B) \cdot \sin x.$$

V následujících odstavcích se na problematiku soustav homogenních lineárních diferenciálních rovnic podíváme trochu z jiného úhlu a ukážeme další možnost řešení.

20.3. Věta. *Nechť*

$$y'_1 = a_{11}y_1 + \cdots + a_{1n}y_n, \\ y'_2 = a_{21}y_1 + \cdots + a_{2n}y_n, \\ \dots\dots\dots \\ y'_n = a_{n1}y_1 + \cdots + a_{nn}y_n$$

je soustava homogenních lineárních diferenciálních rovnic s konstantními koeficienty v reálném oboru. Potom platí:

- (i) *Soustava má netriviální řešení $(c_1 e^{rx}, c_2 e^{rx}, \dots, c_n e^{rx})$ právě tehdy, když je r vlastním číslem matice soustavy a (c_1, \dots, c_n) příslušným vlastním vektorem.*
- (ii) *Jsou-li r_1, \dots, r_k navzájem různá vlastní čísla matice soustavy, potom příslušná řešení jsou lineárně nezávislá.*

- (iii) Jestliže r je k -násobným vlastním číslem matice soustavy, potom existuje k lineárně nezávislých řešení

$$\begin{aligned} & (p_{10}(x)e^{rx}, \dots, p_{n0}(x)e^{rx}), \\ & (p_{11}(x)e^{rx}, \dots, p_{n1}(x)e^{rx}), \\ & \dots\dots\dots \\ & (p_{1,k-1}(x)e^{rx}, \dots, p_{n,k-1}(x)e^{rx}), \end{aligned}$$

kde pro každé $i = 1, \dots, n$ a $j = 0, \dots, k-1$ je $p_{ij}(x)$ polynom stupně nejvýše j .

Důkaz. Označme $A = (a_{ij})$ matici soustavy.

- (i) Uvedená n -tice funkcí je netriviálním řešením dané soustavy právě tehdy, když je

$$\begin{aligned} rc_1e^{rx} &= a_{11}c_1e^{rx} + \dots + a_{1n}c_ne^{rx}, \\ rc_2e^{rx} &= a_{21}c_1e^{rx} + \dots + a_{2n}c_ne^{rx}, \\ & \dots\dots\dots \\ rc_ne^{rx} &= a_{n1}c_1e^{rx} + \dots + a_{nn}c_ne^{rx}, \end{aligned}$$

v maticovém tvaru

$$re^{rx} \cdot c^T = e^{rx} \cdot A \cdot c^T,$$

neboli

$$r \cdot c^T = A \cdot c^T,$$

tj. právě tehdy, když je r vlastním číslem matice A a c příslušným vlastním vektorem.

- (ii) Předpokládejme, že n -tice funkcí

$$(c_{11}e^{r_1x}, \dots, c_{1n}e^{r_1x}), \dots, (c_{k1}e^{r_kx}, \dots, c_{kn}e^{r_kx}),$$

kteří odpovídají vlastním číslům r_1, \dots, r_k , jsou lineárně závislé, tj. existují reálná čísla b_1, \dots, b_k , která nejsou všechna rovna nule, pro která je

$$\begin{aligned} & b_1 \cdot (c_{11}e^{r_1x}, c_{12}e^{r_1x}, \dots, c_{1n}e^{r_1x}) + b_2 \cdot (c_{21}e^{r_2x}, c_{22}e^{r_2x}, \dots, c_{2n}e^{r_2x}) + \dots \\ & \dots + b_k \cdot (c_{k1}e^{r_kx}, c_{k2}e^{r_kx}, \dots, c_{kn}e^{r_kx}) = (0, 0, \dots, 0). \end{aligned}$$

Pro každé $j = 1, \dots, n$ je tedy

$$b_1c_{1j}e^{r_1x} + b_2c_{2j}e^{r_2x} + \dots + b_kc_{kj}e^{r_kx} = 0.$$

odtud

$$(a_{i1} - \frac{c_i}{c_1} a_{11})y_1 = -(a_{i2} - \frac{c_i}{c_1} a_{12})\frac{c_2}{c_1}y_1 - \dots - (a_{in} - \frac{c_i}{c_1} a_{1n})\frac{c_n}{c_1}y_1. \quad (2)$$

Obdobným způsobem přejdeme od výchozí soustavy rovnic $y' = Ay$ k soustavě $n - 1$ rovnic (pro $i = 2, \dots, n$):

$$y'_i - \frac{c_i}{c_1}y'_1 = (a_{i1} - \frac{c_i}{c_1}a_{11})y_1 + (a_{i2} - \frac{c_i}{c_1}a_{12})y_2 + \dots + (a_{in} - \frac{c_i}{c_1}a_{1n})y_n. \quad (3)$$

Jednoduchým dosazením z (2) do (3) — dosazujeme za $(a_{i1} - \frac{c_i}{c_1}a_{11})y_1$ — získáme pro $i = 2, \dots, n$ vztahy

$$y'_i - \frac{c_i}{c_1}y'_1 = (a_{i2} - \frac{c_i}{c_1}a_{12})(y_2 - \frac{c_2}{c_1}y_1) + \dots + (a_{in} - \frac{c_i}{c_1}a_{1n})(y_n - \frac{c_n}{c_1}y_1). \quad (4)$$

Položme nyní

$$\begin{aligned} z_2 = y_2 - \frac{c_2}{c_1}y_1, \dots, z_n = y_n - \frac{c_n}{c_1}y_1, \\ z = (z_2, \dots, z_n). \end{aligned} \quad (5)$$

Získali jsme tak soustavu $n - 1$ lineárních diferenciálních rovnic $z' = Bz$ s maticí

$$B = \begin{pmatrix} a_{22} - \frac{c_2}{c_1}a_{12} & \dots & a_{2n} - \frac{c_2}{c_1}a_{1n} \\ \dots & \dots & \dots \\ a_{n2} - \frac{c_n}{c_1}a_{12} & \dots & a_{nn} - \frac{c_n}{c_1}a_{1n} \end{pmatrix}.$$

Ukážeme, že matice B má $(k - 1)$ -násobné vlastní číslo r .

Zřejmě je

$$c_1 \cdot \det(\lambda E - A) = \begin{vmatrix} c_1(\lambda - a_{11}) & -a_{12} & \dots & -a_{1n} \\ -c_1a_{21} & \lambda - a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ -c_1a_{n1} & -a_{n2} & \dots & \lambda - a_{nn} \end{vmatrix}.$$

Nyní c_2 -násobek druhého sloupce, \dots , c_n -násobek n -tého sloupce přičteme k prvnímu sloupci a využijeme toho, že (c_1, \dots, c_n) je vlastní vektor příslušný k vlastnímu číslu r , tj. vztahů (1). Tedy

$$\begin{aligned} c_1 \cdot \det(\lambda E - A) &= \begin{vmatrix} (\lambda - r)c_1 & -a_{12} & \dots & -a_{1n} \\ (\lambda - r)c_2 & \lambda - a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ (\lambda - r)c_n & -a_{n2} & \dots & \lambda - a_{nn} \end{vmatrix} = \\ &= (\lambda - r) \cdot \begin{vmatrix} c_1 & -a_{12} & \dots & -a_{1n} \\ c_2 & \lambda - a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ c_n & -a_{n2} & \dots & \lambda - a_{nn} \end{vmatrix}. \end{aligned}$$

Nyní přičteme $(-\frac{c_2}{c_1})$ -násobek prvního řádku ke druhému řádku, \dots , $(-\frac{c_n}{c_1})$ -násobek prvního řádku k n -tému řádku a dostaneme:

$$\begin{aligned} c_1 \cdot \det(\lambda E - A) &= (\lambda - r) \cdot \begin{vmatrix} c_1 & -a_{12} & \dots & -a_{1n} \\ 0 & \lambda - a_{22} + \frac{c_2}{c_1} a_{12} & \dots & -a_{2n} + \frac{c_2}{c_1} a_{1n} \\ \dots & \dots & \dots & \dots \\ 0 & -a_{n2} + \frac{c_n}{c_1} a_{12} & \dots & \lambda - a_{nn} + \frac{c_n}{c_1} a_{1n} \end{vmatrix} = \\ &= c_1 \cdot (\lambda - r) \cdot \begin{vmatrix} \lambda - a_{22} + \frac{c_2}{c_1} a_{12} & \dots & -a_{2n} + \frac{c_2}{c_1} a_{1n} \\ \dots & \dots & \dots \\ -a_{n2} + \frac{c_n}{c_1} a_{12} & \dots & \lambda - a_{nn} + \frac{c_n}{c_1} a_{1n} \end{vmatrix}. \end{aligned}$$

Dokázali jsme tedy, že

$$\det(\lambda E - A) = (\lambda - r) \cdot \det(\lambda E - B).$$

Soustava $z' = Bz$ má podle indukčního předpokladu $k - 1$ lineárně nezávislých řešení

$$\begin{aligned} &(q_{21}(x)e^{rx}, q_{31}(x)e^{rx}, \dots, q_{n1}(x)e^{rx}), \\ &(q_{22}(x)e^{rx}, q_{32}(x)e^{rx}, \dots, q_{n2}(x)e^{rx}), \\ &\dots \\ &(q_{2,k-1}(x)e^{rx}, q_{3,k-1}(x)e^{rx}, \dots, q_{n,k-1}(x)e^{rx}), \end{aligned}$$

kde pro každé $i = 2, \dots, n$ a $j = 1, \dots, k - 1$ je $q_{ij}(x)$ polynom stupně nejvýše $j - 1$.

Do rovnice

$$y_1' = a_{11}y_1 + a_{12}y_2 + \dots + a_{1n}y_n$$

dosadíme za y_2, \dots, y_n ze vztahů (5); dospějeme k rovnici

$$y_1' = a_{11}y_1 + a_{12}(z_2 + \frac{c_2}{c_1}y_1) + \dots + a_{1n}(z_n + \frac{c_n}{c_1}y_1),$$

od které snadnou úpravou s využitím (1) dojdeme k rovnici

$$y_1' - ry_1 = a_{12}z_2 + \dots + a_{1n}z_n.$$

Z výše uvedených řešení z_2, \dots, z_n , kde

$$z_2 = q_{2j}(x) \cdot e^{rx}, \quad z_3 = q_{3j}(x) \cdot e^{rx}, \quad \dots, \quad z_n = q_{nj}(x) \cdot e^{rx},$$

získáme řešení

$$y_1 = (a_{12}s_{2j}(x) + a_{13}s_{3j}(x) + \dots + a_{1n}s_{nj}(x)) \cdot e^{rx},$$

kde pro každé $i = 2, \dots, n$ a $j = 1, \dots, k - 1$ je polynom $q_{ij}(x)$ derivací polynomu $s_{ij}(x)$. Polynom

$$p_{1,j}(x) = a_{12}s_{2j}(x) + a_{13}s_{3j}(x) + \dots + a_{1n}s_{nj}(x)$$

má zřejmě stupeň nejvýše $j + 1$. Ze vztahů (5) nyní vypočteme funkce y_2, \dots, y_n ; mají zřejmě tvar uvedený v tvrzení (iii). K těmto $k - 1$ řešením přistupuje ještě řešení

$$(c_1 e^{rx}, c_2 e^{rx}, \dots, c_n e^{rx}) .$$

Nyní ukážeme, že řešení

$$\begin{aligned} & (c_1 e^{rx}, \dots, c_j e^{rx}, \dots, c_n e^{rx}), \\ & (p_{11}(x)e^{rx}, \dots, p_{j1}(x)e^{rx}, \dots, p_{n1}(x)e^{rx}), \\ & (p_{12}(x)e^{rx}, \dots, p_{j2}(x)e^{rx}, \dots, p_{n2}(x)e^{rx}), \\ & \dots\dots\dots \\ & (p_{1,k-1}(x)e^{rx}, \dots, p_{j,k-1}(x)e^{rx}, \dots, p_{n,k-1}(x)e^{rx}) . \end{aligned}$$

jsou lineárně nezávislá. Předpokládejme, že lineární kombinace výše uvedených k řešení s koeficienty d_1, d_2, \dots, d_k je rovna nulové n -tici funkcí, tj. pro každé $j = 1, \dots, n$ je

$$d_1 \cdot c_j e^{rx} + d_2 \cdot p_{j1}(x)e^{rx} + d_3 \cdot p_{j2}(x)e^{rx} + \dots + d_k \cdot p_{j,k-1}(x)e^{rx} = 0 .$$

Vydělíme-li tyto rovnosti nenulovou funkcí e^{rx} , dostáváme pro každé $j = 1, \dots, n$ rovnost

$$d_1 \cdot c_j + d_2 \cdot p_{j1}(x) + d_3 \cdot p_{j2}(x) + \dots + d_k \cdot p_{j,k-1}(x) = 0 .$$

Podle (5) je však pro každé $j = 1, \dots, n$ $y_j = z_j + \frac{c_j}{c_1} y_1$ a odtud

$$p_{j1}(x) = q_{j1}(x) + \frac{c_j}{c_1} p_{11}(x), \quad \dots, \quad p_{j,k-1}(x) = q_{j,k-1}(x) + \frac{c_j}{c_1} p_{1,k-1}(x) .$$

Odtud

$$d_1 \cdot c_1 + d_2 \cdot p_{11}(x) + \dots + d_k \cdot p_{1,k-1}(x) = 0 \tag{6}$$

a pro každé $j = 2, \dots, n$

$$d_1 \cdot c_j + d_2 \cdot (q_{j1}(x) + \frac{c_j}{c_1} p_{11}(x)) + \dots + d_k \cdot (q_{j,k-1}(x) + \frac{c_j}{c_1} p_{1,k-1}(x)) = 0 . \tag{7}$$

Odečteme-li pro každé $j = 2, \dots, n$ $\frac{c_j}{c_1}$ -násobek rovnosti (6) od rovností (7), dojdeme k rovnostem

$$d_2 \cdot q_{j1}(x) + d_3 \cdot q_{j2}(x) + \dots + d_k \cdot q_{j,k-j}(x) = 0, \quad j = 2, \dots, n .$$

Koeficienty d_2, d_3, \dots, d_k jsou tedy vesměs nulové; to vyplývá z lineární nezávislosti výše uvedených $k - 1$ řešení soustavy $z' = Bz$. Protože je $c_1 \neq 0$, je rovněž $d_1 = 0$. Lineární nezávislost výše uvedených k řešení soustavy $y' = Ay$ je tedy dokázána. \square

20.4. Příklady.

(i) Řešme následující soustavu lineárních diferenciálních rovnic:

$$\begin{aligned}y_1' &= -y_1 + y_2 + y_3, \\y_2' &= y_1 - y_2 + y_3, \\y_3' &= y_1 + y_2 + y_3.\end{aligned}$$

Maticí soustavy je matice

$$A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

její charakteristický polynom je $(\lambda + 1)(\lambda - 2)(\lambda + 2)$, vlastním čísly $-1, 2, -2$ odpovídají jako vlastní vektory všechny nenulové vektory podprostorů

$$[(1, 1, -1)], \quad [(1, 1, 2)], \quad [(1, -1, 0)],$$

kterým odpovídají řešení

$$(e^{-x}, e^{-x}, -e^{-x}), \quad (e^{2x}, e^{2x}, 2e^{2x}), \quad (e^{-2x}, -e^{-2x}, 0).$$

Množina všech řešení dané soustavy je vektorový prostor

$$[(1, 1 - 1) \cdot e^{-x}, (1, 1, 2) \cdot e^{2x}, (1, -1, 0) \cdot e^{-2x}].$$

Toto řešení bychom získali následujícím převodem matice A na Jordanův kanonický tvar:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix} = \frac{1}{6} \begin{pmatrix} 2 & 2 & -2 \\ 1 & 1 & 2 \\ 3 & -3 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ -1 & 2 & 0 \end{pmatrix}$$

Povšimněme si, že koeficienty ve sloupcích matice C odpovídají koeficientům jednotlivých řešení fundamentálního systému (první řešení: první sloupec, druhé řešení: druhý sloupec, třetí řešení: třetí sloupec).

Obecným řešením je tedy lineární kombinace

$$(ae^{-x} + be^{2x} + ce^{-2x}, ae^{-x} + be^{2x} - ce^{-2x}, -ae^{-x} + 2be^{2x}).$$

Hledáme-li řešení (y_1, y_2, y_3) určené např. podmínkami

$$y_1(0) = 1, \quad y_2(0) = 0, \quad y_3(0) = -1,$$

dosadíme do obecného řešení a ze soustavy rovnic

$$\begin{aligned} a + b + c &= 1, \\ a + b - c &= 0, \\ -a + 2b &= -1 \end{aligned}$$

vypočteme koeficienty a, b, c a získáme hledané řešení:

$$\left(\frac{2}{3}e^{-x} - \frac{1}{6}e^{2x} + \frac{1}{2}e^{-2x}, \frac{2}{3}e^{-x} - \frac{1}{6}e^{2x} - \frac{1}{2}e^{-2x}, -\frac{2}{3}e^{-x} - \frac{1}{3}e^{2x} \right).$$

(ii) Řešme následující soustavu lineárních diferenciálních rovnic:

$$\begin{aligned} y_1' &= 2y_1 - y_2, \\ y_2' &= y_1 + 4y_2. \end{aligned}$$

Maticí soustavy je matice

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 4 \end{pmatrix},$$

její charakteristický polynom je $(\lambda - 3)^2$, k vlastnímu číslu 3 přísluší jako vlastní vektory všechny nenulové vektory podprostoru $[(1, -1)]$. Uvedená soustava má tedy řešení

$$\left(e^{3x}, -e^{3x} \right) \quad \text{a} \quad \left((ax + b) \cdot e^{3x}, (cx + d) \cdot e^{3x} \right),$$

kde koeficienty a, b, c, d můžeme vypočítat dosazením uvažovaného řešení do zadané soustavy diferenciálních rovnic; dospějeme k soustavě lineárních rovnic

$$\begin{aligned} 3b + a &= 2b - d, \\ 3a &= 2a - c, \\ 3d + c &= b + 4d, \\ 3c &= a + 4c, \end{aligned}$$

ze které vyplývají vztahy mezi hledanými koeficienty:

$$c = -a, \quad d = -a - b.$$

Dvojice funkcí

$$\left((ax + b) \cdot e^{3x}, (-ax - a - b) \cdot e^{3x} \right),$$

kde $a, b \in \mathbb{R}$, dává všechna řešení dané soustavy; množinu všech řešení můžeme zapsat v tvaru

$$\left[(x, -x - 1) \cdot e^{3x}, (1, -1) \cdot e^{3x} \right].$$

Takto vyjádřenou množinu všech řešení bychom získali též pomocí Jordanova kanonického tvaru, tj. pomocí rovnosti

$$J = \begin{pmatrix} 3 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & -1 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = C^{-1}AC,$$

dospěli bychom ke stejnému výsledku. Povšimněme si, že koeficienty ve sloupcích matice C odpovídají koeficientům jednotlivých řešení fundamentálního systému (druhé řešení: druhý sloupec, první řešení: první sloupec – absolutní členy, druhý sloupec – koeficienty u x).

Matice C není určena jednoznačně; různá volba této transformační matice odpovídá různé volbě báze množiny všech řešení, tj. různým fundamentálním systémům.

(iii) Řešme soustavu lineárních diferenciálních rovnic

$$\begin{aligned} y_1' &= y_1 + 2y_2 - \frac{3}{2}y_3, \\ y_2' &= -y_2 + 3y_3, \\ y_3' &= -y_1 + \frac{1}{2}y_2 + 2y_3. \end{aligned}$$

Charakteristickým polynomem matice soustavy

$$\begin{pmatrix} 1 & 2 & -\frac{3}{2} \\ 0 & -1 & 3 \\ -1 & \frac{1}{2} & 2 \end{pmatrix}$$

je polynom $(\lambda - 2)^2(\lambda + 2)$. K vlastnímu číslu 2, resp. -2 přísluší jako vlastní vektory všechny nenulové vektory podprostorů

$$[(1, 2, 2)], \quad \text{resp.} \quad [(-5, 6, -2)].$$

Uvedená soustava diferenciálních rovnic má tedy řešení

$$(e^{2x}, 2e^{2x}, 2e^{2x}), \quad (-5e^{-2x}, 6e^{-2x}, -2e^{-2x}).$$

Pro vlastní číslo 2 existuje ještě řešení tvaru

$$((ax + b) \cdot e^{2x}, (cx + d) \cdot e^{2x}, (ex + f) \cdot e^{2x});$$

potřebné vztahy mezi koeficienty a, b, c, d, e, f můžeme vypočítat dosazením obecného řešení do zadané soustavy. Získáme soustavu lineárních rovnic

$$\begin{aligned} 2b + a &= b + 2d - \frac{3}{2}f, & 2a &= a + 2c - \frac{3}{2}e, \\ 2d + c &= -d + 3f, & 2c &= -c + 3e, \\ 2f + e &= -b + \frac{1}{2}d + 2f, & 2e &= -a + \frac{1}{2}c + 2e, \end{aligned}$$

ze které získáme následující vztahy mezi koeficienty:

$$c = 2a, \quad d = 4a + 2b, \quad e = 2a, \quad f = \frac{14}{3}a + 2b.$$

Z obecného řešení

$$\left((ax + b) \cdot e^{2x}, (2ax + 4a + 2b) \cdot e^{2x}, \left(2ax + \frac{14}{3}a + 2b\right) \cdot e^{2x} \right)$$

snadno získáme dvě lineárně nezávislá řešení a tak dojdeme k fundamentálnímu systému dané soustavy. Množinu všech řešení zapíšeme v tvaru:

$$\left[\left(x, 2x + 4, 2x + \frac{14}{3}\right) \cdot e^{2x}, (1, 2, 2) \cdot e^{2x}, (-5, 6, -2) \cdot e^{-2x} \right],$$

Toto řešení bychom získali následujícím převodem matice A na Jordanův kanonický tvar:

$$\begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix} = \frac{1}{64} \begin{pmatrix} -24 & -12 & 24 \\ 54 & 35 & -30 \\ -2 & 7 & -6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & -\frac{3}{2} \\ 0 & -1 & 3 \\ -1 & \frac{1}{2} & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & -5 \\ 4 & 2 & 6 \\ \frac{14}{3} & 2 & -2 \end{pmatrix}$$

(iv) Řešme následující soustavu lineárních diferenciálních rovnic (jde o stejnou soustavu jako v příkladu 20.2(i)):

$$\begin{aligned} y_1' &= y_2, \\ y_2' &= y_3, \\ y_3' &= y_1 - 3y_2 + 3y_3. \end{aligned}$$

Charakteristickým polynomem matice soustavy

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 3 \end{pmatrix}$$

je polynom $(\lambda - 1)^3$. K vlastnímu číslu 1 přísluší jako vlastní vektory všechny nenulové vektory podprostoru $[(1, 1, 1)]$. Uvedená soustava diferenciálních rovnic má tedy řešení

$$(e^x, e^x, e^x).$$

Existují však ještě řešení tvaru

$$\begin{aligned} & \left((mx + n) \cdot e^x, (px + q) \cdot e^x, (rx + s) \cdot e^x \right), \\ & \left((ax^2 + bx + c) \cdot e^x, (dx^2 + ex + f) \cdot e^x, (gx^2 + hx + i) \cdot e^x \right); \end{aligned}$$

potřebné vztahy mezi koeficienty můžeme vypočítat dosazením do zadané soustavy diferenciálních rovnic; získáme soustavu lineárních rovnic pro koeficienty $a, b, c, d, e, f, g, h, i$:

$$\begin{aligned} b + c &= f, & e + f &= i, & h + i &= c - 3f + 3i, \\ 2a + b &= e, & 2d + e &= h, & 2g + h &= b - 3e + 3h, \\ a &= d, & d &= g, & g &= a - 3d + 3g. \end{aligned}$$

Snadno zjistíme, že

$$d = a, \quad e = 2a + b, \quad f = b + c, \quad g = a, \quad h = 4a + b, \quad i = 2a + 2b + c.$$

Získané řešení

$$\left([ax^2 + bx + c] \cdot e^x, [ax^2 + (2a + b)x + b + c] \cdot e^x, [ax^2 + (4a + b)x + 2a + 2b + c] \cdot e^x \right)$$

můžeme zapsat jako lineární kombinaci tří lineárně nezávislých řešení (s koeficienty a, b, c). Množinu všech řešení dané soustavy můžeme zapsat jako vektorový prostor

$$\left[(1, 1, 1) \cdot e^x, (x, x + 1, x + 2) \cdot e^x, \left(\frac{1}{2}x^2, \frac{1}{2}x^2 + x, \frac{1}{2}x^2 + 2x + 1 \right) \cdot e^x \right].$$

Koeficienty jednotlivých polynomů můžeme vyčíst z transformační matice B , která převádí matici A na Jordanův kanonický tvar J :

$$J = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 & 1 \\ -1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} = B^{-1}AB$$

Poznamenejme, že v příkladu 20.2(i) byla matice A na Jordanův kanonický tvar převedena pomocí matice $C \neq B$. Snadno zjistíme, že maticím B a C odpovídají fundamentální systémy, které jsou „velmi blízké“, jeden z druhého získáme jednoduchými lineárními kombinacemi.

V. FORMY

21. LINEÁRNÍ FORMY

21.1. Definice. Nechť V je vektorový prostor nad tělesem T . *Lineární formou* na prostoru V budeme rozumět každé zobrazení f prostoru V do tělesa T , pro které platí:

$$\begin{aligned} \text{(i)} \quad & \forall x, y \in V \quad f(x + y) = f(x) + f(y) , \\ \text{(ii)} \quad & \forall x \in V \quad \forall a \in T \quad f(ax) = a \cdot f(x) . \end{aligned}$$

Vlastnosti (i), (ii) je možno shrnout do jediné:

$$\forall x, y \in V \quad \forall a, b \in T \quad f(ax + by) = a \cdot f(x) + b \cdot f(y)$$

Užitím matematické indukce dostaneme obecnou rovnost:

$$\forall x_1, \dots, x_n \in V \quad \forall a_1, \dots, a_n \in T \quad f\left(\sum_{i=1}^n a_i x_i\right) = \sum_{i=1}^n a_i \cdot f(x_i)$$

Vzhledem k tomu, že těleso T je vektorovým prostorem samo nad sebou, nejsou lineární formy na prostoru V nic jiného než homomorfismy prostoru V do prostoru T , tj. prvky prostoru $\text{Hom}(V, T)$. Pojmy, které jsme v předchozích paragrafech zavedli pro homomorfismy, a tvrzení, která jsme pro ně dokázali, budeme tedy používat i pro lineární formy.

21.2. Příklady.

(i) Zobrazení, které každému vektoru prostoru V přiřazuje nulový prvek tělesa T , je tzv. *nulová* lineární forma na prostoru V . Ostatní lineární formy na prostoru V se nazývají *nenulové*.

(ii) Zobrazení, které každému vektoru $(x_1, \dots, x_n) \in T^n$ přiřazuje lineární kombinaci $a_1 x_1 + \dots + a_n x_n$, kde skaláry $a_1, \dots, a_n \in T$ jsou pevně zvolené, je lineární forma na prostoru T^n .

(iii) Zobrazení, které každé matici A řádu n nad tělesem T přiřazuje její stopu $\text{tr } A$, je lineární forma na prostoru $T^{n \times n}$.

(iv) Nechť V je prostor všech reálných funkcí reálné proměnné, které jsou spojitě na intervalu $\langle a, b \rangle$. Zobrazení, které každé funkci $g \in V$ přiřazuje číslo $\int_a^b g(x) dx$, je lineární forma na prostoru V . Podobně je lineární formou na prostoru V zobrazení, které každé funkci $g \in V$ přiřazuje číslo $\int_a^b g(x) \varphi(x) dx$, kde φ je pevně zvolená funkce prostoru V .

(v) Zobrazení, které každému polynomu $p \in T[x]$ přiřazuje prvek

$$\sum_{i=1}^k a_i p(c_i) \in T,$$

kde $a_1, \dots, a_k, c_1, \dots, c_k \in T$ jsou pevně zvolené prvky, je lineární forma na prostoru $T[x]$.

21.3. Poznámka. Pro nulovou lineární formu f na prostoru V je $\text{Ker } f = V$, tj. $d(f) = \dim V$, a $\text{Im } f = O$, tj. $r(f) = 0$. Jestliže je f nenulová lineární forma na prostoru V , je nutně $r(f) = 1$, tj. f je epimorfismus. Podle věty o hodnotě a defektu je $\dim V = d(f) + 1$. Má-li tedy prostor V dimenzi n , má jádro $\text{Ker } f$ nenulové lineární formy f dimenzi $n - 1$.

21.4. Poznámka. Každá lineární forma f na prostoru V je určena svými hodnotami v libovolné bázi prostoru V (viz 10.8); jestliže je $\{v_\alpha; \alpha \in \Lambda\}$ báze prostoru V , potom je forma f určena indexovaným souborem $\{f(v_\alpha); \alpha \in \Lambda\}$.

Protože je každý nenulový vektor $v \in V$ prvkem nějaké báze prostoru V , existuje podle předešlého lineární forma f taková, že $f(v) \neq 0$. Ke každému nenulovému vektoru $v \in V$ tedy existuje forma f na prostoru V , pro kterou $f(v) \neq 0$.

Jestliže je W podprostor prostoru V a vektor $v \in V$ v něm neleží, existuje z obdobných důvodů na prostoru V forma f , která je nulová na celém podprostoru W a pro kterou je $f(v) \neq 0$.

21.5. Poznámka. Nechť V je prostor dimenze n a $N = \{v_1, \dots, v_n\}$ jeho báze, nechť f je lineární forma na prostoru V . *Maticí lineární formy f vzhledem k bázi N* budeme rozumět matici homomorfismu f vzhledem k bázím N a $\{1\}$, tj. matici

$$(f(v_1), f(v_2), \dots, f(v_n)).$$

Jestliže je vektor $x \in V$ zadán svými souřadnicemi vzhledem k bázi N , tj. $\langle v \rangle_N = (x_1, \dots, x_n)$, potom je podle 11.2

$$f(x) = (f(v_1), f(v_2), \dots, f(v_n)) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

tj.

$$f(x) = f(v_1) \cdot x_1 + f(v_2) \cdot x_2 + \dots + f(v_n) \cdot x_n.$$

Této rovnosti se někdy říká *analytické vyjádření* lineární formy f vzhledem k bázi N . Hodnota formy f ve vektoru x se tedy vypočte jako součet součinů hodnot formy f ve vektorech báze N a souřadnic vektoru x vzhledem k téže bázi N .

Jestliže A je matice formy f vzhledem k bázi N a C je matice přechodu od báze M k bázi N , potom je AC matice formy f vzhledem k bázi M (viz 11.11).

21.6. Definice. Nechť V je vektorový prostor nad tělesem T . *Duálním prostorem* k prostoru V budeme rozumět prostor $V^* = \text{Hom}(V, T)$, tj. prostor všech lineárních forem na prostoru V .

Lineární formy na prostoru V tedy sčítáme a násobíme skalárem jako homomorfismy prostoru V do prostoru T (viz 10.27 a 7.8(ix)).

Zobrazení, které každé lineární formě na prostoru V přiřazuje její matici vzhledem k pevně zvolené bázi N , je izomorfismus prostoru V^* na prostor $T^{1 \times n}$ (viz 11.13). Lineární závislost či nezávislost lineárních forem můžeme tedy zjistit tak, že stanovíme lineární závislost či nezávislost jejich matic jako vektorů prostoru $T^{1 \times n}$ (tj. T^n). Stejným způsobem můžeme zjištění dimenze podprostoru $[f_1, \dots, f_m]$ prostoru V^* převést na stanovení hodnoty matice typu $m \times n$, jejíž řádky jsou maticemi forem f_1, \dots, f_m vzhledem k nějaké pevně zvolené bázi prostoru V .

21.7. Věta. *Nechť V je vektorový prostor nad tělesem T . Jestliže má prostor V konečnou dimenzi, je $\dim V^* = \dim V$.*

Důkaz. Jestliže je $\dim V = n$, potom je podle věty 11.13

$$\dim V^* = \dim \text{Hom}(V, T) = \dim V \cdot \dim T = n \cdot 1 = n. \quad \square$$

21.8. Definice. Nechť V je vektorový prostor dimenze n nad tělesem T a nechť $N = \{v_1, \dots, v_n\}$ je jeho báze. Báze $N^* = \{f_1, \dots, f_n\}$ duálního prostoru V^* se nazývá *duální* k bázi N , jestliže pro každé $i, j = 1, \dots, n$ je

$$f_i(v_j) = \delta_{ij}.$$

Jestliže je báze $\{f_1, f_2, \dots, f_n\}$ duální k bázi $N = \{v_1, v_2, \dots, v_n\}$, potom matice forem f_1, f_2, \dots, f_n vzhledem k bázi N tvoří podle definice 21.8 kanonickou bázi prostoru $T^{1 \times n}$ (resp. T^n). Analytická vyjádření forem f_1, f_2, \dots, f_n vzhledem k bázi N jsou tedy

$$f_1(x) = x_1, \quad f_2(x) = x_2, \quad \dots, \quad f_n(x) = x_n.$$

21.9. Věta. *Nechť V je vektorový prostor konečné dimenze nad tělesem T . Potom ke každé bázi prostoru V existuje právě jediná duální báze prostoru V^* .*

Důkaz. Nechť $N = \{v_1, v_2, \dots, v_n\}$ je báze prostoru V . Přiřadíme-li každé lineární formě $f \in V^*$ její matici vzhledem k bázi N , dostáváme podle věty 11.13 izomorfismus Ψ prostoru $V^* = \text{Hom}(V, T)$ na prostor $T^{1 \times n}$ matic typu $1 \times n$. Kanonické bázi prostoru $T^{1 \times n}$ odpovídá při izomorfismu Ψ , resp. Ψ^{-1} nějaká báze $\{f_1, f_2, \dots, f_n\}$ prostoru V^* :

Tato n -tice je však zároveň maticí formy f vzhledem k bázi N , takže matice formy f vzhledem k bázi N a n -tice souřadnic formy f vzhledem k bázi N^* jsou totožné.

(ii) Každý vektor $v \in V$ můžeme vyjádřit souřadnicemi vzhledem k bázi N . Jestliže

$$\langle v \rangle_N = (b_1, b_2, \dots, b_n), \quad \text{tj.} \quad v = b_1 v_1 + b_2 v_2 + \dots + b_n v_n,$$

potom je pro každé $i = 1, \dots, n$

$$f_i(v) = f_i(b_1 v_1 + b_2 v_2 + \dots + b_n v_n) = b_i,$$

neboť báze N^* je duální k bázi N . Souřadnice vektoru v vzhledem k bázi N jsou tedy rovny hodnotám forem báze N^* ve vektoru v , tj.

$$\langle v \rangle_N = (f_1(v), f_2(v), \dots, f_n(v)).$$

21.11. Poznámka. Nechť V je vektorový prostor, $N = \{v_1, \dots, v_n\}$ jeho báze, $M = \{f_1, \dots, f_n\}$ báze duálního prostoru V^* a $K = \{u_1, \dots, u_n\}$ nějaká další báze prostoru V .

Utvořme matici $A = (a_{ik})$ řádu n , která má v řádcích zapsány po řadě matice forem f_1, \dots, f_n vzhledem k bázi K , tj. pro každé $i = 1, \dots, n$ je

$$(f_i(u_1), \dots, f_i(u_n)) = (a_{i1}, \dots, a_{in}).$$

Matice A je regulární, neboť formy f_1, \dots, f_n tvoří bázi (lineárně nezávislým formám odpovídají lineárně nezávislé řádky matice A — viz poznámka za definicí 21.6). Utvořme matici $B = (b_{kj})$ řádu n , která má ve sloupcích souřadnice vektorů báze N vzhledem k bázi K , tj.

$$\langle v_j \rangle_K = (b_{1j}, \dots, b_{nj}).$$

Matice B je regulární, neboť vektory v_1, \dots, v_n jsou lineárně nezávislé.

Báze M je duální k bázi N právě tehdy, když jsou matice A a B navzájem inverzní. Pro každé $i, j = 1, \dots, n$ vypočítáme totiž hodnotu $f_i(v_j)$ dosazením souřadnic $\langle v_j \rangle_K$ do analytického vyjádření formy f_i vzhledem k bázi K , tj. „maticově“ vynásobíme i -tý řádek matice A a j -tý sloupec matice B :

$$f_i(v_j) = (f_i(u_1), \dots, f_i(u_n)) \cdot \langle v_j \rangle_K^T = \sum_{k=1}^n a_{ik} b_{kj}.$$

Z této úvahy dostáváme *třetí důkaz* existence duální báze. Protože je matice B regulární, existuje k ní inverzní matice $A = B^{-1}$ a hledané formy f_1, \dots, f_n jsou dány svými maticemi vzhledem k bázi K — těmito maticemi jsou řádky matice A .

Dostáváme však i duální tvrzení. Ke každé bázi M duálního prostoru V^* existuje báze N prostoru V taková, že M je duální k N . Protože je matice A regulární, existuje k ní inverzní matice $B = A^{-1}$ a hledané vektory v_1, \dots, v_n jsou dány svými souřadnicemi vzhledem k bázi K — tyto souřadnice jsou ve sloupcích matice B .

Předchozí úvaha dává další metodu výpočtu. Duální bázi můžeme v konkrétních případech počítat podle definice (viz 21.8) nebo převodem analytických vyjádření (viz 21.8 a 21.5) nebo pomocí inverzní matice (viz 21.11).

21.12. Příklady.

(i) Najdeme duální bázi $N^* = \{f_1, f_2, f_3\}$ prostoru $(\mathbb{Z}_7^3)^*$ k bázi

$$N = \{(1, 1, 1), (0, 1, 1), (0, 0, 1)\}$$

prostoru \mathbb{Z}_7^3 ; formy f_1, f_2, f_3 zadáme analytickými vyjádřeními vzhledem ke kanonické bázi prostoru \mathbb{Z}_7^3 .

1. *způsob.* Vektory báze N se při formách f_1, f_2, f_3 zobrazují na nuly a jedničky (viz definice duální báze), jak je znázorněno v následujícím schématu:

$$\begin{array}{rcccl} & f_1 & f_2 & f_3 & \\ (1, 1, 1) & \longrightarrow & 1 & 0 & 0 \\ (0, 1, 1) & \longrightarrow & 0 & 1 & 0 \\ (0, 0, 1) & \longrightarrow & 0 & 0 & 1 \end{array}$$

Snadnou úpravou zjistíme, kam se zobrazí při f_1, f_2, f_3 vektory kanonické báze. Šestinásobek celého druhého řádku přičteme k prvnému a potom šestinásobek celého třetího řádku přičteme ke druhému:

$$\begin{array}{rcccl} & f_1 & f_2 & f_3 & \\ (1, 0, 0) & \longrightarrow & 1 & 6 & 0 \\ (0, 1, 0) & \longrightarrow & 0 & 1 & 6 \\ (0, 0, 1) & \longrightarrow & 0 & 0 & 1 \end{array}$$

Nyní známe hodnoty forem f_1, f_2, f_3 ve vektorech kanonické báze, tj. známe jejich analytická vyjádření vzhledem ke kanonické bázi:

$$f_1(x) = x_1, \quad f_2(x) = 6x_1 + x_2, \quad f_3(x) = 6x_2 + x_3.$$

2. *způsob.* Matice forem f_1, f_2, f_3 vzhledem k bázi N vynásobíme maticí přechodu od kanonické báze k bázi N a tak převedeme analytická vyjádření forem f_1, f_2, f_3 vzhledem k bázi N (ty známe — viz 21.8) na analytická vyjádření vzhledem ke kanonické bázi.

Analytická vyjádření forem f_1, f_2, f_3 vzhledem k bázi N jsou

$$f_1(x) = x_1, \quad f_2(x) = x_2, \quad f_3(x) = x_3,$$

matice těchto forem vzhledem k bázi N jsou tedy $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ a jejich součiny s maticí přechodu

$$\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 0 & 6 & 1 \end{pmatrix}$$

od kanonické báze k bázi N jsou řádky této matice, tj. $(1, 0, 0)$, $(6, 1, 0)$, $(0, 6, 1)$. Analytická vyjádření forem f_1, f_2, f_3 vzhledem ke kanonické bázi jsou tedy

$$f_1(x) = x_1, \quad f_2(x) = 6x_1 + x_2, \quad f_3(x) = 6x_2 + x_3.$$

3. *způsob*. Vektory báze N napíšeme do sloupců matice B , najdeme matici B^{-1} a z jejích řádků zapíšeme analytická vyjádření forem f_1, f_2, f_3 vzhledem ke kanonické bázi (viz 21.11). Je

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 0 & 6 & 1 \end{pmatrix}$$

a tedy

$$f_1(x) = x_1, \quad f_2(x) = 6x_1 + x_2, \quad f_3(x) = 6x_2 + x_3.$$

Je užitečné si uvědomit, že uvedené tři způsoby jsou numericky prakticky totožné. Vždy jde o výpočet inverzní matice; v prvním a druhém způsobu je to však poněkud zamaskováno.

(ii) Najdeme duální bázi $M^* = \{f_1, f_2, f_3\}$ k bázi $M = \{p_1, p_2, p_3\}$ prostoru V všech polynomů nejvýše druhého stupně s reálnými koeficienty, kde

$$p_1(x) = 2x^2 + x + 1, \quad p_2(x) = x^2 + x + 1, \quad p_3(x) = -x^2 + x + 2.$$

Koeficienty zadaných polynomů napíšeme do sloupců matice A a vypočteme inverzní matici A^{-1} .

$$A = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 1 & -3 & 2 \\ -1 & 5 & -3 \\ 0 & -1 & 1 \end{pmatrix}.$$

Nyní je třeba výsledek správně interpretovat. Označíme-li $K = \{x^2, x, 1\}$ bázi prostoru V , pak ve sloupcích matice A jsou souřadnice vektorů p_1, p_2, p_3 báze M vzhledem k bázi K . V řádcích matice A^{-1} jsou matice forem f_1, f_2, f_3 vzhledem k bázi K , tedy

$$\begin{aligned} f_1(ax^2 + bx + c) &= a - 3b + 2c, \\ f_2(ax^2 + bx + c) &= -a + 5b - 3c, \\ f_3(ax^2 + bx + c) &= -b + c. \end{aligned}$$

21.13. Příklad. Uvažujme vektorový prostor V všech polynomů stupně nejvýše n s reálnými koeficienty. Nechť c_0, c_1, \dots, c_n jsou navzájem různá reálná čísla. Zobrazení f_0, f_1, \dots, f_n vektorového prostoru V do tělesa reálných čísel, která polynomu $p \in V$ přiřazují po řadě čísla $p(c_0), p(c_1), \dots, p(c_n)$, tj. $f_i(p) = p(c_i)$, jsou lineární formy na prostoru V (viz 21.2(v)). Předpokládejme, že nějaká lineární kombinace forem f_0, f_1, \dots, f_n je rovna nulové lineární formě, tj.

$$a_0 f_0 + a_1 f_1 + \dots + a_n f_n = 0 .$$

Aplikujeme-li tuto rovnost na polynomy $1, x, x^2, \dots, x^n$, dostaneme rovnosti

$$\begin{aligned} a_0 + \dots + a_n &= 0 , \\ a_0 c_0 + \dots + a_n c_n &= 0 , \\ a_0 c_0^2 + \dots + a_n c_n^2 &= 0 , \\ \dots & \\ a_0 c_0^n + \dots + a_n c_n^n &= 0 . \end{aligned}$$

Vektor (a_0, a_1, \dots, a_n) je tedy řešením homogenní soustavy lineárních rovnic s maticí

$$A = \begin{pmatrix} 1 & \dots & 1 \\ c_0 & \dots & c_n \\ c_0^2 & \dots & c_n^2 \\ \dots & \dots & \dots \\ c_0^n & \dots & c_n^n \end{pmatrix} ,$$

jejímž determinanem je Vandermondův determinant čísel c_0, c_1, \dots, c_n (viz 15.7). Vzhledem k tomu, že čísla c_0, c_1, \dots, c_n jsou navzájem různá, je matice A regulární a tedy $a_0 = a_1 = \dots = a_n = 0$. Množina $M = \{f_0, \dots, f_n\}$ je proto lineárně nezávislá a je tedy bází prostoru V^* .

Snadno se ověří, že báze $N = \{p_0, p_1, \dots, p_n\}$ prostoru V , ke které je báze M duální, je tvořena tzv. *Lagrangeovými polynomy*

$$p_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^n \frac{x - c_j}{c_i - c_j} , \quad i = 0, 1, \dots, n .$$

21.14. Poznámka. Pojem duální báze je definován pouze u prostorů konečné dimenze. U nekonečně dimenzionálních prostorů dospějeme obdobnou konstrukcí pouze k lineárně nezávislé množině prvků duálního prostoru.

Nechť $N = \{v_\alpha; \alpha \in \Lambda\}$ je báze nekonečně dimenzionálního prostoru V . Definujme pro každé $\alpha \in \Lambda$ lineární formu f_α na prostoru V určením jejich hodnot na vektorech báze N :

$$f_\alpha(v_\beta) = \delta_{\alpha\beta} = \begin{cases} 1 & \text{pro } \beta = \alpha , \\ 0 & \text{pro } \beta \neq \alpha . \end{cases}$$

Snadno se ukáže (stejně jako v druhém důkazu věty 21.9), že množina

$$N^* = \{f_\alpha; \alpha \in \Lambda\}$$

je lineárně nezávislá. Tato množina však není bází prostoru V^* . Na prostoru V totiž existuje velké množství forem, které není možno vyjádřit jako lineární kombinace prvků množiny N^* ; je to např. forma f , pro kterou $f(v_\alpha) = 1$ pro každé $\alpha \in \Lambda$, nebo obecněji jakákoli forma, která má nenulové hodnoty na nekonečně mnoha vektorech báze N . Přestože množina N^* není bází, užívá se v různých úvahách a konstrukcích (viz např. 21.19, 21.32(ix), 21.33).

21.15. Poznámka. Pro další úvahy bude užitečné zavést nové označení, které je hojně užíváno zejména ve funkcionální analýze. Jestliže $v \in V$ a $f \in V^*$, pak symbolem $\langle v, f \rangle$ budeme rozumět provedení formy f na vektor v , tj.

$$\langle v, f \rangle = f(v) .$$

Symbolem $\langle ., . \rangle$ můžeme označit zobrazení kartézského součinu prostorů V a V^* do tělesa T , které každému vektoru $v \in V$ a každé formě $f \in V^*$ přiřazuje skalár $\langle v, f \rangle = f(v) \in T$. Toto zobrazení má následující vlastnosti:

- (i) $\forall v_1, v_2 \in V \quad \forall f \in V^* \quad \langle v_1 + v_2, f \rangle = \langle v_1, f \rangle + \langle v_2, f \rangle ,$
- (ii) $\forall v \in V \quad \forall a \in T \quad \forall f \in V^* \quad \langle av, f \rangle = a \cdot \langle v, f \rangle ,$
- (iii) $\forall v \in V \quad \forall f_1, f_2 \in V^* \quad \langle v, f_1 + f_2 \rangle = \langle v, f_1 \rangle + \langle v, f_2 \rangle ,$
- (iv) $\forall v \in V \quad \forall a \in T \quad \forall f \in V^* \quad \langle v, af \rangle = a \cdot \langle v, f \rangle .$

První dvě vlastnosti vznikly přepisem faktu, že f je lineární forma (viz definice 21.1), třetí je přepisem definice součtu dvou lineárních forem a čtvrtá přepisem definice násobku lineární formy. Prvé dvě vlastnosti představují linearitu symbolu $\langle ., . \rangle$ v první složce, druhé dvě linearitu v druhé složce. Z těchto důvodů říkáme, že zobrazení $\langle ., . \rangle : V \times V^* \rightarrow T$ je *bilineární*.

21.16. Poznámka. Stejně jako jsme k prostoru V vytvořili duální vektorový prostor $V^* = \text{Hom}(V, T)$, můžeme utvořit duální prostor $V^{**} = (V^*)^* = \text{Hom}(V^*, T)$ k prostoru V^* , duální prostor $V^{***} = (V^{**})^* = \text{Hom}(V^{**}, T)$ k prostoru V^{**} atd. Od vektorového prostoru V tak dospějeme k posloupnosti vektorových prostorů

$$V, V^*, V^{**}, V^{***}, \dots$$

Prostoru V^* , resp. V^{**} se někdy říká *duál*, resp. *druhý duál* prostoru V .

Každou lineární formu $f \in V^*$ můžeme zapsat také tak, že v bilineárním zobrazení $\langle ., . \rangle$ tuto formu fixujeme na druhé složce:

$$f = \langle ., f \rangle : V \rightarrow T .$$

Fixujeme-li však v bilineárním zobrazení $\langle ., . \rangle$ na první složce libovolný vektor $v \in V$, pak vzhledem k linearitě v druhé složce je zobrazení

$$v^{**} = \langle v, . \rangle : V^* \rightarrow T$$

lineární formou na prostoru V^* , tj. prvkem prostoru V^{**} . Každý vektor $v \in V$ tedy přirozeným způsobem určuje lineární formu $v^{**} \in V^{**}$ na prostoru V^* . Toto zjištění motivuje následující definici.

21.17. Definice. Zobrazení Φ prostoru V do prostoru V^{**} , které vektoru $v \in V$ přiřadí lineární formu $v^{**} \in V^{**}$ na prostoru V^* , která každé formě $f \in V^*$ přiřazuje skalár

$$v^{**}(f) = f(v) ,$$

se nazývá *kanonické*.

Rovnost, která definuje obraz v^{**} vektoru v při kanonickém zobrazení Φ , může být zapsána pomocí bilineárního symbolu $\langle \cdot, \cdot \rangle$ v tvaru

$$\langle f, v^{**} \rangle = \langle v, f \rangle .$$

21.18. Věta. *Kanonické zobrazení Φ prostoru V do prostoru V^{**} je monomorfismus.*

Důkaz. Dokažme nejprve, že kanonické zobrazení Φ je homomorfismus. Je třeba ukázat, že pro každé $x, y \in V$ a každé $a \in T$ je

$$\Phi(x + y) = \Phi(x) + \Phi(y) , \quad \Phi(ax) = a \cdot \Phi(x) ,$$

neboli

$$(x + y)^{**} = x^{**} + y^{**} , \quad (ax)^{**} = a \cdot x^{**} .$$

Pro každé $f \in V^*$ je

$$\begin{aligned} \langle f, (x + y)^{**} \rangle &= \langle x + y, f \rangle = \langle x, f \rangle + \langle y, f \rangle = \langle f, x^{**} \rangle + \langle f, y^{**} \rangle = \\ &= \langle f, x^{**} + y^{**} \rangle , \end{aligned}$$

$$\langle f, (ax)^{**} \rangle = \langle ax, f \rangle = a \cdot \langle x, f \rangle = a \cdot \langle f, x^{**} \rangle = \langle f, a \cdot x^{**} \rangle ,$$

takže rovnosti, které jsme chtěli dokázat, opravdu platí a Φ je homomorfismus.

Nyní ukážeme, že Φ je monomorfismus. Jestliže je $v \in V$ nenulový vektor a $f \in V^*$ forma, pro kterou $\langle v, f \rangle \neq 0$ (viz 21.4), potom je

$$\langle f, v^{**} \rangle = \langle v, f \rangle \neq 0 ,$$

takže $\Phi(v) = v^{**}$ je nenulový prvek prostoru V^{**} ; kanonické zobrazení Φ je monomorfismus, neboť jádro $\text{Ker } \Phi$ je nulové. \square

21.19. Věta. *Kanonické zobrazení Φ prostoru V do prostoru V^{**} je izomorfismus právě tehdy, když má prostor V konečnou dimenzi.*

Důkaz. Jestliže má prostor V konečnou dimenzi, je podle 21.7

$$\dim V = \dim V^* = \dim V^{**} .$$

Protože je kanonické zobrazení Φ monomorfismem prostoru V do prostoru V^{**} , je podle 10.21 Φ izomorfismus.

Předpokládejme naopak, že V je prostor nekonečné dimenze; nechť $\{v_\alpha; \alpha \in \Lambda\}$ je jeho báze. Nechť $M = \{f_\alpha; \alpha \in \Lambda\}$ je množina lineárních forem na prostoru V , taková, že

$$\langle v_\alpha, f_\beta \rangle = f_\beta(v_\alpha) = \delta_{\alpha\beta} = \begin{cases} 1 & \text{pro } \beta = \alpha, \\ 0 & \text{pro } \beta \neq \alpha. \end{cases}$$

Množina M je lineárně nezávislou podmnožinou prostoru V^* (viz 21.14), nechť N je báze prostoru V^* obsahující množinu M .

Podle věty 10.15 je množina $\{v_\alpha^{**}; \alpha \in \Lambda\}$ bází podprostoru $\text{Im } \Phi = \Phi(V)$ prostoru V^{**} . Přitom je

$$\langle f_\beta, v_\alpha^{**} \rangle = \langle v_\alpha, f_\beta \rangle = \delta_{\alpha\beta}.$$

Nechť $F \in V^{**}$ je taková lineární forma na prostoru V^* , že pro každé $f \in N$ je $\langle f, F \rangle = 1$ (forma F existuje podle 21.4). Forma F není lineární kombinací forem v_α^{**} , $\alpha \in \Lambda$, neboť každá taková lineární kombinace má pouze konečně mnoho nenulových hodnot na nekonečné množině M . Forma F tedy neleží v podprostoru $\Phi(V)$; proto je $\Phi(V) \neq V^{**}$ a Φ není izomorfismus. \square

21.20. Poznámka. Ve větě 21.18 jsme viděli, že vektorový prostor V je přirozeným způsobem izomorfní s podprostorem $\Phi(V)$ prostoru V^{**} . Prostor V se proto pomocí monomorfismu Φ s podprostorem $\Phi(V)$ často ztotožňuje a považuje se za podprostor prostoru V^{**} ; každý vektor $v \in V$ se tak ztotožňuje se svým obrazem $v^{**} = \Phi(v)$ a je chápán jako lineární forma na prostoru V^* .

Jestliže má prostor V konečnou dimenzi, potom je $\Phi(V) = V^{**}$; prostor V je ztotožněn s prostorem V^{**} , tj. V je duálním prostorem k prostoru V^* . Prostory V a V^* jsou tedy *navzájem duální*, lineární formy na prostoru V^* jsou *ztotožněny* pomocí izomorfismu Φ s vektory prostoru V : ke každé formě $F \in V^{**}$ existuje právě jediný vektor $v \in V$, takový, že pro každé $f \in V^*$ je

$$\langle f, F \rangle = \langle v, f \rangle.$$

Jestliže N^* je báze prostoru V^* , která je duální k bázi N prostoru V , potom je naopak N jako báze prostoru V^{**} duální k bázi N^* , tj. báze N a N^* jsou *navzájem duální*. Tato skutečnost již byla naznačena v odstavcích 21.10 a 21.11.

Jestliže má prostor V nekonečnou dimenzi, pak existují lineární formy na prostoru V^* , které neleží v podprostoru $\Phi(V)$ prostoru V a není je možno výše uvedeným způsobem popsat (viz 21.19). Dimenze prostorů V, V^*, V^{**}, \dots se stále zvětšují.

21.21. Poznámka. Nechť U a V jsou vektorové prostory nad tělesem T a F homomorfismus prostoru U do prostoru V . Jestliže f je lineární forma na prostoru V , potom složení fF homomorfismů F a f je homomorfismus prostoru U do tělesa T , tj. lineární forma na prostoru U .

$$\begin{array}{c}
 \overbrace{\hspace{10em}}^{fF \in U^*} \\
 T \longleftarrow \xrightarrow{f \in V^*} V \longleftarrow \xrightarrow{F} U
 \end{array}$$

Zobrazení F^* , které každé formě $f \in V^*$ přiřadí formu $fF \in U^*$, je homomorfismus prostoru V^* do prostoru U^* . Pro každé $f, g \in V^*$ a každé $a \in T$ je totiž

$$\begin{aligned}
 F^*(f + g) &= (f + g)F = fF + gF = F^*(f) + F^*(g) , \\
 F^*(af) &= (af)F = a \cdot (fF) = a \cdot F^*(f) .
 \end{aligned}$$

Homomorfismus F^* tedy funguje takto: pro každou lineární formu $f \in V^*$ je $F^*(f) \in U^*$ taková lineární forma, že pro každý vektor $u \in U$ je

$$[F^*(f)](u) = (fF)(u) = f(F(u)) ,$$

neboli

$$\forall u \in U \quad \forall f \in V^* \quad \langle F(u), f \rangle = \langle u, F^*(f) \rangle .$$

Vztah homomorfismů F a F^* je možno znázornit na následujícím schématu:

$$\begin{array}{ccc}
 V & \xleftarrow{F} & U \\
 F(u) & \xleftarrow{\quad} & u \\
 \\
 f & \xrightarrow{\quad} & F^*(f) \\
 V^* & \xrightarrow{F^*} & U^*
 \end{array}$$

$$\langle F(u), f \rangle = \langle u, F^*(f) \rangle$$

21.22. Definice. Nechť U a V jsou vektorové prostory nad tělesem T a F homomorfismus prostoru U do prostoru V . *Duálním homomorfismem* k homomorfismu F budeme rozumět homomorfismus F^* prostoru V^* do prostoru U^* , který každé lineární formě $f \in V^*$ přiřazuje lineární formu $fF \in U^*$, tj. F^* je definován rovností

$$F^*(f) = fF .$$

21.23. Poznámka.

(i) Duálním homomorfismem k identickému automorfismu prostoru U je identický automorfismus prostoru U^* , tj.

$$(1_U)^* = 1_{U^*} .$$

Pro každou formu $f \in U^*$ je totiž $(1_U)^*(f) = f \cdot 1_U = f$.

(ii) Jestliže F je homomorfismus prostoru U do prostoru V a G homomorfismus prostoru V do prostoru W , potom je F^*G^* duálním homomorfismem k homomorfismu GF , tj.

$$(GF)^* = F^*G^* .$$

Pro každou formu $f \in W^*$ je totiž

$$(GF)^*(f) = f(GF) = (fG)F = F^*(fG) = F^*(G^*(f)) = (F^*G^*)(f) .$$

(iii) Jestliže je F izomorfismus prostoru U na prostor V , potom je F^* izomorfismus prostoru V^* na prostor U^* a

$$(F^*)^{-1} = (F^{-1})^* .$$

Je totiž $F^{-1}F = 1_U$ a $FF^{-1} = 1_V$, podle (i) a (ii) je

$$F^*(F^{-1})^* = 1_{U^*} \quad \text{a} \quad (F^{-1})^*F^* = 1_{V^*} ,$$

tj. F^* je izomorfismus a $(F^*)^{-1} = (F^{-1})^*$.

21.24. Věta. *Nechť U a V jsou vektorové prostory nad tělesem T . Zobrazení $*$, které každému homomorfismu F prostoru U do prostoru V přiřazuje jeho duální homomorfismus F^* , je monomorfismus vektorového prostoru $\text{Hom}(U, V)$ do vektorového prostoru $\text{Hom}(V^*, U^*)$.*

Důkaz. Máme dokázat, že pro každé dva homomorfismy $F, G \in \text{Hom}(U, V)$ a každý skalár $a \in T$ platí rovnosti

$$(F + G)^* = F^* + G^* , \quad (aF)^* = a \cdot F^* .$$

Jestliže $f \in V^*$, potom je

$$(F + G)^*(f) = f(F + G) = fF + fG = F^*(f) + G^*(f) = (F^* + G^*)(f) ,$$

$$(aF)^*(f) = f(aF) = a \cdot (fF) = a \cdot F^*(f) = (a \cdot F^*)(f) ,$$

takže uvažované rovnosti platí a zobrazení $*$ je homomorfismus.

Nyní dokážeme, že jádro tohoto homomorfismu je nulové; uvědomíme si, že pro nenulový homomorfismus $F \in \text{Hom}(U, V)$ je duální homomorfismus F^* také nenulový. Je-li F nenulový, existuje vektor $u \in U$, takový, že $F(u)$ je nenulový vektor prostoru V . Nechť $f \in V^*$ je forma taková, že $\langle F(u), f \rangle \neq 0$ (viz 21.4). Nyní je

$$\langle u, F^*(f) \rangle = \langle F(u), f \rangle \neq 0 ,$$

takže forma $F^*(f) \in U^*$ je nenulová a tedy i homomorfismus F^* je nenulový. \square

21.25. Věta. *Nechť F je homomorfismus prostoru U do prostoru V a F^* homomorfismus k němu duální. Potom platí:*

- (i) *F je epimorfismus, právě když je F^* monomorfismus.*
- (ii) *F je monomorfismus, právě když je F^* epimorfismus.*

Důkaz. Jestliže je F epimorfismus, pak existuje homomorfismus G prostoru V do prostoru U , pro který $FG = 1_V$ (viz 10.14). Je tedy $(FG)^* = (1_V)^*$, podle 21.23 je $G^*F^* = 1_{V^*}$ a F^* je podle věty 10.15 monomorfismus.

Jestliže je F monomorfismus, pak existuje homomorfismus G prostoru V do prostoru U , pro který $GF = 1_U$ (viz 10.15). Je tedy $(GF)^* = (1_U)^*$, podle 21.23 je $F^*G^* = 1_{U^*}$ a F^* je epimorfismus podle věty 10.14.

Nechť F^* je epimorfismus a $u \in U$ nenulový vektor. Pak existuje forma $g \in U^*$ taková, že $\langle u, g \rangle \neq 0$. Protože je F^* epimorfismus, existuje forma $f \in V^*$, pro kterou $F^*(f) = g$. Nyní je

$$\langle F(u), f \rangle = \langle u, F^*(f) \rangle = \langle u, g \rangle \neq 0,$$

takže $F(u) \neq o$. Homomorfismus F je monomorfismus, neboť každý nenulový vektor zobrazuje na nenulový vektor.

Nechť F^* je monomorfismus. Předpokládejme, že $F(U) \neq V$, tj. F není epimorfismus. Nechť $f \in V^*$ je nenulová forma, která je na celém podprostoru $F(U)$ rovna nule (viz 21.4), tj. pro každé $u \in U$ je $\langle F(u), f \rangle = 0$. Protože je F^* monomorfismus, je $F^*(f) \in U^*$ nenulová forma a existuje vektor $u \in U$ takový, že $\langle u, F^*(f) \rangle \neq 0$. To je však spor s rovností

$$\langle u, F^*(f) \rangle = \langle F(u), f \rangle. \quad \square$$

21.26. Věta. *Nechť U, V jsou vektorové prostory konečných dimenzí nad tělesem T , nechť M, N jsou jejich báze a M^*, N^* báze prostorů U^*, V^* , které jsou duální k bázím M, N . Jestliže homomorfismus F prostoru U do prostoru V má vzhledem k bázím M, N matici A , potom duální homomorfismus F^* prostoru V^* do prostoru U^* má vzhledem k bázím N^*, M^* matici A^T .*

Důkaz. Nechť A je matice homomorfismu F vzhledem k bázím M, N a B je matice homomorfismu F^* vzhledem k bázím N^*, M^* . Jestliže f je i -tý prvek báze N^* , potom i -tý sloupec matice B je vektor $\langle F^*(f) \rangle_{M^*}$. Podle 21.10 je tento vektor roven matici formy $F^*(f)$ vzhledem k bázi M . Matice formy $F^*(f) = fF$ vzhledem k bázi M je dále rovna součinu CA matice C formy f vzhledem k bázi N a matice A homomorfismu F vzhledem k bázím M a N .

V matici C je na i -tém místě jednička a jinak samé nuly, neboť forma f je i -tým prvkem báze N^* , která je duální k bázi N , takže výsledný součin CA je roven i -tému řádku matice A . Ukázali jsme tedy, že i -tý sloupec matice B je roven i -tému řádku matice A , tj. $B = A^T$. \square

21.27. Důsledek. *Nechť U je vektorový prostor konečné dimenze, M, N jeho dvě báze a M^*, N^* báze duálního prostoru U^* , které jsou k nim duální. Jestliže A je matice přechodu od báze M k bázi N , potom $(A^T)^{-1}$ je matice přechodu od báze M^* k bázi N^* .*

Důkaz. Protože je matice A maticí identického automorfismu 1_U prostoru U vzhledem k bázím M, N , je podle předchozí věty matice A^T maticí homomorfismu $(1_U)^* = 1_{U^*}$ vzhledem k bázím N^* a M^* , tj. maticí přechodu od báze N^* k bázi M^* . Matice $(A^T)^{-1}$ je tedy maticí přechodu od báze M^* k bázi N^* . \square

21.28. Důsledek. *Nechť U, V jsou prostory konečných dimenzí a F homomorfismus prostoru U do prostoru V . Potom je hodnota homomorfismu F stejná jako hodnota homomorfismu F^* k němu duálního.*

Důkaz. Tvrzení vyplývá z věty 21.26 a věty 12.4. \square

Stejně jako jsme od vektorového prostoru V dvojí dualizací dospěli k vektorovému prostoru V^{**} , dojdeme od homomorfismu F prostoru U do prostoru V dvojí dualizací k homomorfismu F^{**} prostoru U^{**} do prostoru V^{**} . Následující věta vyjasňuje vztah homomorfismů F a F^{**} .

21.29. Věta. *Nechť U a V jsou vektorové prostory nad tělesem T a Φ_U , resp. Φ_V kanonická zobrazení prostoru U do prostoru U^{**} , resp. prostoru V do prostoru V^{**} . Pro každý homomorfismus F prostoru U do prostoru V je diagram*

$$\begin{array}{ccc} V & \xleftarrow{F} & U \\ \Phi_V \downarrow & & \downarrow \Phi_U \\ V^{**} & \xleftarrow{F^{**}} & U^{**} \end{array}$$

*komutativní, tj. $\Phi_V \cdot F = F^{**} \cdot \Phi_U$.*

Důkaz. Rovnost $\Phi_V \cdot F = F^{**} \cdot \Phi_U$ dokážeme, když ověříme, že pro libovolný vektor $u \in U$ platí rovnost

$$(\Phi_V \cdot F)(u) = (F^{**} \cdot \Phi_U)(u) ,$$

neboli vzhledem k definici kanonických zobrazení Φ_U a Φ_V

$$(F(u))^{**} = F^{**}(u^{**}) .$$

Na obou stranách této rovnosti jsou prvky prostoru V^{**} , tj. lineární formy na prostoru V^* . Jejich rovnost dokážeme, když ověříme, že pro libovolný prvek $f \in V^*$ je

$$\langle f, (F(u))^{**} \rangle = \langle f, F^{**}(u^{**}) \rangle .$$

Levá strana je podle definice kanonického zobrazení rovna $\langle F(u), f \rangle$. Pravou stranu upravíme s přihlédnutím k definicím duálního homomorfismu a kanonického zobrazení:

$$\langle f, F^{**}(u^{**}) \rangle = \langle F^*(f), u^{**} \rangle = \langle u, F^*(f) \rangle = \langle F(u), f \rangle$$

Platí tedy rovnost $\Phi_V \cdot F = F^{**} \cdot \Phi_U$, tj. výše uvedený diagram je opravdu komutativní. \square

Pokud prostory U, V chápeme jako podprostory prostorů U^{**}, V^{**} (viz 21.20), můžeme tvrzení předchozí věty vyslovit takto:

*Homomorfismus F^{**} je rozšířením homomorfismu F , tj. pro každé $u \in U$ je $F^{**}(u) = F(u)$.*

Jestliže má prostor U konečnou dimenzi, potom je $U^{**} = U$ a $F^{**} = F$.

Jsou-li U, V prostory konečných dimenzí, je $U^{**} = U$, $V^{**} = V$, $F^{**} = F$ a homomorfismy F a F^* jsou navzájem duální.

21.30. Poznámka. Zobrazení $"^*$ ", které každému prostoru V přiřazuje duální prostor V^* a každému homomorfismu F duální homomorfismus F^* je vzhledem k 21.23(i), (ii) *kontravariantním funktorem* kategorie \mathcal{C} všech vektorových prostorů nad daným tělesem T do téže kategorie \mathcal{C} . Tento funktor je podle věty 21.24 *aditivní* a *věrný*.

Přiřadíme-li každému prostoru V kanonické zobrazení Φ_V prostoru V do prostoru V^{**} , dostáváme podle 21.29 *transformaci* identického funktoru a druhé mocniny funktoru $"^*$ ".

21.31. Definice. Nechť V je vektorový prostor nad tělesem T . *Anihilátorem* M^0 podmnožiny M prostoru V nazveme množinu všech lineárních forem na prostoru V , které mají nulovou hodnotu ve všech vektorech množiny M , tj.

$$M^0 = \{f \in V^*; \forall v \in M \quad \langle v, f \rangle = 0\} .$$

Anihilátorem 0K podmnožiny K prostoru V^* nazveme množinu všech vektorů prostoru V , na kterých mají všechny formy množiny K nulové hodnoty, tj.

$${}^0K = \{v \in V; \forall f \in K \quad \langle v, f \rangle = 0\} .$$

21.32. Vlastnosti anihilátorů. Nechť V je vektorový prostor nad tělesem T . Potom platí:

$$(i) \quad V^0 = O, \quad O^0 = V^*, \quad {}^0(V^*) = O, \quad {}^0O = V .$$

(ii) Jestliže $f \in V^*$ a $v \in V$, potom je

$${}^0\{f\} = \text{Ker } f ,$$

$$\{v\}^0 = \{f \in V^*; \langle v, f \rangle = 0\} = \{f \in V^*; \langle f, v^{**} \rangle = 0\} = \text{Ker } v^{**} ,$$

kde $v^{**} \in V^{**}$ je obraz vektoru $v \in V$ při kanonickém zobrazení Φ prostoru V do prostoru V^{**} .

(iii) Jestliže je M podmnožina prostoru V a K podmnožina prostoru V^* , potom

$$M^0 = \bigcap_{v \in M} \{v\}^0 = \bigcap_{v \in M} \text{Ker } v^{**} ,$$

$${}^0K = \bigcap_{f \in K} {}^0\{f\} = \bigcap_{f \in K} \text{Ker } f .$$

Anihilátor M^0 , resp. 0K je tedy podprostorem prostoru V^* , resp. V .

(iv) Jsou-li $M_1 \subseteq M_2$ podmnožiny prostoru V a $K_1 \subseteq K_2$ podmnožiny prostoru V^* , potom je

$$M_2^0 \subseteq M_1^0 \quad \text{a} \quad {}^0K_2 \subseteq {}^0K_1 .$$

Tato dvě tvrzení vyplývají ihned z definice 21.31, resp. z rovností uvedených v (iii).

(v) Jestliže je M podmnožina prostoru V a K podmnožina prostoru V^* , potom je

$$M^0 = [M]^0 \quad \text{a} \quad {}^0K = {}^0[K] .$$

Z inkluze $M \subseteq [M]$ vyplývá podle (iv) inkluze $[M]^0 \subseteq M^0$. Jestliže forma f leží v anihilátoru M^0 , pak má nulové hodnoty na všech vektorech množiny M a tedy i na jejich lineárních kombinacích, takže leží i v anihilátoru $[M]^0$. Stejně se dokáže druhá rovnost.

(vi) Pro každou podmnožinu M prostoru V je

$$[M] = {}^0(M^0) .$$

Inkluze $M \subseteq {}^0(M^0)$ triviálně vyplývá z definice anihilátorů. Protože je každý anihilátor podprostorem, plyne odtud inkluze $[M] \subseteq {}^0(M^0)$. Jestliže vektor $v \in V$ neleží v $[M]$, existuje podle 21.4 forma f , která je nulová na podprostoru $[M]$ a pro kterou je $f(v) \neq 0$. Tedy $f \in M^0$, $v \notin {}^0(M^0)$ a rovnost $[M] = {}^0(M^0)$ platí.

(vii) Jsou-li M_1, M_2 podmnožiny prostoru V , pro které je $M_1^0 = M_2^0$, potom je $[M_1] = [M_2]$.

Z rovnosti $M_1^0 = M_2^0$ totiž vyplývá podle (vi)

$$[M_1] = {}^0(M_1^0) = {}^0(M_2^0) = [M_2] .$$

(viii) Pro podmnožinu M prostoru V platí:

$$M^0 = V^* \text{ právě tehdy, když } [M] = O ,$$

$$M^0 = O \text{ právě tehdy, když } [M] = V .$$

Jestliže je $M^0 = V^*$, pak $M^0 = O^0$ a podle (vii) je $[M] = O$. Jestliže je $[M] = O$, pak je podle (v) a (i) $M^0 = O^0 = V^*$. Druhá ekvivalence se dokáže stejně.

(ix) Jestliže je K podmnožina prostoru V^* , potom je

$$[K] \subseteq ({}^0K)^0 .$$

Inkluze $K \subseteq ({}^0K)^0$ vyplývá z definice anihilátorů; protože je každý anihilátor podprostorem, je $[K] \subseteq ({}^0K)^0$.

Rovnost v uvedené inkluzi obecně neplatí. Předpokládejme, že má prostor V nekonečnou dimenzi, $\{v_\alpha; \alpha \in \Lambda\}$ je jeho báze a $N = \{f_\alpha; \alpha \in \Lambda\}$ je lineárně nezávislá podmnožina prostoru V^* (viz 21.14 a 21.19) definovaná rovnostmi

$$\forall \alpha, \beta \in \Lambda \quad f_\alpha(v_\beta) = \delta_{\alpha\beta} .$$

Zřejmě je ${}^0N = O$, $({}^0N)^0 = O^0 = V^*$ a přitom (viz 21.14) je $[N] \neq ({}^0N)^0 = V^*$. Ukažme ještě méně triviální příklad. Zvolme pevně nějaké $\gamma \in \Lambda$. Jestliže

$$K = \{f_\alpha; \alpha \in \Lambda, \alpha \neq \gamma\} ,$$

pak ${}^0K = [v_\gamma]$ a anihilátor $({}^0K)^0$ obsahuje mimo podprostor $[K]$ ještě velké množství forem, které mají nulovou hodnotu ve vektoru v_γ a na ostatních vektorech v_α , $\alpha \in \Lambda$, $\alpha \neq \gamma$, mají nekonečně mnoho nenulových hodnot.

Tvrzení (ix) tedy nekorresponduje přesně s tvrzením (vi) a nelze tedy pro druhý typ anihilátoru dokázat obdobu tvrzení (vii).

(x) Jestliže je K podmnožina prostoru V^* , pak ${}^0K = V$ právě když $[K] = O$.

Jestliže je ${}^0K = V$, pak podle (ix) je $[K] \subseteq ({}^0K)^0 = V^0 = O$. Jestliže je $[K] = O$, pak je podle (v) a (i) ${}^0K = {}^0O = V$.

Rovnost ${}^0K = O$ není ekvivalentní s rovností $[K] = V^*$; jestliže je $[K] = V^*$, pak je ${}^0K = O$, ale opak obecně neplatí. To jsme viděli již v předchozím bodu (ix), kde je ${}^0N = O$ a $[N] \neq V^*$.

21.33. Věta. *Nechť V je vektorový prostor nad tělesem T .*

(i) *Jestliže má prostor V konečnou dimenzi, pak pro každou podmnožinu M prostoru V platí rovnost*

$$\dim V = \dim[M] + \dim M^0$$

a pro každou podmnožinu K prostoru V^ platí rovnosti*

$$\dim V = \dim[K] + \dim {}^0K , \quad [K] = ({}^0K)^0 .$$

(ii) *Jestliže má prostor V nekonečnou dimenzi, pak pro každou podmnožinu M prostoru V platí*

$$\dim V \leq \dim[M] + \dim M^0 \leq \dim V^* .$$

Důkaz.

(i) Nechť $\{v_1, \dots, v_k\}$ je báze podprostoru $[M]$ a $\{v_1, \dots, v_n\}$ báze prostoru V . Nechť dále $\{f_1, \dots, f_n\}$ je báze prostoru V^* , která je duální k bázi $\{v_1, \dots, v_n\}$. Jestliže forma

$$f = a_1 f_1 + \dots + a_k f_k + \dots + a_n f_n$$

leží v anihilátoru M^0 podprostoru $[M]$, potom je

$$f(v_1) = a_1 = 0, \quad \dots, \quad f(v_k) = a_k = 0.$$

Na druhé straně je zřejmě $f_{k+1}, \dots, f_n \in M^0$, takže je $M^0 = [f_{k+1}, \dots, f_n]$ a

$$\dim V = n = k + (n - k) = \dim[M] + \dim M^0.$$

Druhá rovnost se dokáže obdobně. Nakonec je podle obou rovností (položíme $[M] = {}^0K$)

$$\dim V = \dim[K] + \dim {}^0K = \dim {}^0K + \dim ({}^0K)^0,$$

takže $\dim[K] = \dim ({}^0K)^0$ a vzhledem k 21.32(ix) je $[K] = ({}^0K)^0$.

(ii) Nechť $\{v_\alpha; \alpha \in \Lambda\}$ je báze prostoru V , přičemž $\{v_\alpha; \alpha \in \Lambda_1\}$ je báze podprostoru $[M]$. Nechť dále $\{f_\alpha; \alpha \in \Lambda\}$ je lineárně nezávislá podmnožina prostoru V^* (viz 21.14 a 21.19) definovaná rovnostmi

$$\forall \alpha, \beta \in \Lambda \quad f_\alpha(v_\beta) = \delta_{\alpha\beta}.$$

Jestliže nějaká lineární kombinace forem f_α , $\alpha \in \Lambda$, leží v anihilátoru M^0 , pak neobsahuje nenulové násobky forem f_α , $\alpha \in \Lambda_1$ (stejně jako v případě (i), kdy šlo o konečnou dimenzi). Na druhé straně je zřejmě $\{f_\alpha; \alpha \in \Lambda \setminus \Lambda_1\} \subseteq M^0$. Tuto lineárně nezávislou množinu rozšíříme na bázi

$$\{f_\alpha; \alpha \in (\Lambda \setminus \Lambda_1) \cup \Lambda_2\}$$

anihilátoru M^0 . Množiny Λ a Λ_2 jsou zřejmě disjunktní. Množina $\{f_\alpha; \alpha \in \Lambda \cup \Lambda_2\}$ je lineárně nezávislá; je-li totiž $g_1 + g_2 = 0$, kde g_1 je lineární kombinace forem f_α , $\alpha \in (\Lambda \setminus \Lambda_1) \cup \Lambda_2$, a g_2 je lineární kombinace forem f_α , $\alpha \in \Lambda_1$, pak $g_1 = -g_2 \in M^0$, podle předchozího je $g_2 = 0$ a z lineární nezávislosti množin $\{f_\alpha; \alpha \in (\Lambda \setminus \Lambda_1) \cup \Lambda_2\}$ a $\{f_\alpha; \alpha \in \Lambda_1\}$ vyplývá, že lineární kombinace $g_1 + g_2$ je triviální. Množina $\{f_\alpha; \alpha \in \Lambda \cup \Lambda_2\}$ je tedy lineárně nezávislá, můžeme ji doplnit na bázi prostoru V^* . Nyní je

$$\begin{aligned} \dim V &= |\Lambda| = |\Lambda_1| + |\Lambda \setminus \Lambda_1| \leq \\ &\leq \dim[M] + \dim M^0 = |\Lambda_1| + |\Lambda \setminus \Lambda_1| + |\Lambda_2| = |\Lambda| + |\Lambda_2| \leq \dim V^*. \quad \square \end{aligned}$$

Odlíšnost vlastností (ix) a (vi) v 21.32 nás vede k následující definici.

21.34. Definice. Nechť V je vektorový prostor nad tělesem T . Podprostor W duálního prostoru V^* , pro který platí rovnost $({}^0W)^0 = W$, se nazývá *algebraicky saturovaný*.

21.35. Poznámka. Jsou-li W_1 a W_2 algebraicky saturované podprostory prostoru V^* , pak z rovnosti ${}^0W_1 = {}^0W_2$ vyplývá rovnost $W_1 = W_2$. Je totiž

$$W_1 = ({}^0W_1)^0 = ({}^0W_2)^0 = W_2 ,$$

podobně jako v tvrzení (vii) v 21.32.

Z věty 21.33(i) ihned vyplývá následující tvrzení. Jestliže má prostor V konečnou dimenzi, potom je každý podprostor duálního prostoru V^* algebraicky saturovaný.

Dva příklady podprostorů, které nejsou algebraicky saturované, jsme viděli v 21.32(ix).

21.36. Poznámka. Jestliže je K podmnožinou prostoru V^* , pak můžeme uvažovat i anihilátor K^0 obsahující všechny formy prostoru V^{**} , které jsou rovny nule na všech prvcích množiny K , tj.

$$K^0 = \{F \in V^{**}; \forall f \in K \quad \langle f, F \rangle = 0\} .$$

Vzhledem k tomu, že pro každý vektor $v \in V$ a každou formu $f \in V^*$ je

$$\langle v, f \rangle = \langle f, v^{**} \rangle ,$$

kde v^{**} je obraz vektoru v při kanonickém zobrazení Φ prostoru V do prostoru V^{**} , je

$$\Phi({}^0K) = \Phi(V) \cap K^0 .$$

Při ztotožnění prostorů V a $\Phi(V)$ monomorfismem Φ je tedy

$${}^0K = V \cap K^0 ;$$

má-li prostor V konečnou dimenzi, je $V = V^{**}$ a ${}^0K = K^0$.

Uvedme ještě do souvislosti anihilátory a duální homomorfismus. Následující věta říká, že jádro a obraz homomorfismu F^* jsou anihilátory obrazu a jádra homomorfismu F a naopak jádro a obraz homomorfismu F jsou anihilátory obrazu a jádra homomorfismu F^* . Podstatným způsobem tak věta 21.37 zobecňuje větu 21.25, která je jejím triviálním důsledkem.

21.37. Věta. *Nechť F je homomorfismus vektorového prostoru U do vektorového prostoru V a F^* homomorfismus k němu duální. Potom platí:*

- (i) $\text{Ker } F = {}^0(\text{Im } F^*)$, $\text{Im } F = {}^0(\text{Ker } F^*)$,
- (ii) $\text{Ker } F^* = (\text{Im } F)^0$, $\text{Im } F^* = (\text{Ker } F)^0$.

Důkaz. Forma $f \in V^*$ leží v $(\text{Im } F)^0$ právě tehdy, když pro každé $u \in U$ je $\langle F(u), f \rangle = 0$. Protože je však $\langle F(u), f \rangle = \langle u, F^*(f) \rangle$, je to ekvivalentní s rovností $F^*(f) = 0$ neboli $f \in \text{Ker } F^*$. Tedy $(\text{Im } F)^0 = \text{Ker } F^*$ a užitím 21.32(vi) dostáváme rovnost $\text{Im } F = {}^0(\text{Im } F)^0 = {}^0(\text{Ker } F^*)$.

Vektor $u \in U$ leží v ${}^0(\text{Im } F^*)$ právě tehdy, když pro každé $f \in V^*$

$$0 = \langle u, F^*(f) \rangle = \langle F(u), f \rangle ,$$

tj. právě když $F(u) = 0$, neboli $u \in \text{Ker } F$. Odtud $\text{Ker } F = {}^0(\text{Im } F^*)$. Podle 21.32(vi) je tedy

$$(\text{Ker } F)^0 = ({}^0(\text{Im } F^*))^0 \supseteq \text{Im } F^* .$$

Jestliže je $0 \neq g \in (\text{Ker } F)^0$, definujme $f \in V^*$ takto: Zvolme bázi N podprostoru $\text{Ker } F$, rozšířme ji na bázi M prostoru U . Lineárně nezávislou množinu $F(M \setminus N)$ rozšířme na bázi K prostoru V . Pro každé $u \in M \setminus N$ definujme

$$\langle F(u), f \rangle = \langle u, g \rangle ,$$

pro každé $v \in K \setminus F(M \setminus N)$ definujme $\langle v, f \rangle = 0$. Nyní je zřejmě pro každé $u \in M$

$$\langle u, F^*(f) \rangle = \langle F(u), f \rangle = \langle u, g \rangle ,$$

tj. $F^*(f) = g$ a $g \in \text{Im } F^*$. Dokázali jsme tedy i druhou inkluzi

$$(\text{Ker } F)^0 \subseteq \text{Im } F^* . \quad \square$$

21.38. Věta. *Nechť V je vektorový prostor dimenze n .*

- (i) *Každý m -dimenzionální podprostor W prostoru V je možno vyjádřit jako průnik $n - m$ podprostorů dimenze $n - 1$. Tyto podprostory lze chápat jako jádra lineárních forem f_1, \dots, f_{n-m} ; vektor $v \in V$ leží v podprostoru W právě tehdy, když*

$$f_1(v) = 0 , \quad \dots , \quad f_{n-m}(v) = 0 .$$

- (ii) *Každou m -dimenzionální lineární množinu $u + W$ prostoru V je možno vyjádřit jako průnik $n - m$ lineárních množin dimenze $n - 1$. Tyto lineární množiny lze vyjádřit pomocí vektoru u a jader lineárních forem f_1, \dots, f_{n-m} ; vektor $v \in V$ leží v lineární množině $u + W$ právě tehdy, když*

$$f_1(v) = f_1(u) , \quad \dots , \quad f_{n-m}(v) = f_{n-m}(u) .$$

Důkaz.

(i) Podle 21.32(vi) a 21.33(i) je $W = {}^0(W^0)$, kde $\dim W^0 = n - m$. Je-li $\{f_1, \dots, f_{n-m}\}$ báze prostoru W^0 , je podle 21.32(iii)

$$W = {}^0(W^0) = {}^0\{f_1, \dots, f_{n-m}\} = \bigcap_{i=1}^{n-m} \text{Ker } f_i .$$

Podprostor W je tedy průnikem $n - m$ podprostorů $\text{Ker } f_i$, $i = 1, \dots, n - m$, které mají dimenzi $n - 1$ (viz 21.3).

Uvědomme si, že se předchozí důkaz dá jednodušeji zapsat bez užití pojmu anihilátor. Nechť $\{v_1, \dots, v_m\}$ je báze podprostoru W , $N = \{v_1, \dots, v_m, \dots, v_n\}$ báze prostoru V a $\{g_1, \dots, g_n\}$ báze prostoru V^* , která je k bázi N duální. Snadno se ukáže, že vektor $x \in V$ leží v podprostoru W právě tehdy, když je

$$g_{m+1}(x) = \dots = g_{m+n}(x) = 0 .$$

(ii) Podle (i) je

$$W = \bigcap_{i=1}^{n-m} \text{Ker } f_i$$

a tedy

$$u + W = u + \bigcap_{i=1}^{n-m} \text{Ker } f_i = \bigcap_{i=1}^{n-m} (u + \text{Ker } f_i) .$$

Vektor $v \in V$ leží v lineární množině $u + W$ právě tehdy, když $v - u \in W$; to nastane podle (i) právě tehdy, když pro $i = 1, \dots, n - m$ je $f_i(v - u) = 0$ neboli $f_i(v) = f_i(u)$. \square

21.39. Poznámka. Buď dána homogenní soustava n lineárních rovnic o m neznámých nad tělesem T :

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m &= 0 , \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m &= 0 , \\ \dots & \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nm}x_m &= 0 . \end{aligned}$$

Na prostoru T^m definujme lineární formy f_1, f_2, \dots, f_n jejich analytickým vyjádřením vzhledem ke kanonické bázi:

$$\begin{aligned} f_1(x) &= a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m , \\ f_2(x) &= a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m , \\ \dots & \\ f_n(x) &= a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nm}x_m . \end{aligned}$$

Nalézt množinu všech řešení uvedené soustavy lineárních rovnic je tedy podle definice 21.31 totéž jako najít anihilátor ${}^0\{f_1, \dots, f_n\}$. Z předchozích výsledků tedy vyplývá následující zjištění o homogenních soustavách lineárních rovnic.

Množina všech řešení homogenní soustavy n lineárních rovnic o m neznámých nad tělesem T je podprostorem prostoru T^m , který má dimenzi

$$m - \dim [f_1, \dots, f_n] = m - \dim A ,$$

kde A je matice uvažované soustavy.

Tímto způsobem by bylo možno partii o soustavách lineárních rovnic vyložit na základě anihilátorů lineárních forem. V některých knížkách či učebnicích je právě tohoto způsobu užito.

21.40. Poznámka. Ve funkcionální analýze se lineárním formám říká *lineární funkcionály*. Je-li V reálný nebo komplexní vektorový prostor, pak duální prostor V^* se často značí V^f (prostor funkcionálů na prostoru V). Provedení formy $x' \in V^f$ na vektor $x \in V$ se značí $\langle x, x' \rangle$. S tímto bilineárním symbolem jsme již pracovali.

Na reálných vektorových prostorech se vyšetřují též tzv. *sublineární funkcionály*. Zobrazení f reálného vektorového prostoru V do tělesa \mathbb{R} se nazývá *sublineární funkcionál*, jestliže pro každé $x, y \in V$ a každé $a \in \mathbb{R}$, $a \geq 0$, platí:

$$f(x + y) \leq f(x) + f(y) , \quad f(ax) = a \cdot f(x) .$$

Často se vyšetřují rozšíření lineárních funkcionálů, která splňují některé další vlastnosti. Jako příklad můžeme uvést následující větu:

Nechť V je reálný vektorový prostor a W jeho podprostor. Nechť g je lineární funkcionál definovaný na W a f je sublineární funkcionál definovaný na celém prostoru V . Jestliže $g(x) \leq f(x)$ pro každé $x \in W$, pak existuje takové rozšíření G lineárního funkcionálu g na celý prostor V , že pro každé $x \in V$ je $G(x) \leq f(x)$.

22. SEMILINEÁRNÍ FORMY

NA KOMPLEXNÍCH PROSTORECH

V teorii komplexních vektorových prostorů se místo lineárních forem užívají tzv. semilineární formy.

Symbolem \bar{a} budeme v dalším rozumět komplexně sdružené číslo ke komplexnímu číslu a , symbolem $|a|$ budeme značit absolutní hodnotu (modul) tohoto čísla. Jestliže je tedy

$$a = \operatorname{Re} a + i \cdot \operatorname{Im} a ,$$

potom je

$$\bar{a} = \operatorname{Re} a - i \cdot \operatorname{Im} a , \quad |a| = \sqrt{(\operatorname{Re} a)^2 + (\operatorname{Im} a)^2} , \quad a \cdot \bar{a} = |a|^2 .$$

Připomeňme ještě, že pro libovolná dvě komplexní čísla a, b platí:

$$\overline{a+b} = \bar{a} + \bar{b} , \quad \overline{ab} = \bar{a} \cdot \bar{b} , \quad |ab| = |a| \cdot |b| .$$

22.1. Definice. Nechť V je komplexní vektorový prostor. *Semilineární formou* na prostoru V budeme rozumět každé zobrazení f prostoru V do tělesa \mathbb{C} , pro které platí:

- (i) $\forall x, y \in V \quad f(x+y) = f(x) + f(y)$,
- (ii) $\forall x \in V \quad \forall a \in \mathbb{C} \quad f(ax) = \bar{a} \cdot f(x)$.

Vlastnosti (i), (ii) je možno shrnout do jediné:

$$\forall x, y \in V \quad \forall a, b \in \mathbb{C} \quad f(ax + by) = \bar{a} \cdot f(x) + \bar{b} \cdot f(y)$$

Užitím matematické indukce dostaneme obecnou rovnost:

$$\forall x_1, \dots, x_n \in V \quad \forall a_1, \dots, a_n \in \mathbb{C} \quad f\left(\sum_{i=1}^n a_i x_i\right) = \sum_{i=1}^n \bar{a}_i \cdot f(x_i)$$

Semilineární formy na prostoru V jsou právě tzv. *semihomomorfismy*¹ prostoru V do prostoru \mathbb{C} . Zobrazení f prostoru V do tělesa \mathbb{C} je zřejmě semilineární formou právě tehdy, když je zobrazení \bar{f} , které vektoru $v \in V$ přiřadí číslo $\bar{f}(v)$, formou lineární.

¹ Semihomomorfismem komplexního prostoru U do komplexního prostoru V rozumíme zobrazení f , pro které platí

- (i) $\forall u_1, u_2 \in U \quad f(u_1 + u_2) = f(u_1) + f(u_2)$,
- (ii) $\forall u \in U \quad \forall a \in \mathbb{C} \quad f(au) = \bar{a} \cdot f(u)$.

Pro semihomomorfismy komplexních vektorových prostorů je možno zavést obdobné pojmy a dokázat obdobná tvrzení jako pro homomorfismy vektorových prostorů nad obecným tělesem T .

22.2. Příklady.

(i) Necht a_1, a_2, \dots, a_n jsou pevně zvolená komplexní čísla. Zobrazení f , které každému vektoru $x = (x_1, x_2, \dots, x_n) \in \mathbb{C}^n$ přiřazuje číslo

$$f(x) = a_1 \overline{x_1} + a_2 \overline{x_2} + \dots + a_n \overline{x_n} ,$$

je semilineární forma na prostoru \mathbb{C}^n .

(ii) Zobrazení f , které každé komplexní matici řádu n přiřazuje komplexně sdružené číslo k její stopě, tj.

$$f(A) = \overline{\operatorname{tr} A} ,$$

je semilineární forma na prostoru $\mathbb{C}^{n \times n}$. Tento příklad je vlastně modifikací příkladu (i).

(iii) Necht V je vektorový prostor komplexních funkcí reálné proměnné, které jsou spojité na intervalu $\langle a, b \rangle$, necht $\varphi \in V$ je daná funkce tohoto prostoru a $c \in \langle a, b \rangle$ pevně zvolené číslo. Zobrazení f , které každé funkci $p \in V$ přiřazuje číslo

$$f(p) = \overline{p(c)} ,$$

je semilineární formou na prostoru V . Semilineární formou na prostoru V je rovněž zobrazení g , které každé funkci $p \in V$ přiřazuje číslo

$$g(p) = \int_a^b \varphi(x) \overline{p(x)} dx .$$

(iv) Zobrazení f , které každému polynomu p s komplexními koeficienty přiřazuje komplexní číslo

$$f(p) = \sum_{i=1}^k a_i \overline{p(c_i)} ,$$

kde a_1, \dots, a_k a c_1, \dots, c_k jsou pevně zvolená komplexní čísla, je semilineární formou na prostoru $\mathbb{C}[x]$.

Pro semilineární formy můžeme zavést mnohé pojmy, které jsme zavedli pro formy lineární, a dokázat řadu tvrzení, která odpovídají obdobným tvrzením, která jsme v předchozím paragrafu zformulovali a dokázali pro formy lineární. Některá základní fakta uvedeme v následujícím přehledu (číslování odstavců odpovídá číslování užitému v předchozím paragrafu).

22.3. Poznámka. Nenulová semilineární forma f na komplexním vektorovém prostoru V je surjekce; je-li $\dim V = n$, je $d(f) = \dim \operatorname{Ker} f = n - 1$.

22.4. Poznámka. Každá semilineární forma na komplexním vektorovém prostoru V je určena svými hodnotami v libovolně zvolené bázi prostoru V .

22.5. Poznámka. Nechť V je komplexní prostor, $N = \{v_1, \dots, v_n\}$ jeho báze a nechť f je semilineární forma na prostoru V . *Maticí semilineární formy f vzhledem k bázi N* budeme rozumět matici

$$A = (f(v_1), f(v_2), \dots, f(v_n)).$$

Pro každý vektor $x \in V$, kde $\langle x \rangle_N = (x_1, x_2, \dots, x_n)$, je

$$f(x) = A \cdot \overline{\langle x \rangle}_N^T = f(v_1) \cdot \overline{x_1} + f(v_2) \cdot \overline{x_2} + \dots + f(v_n) \cdot \overline{x_n}.$$

Této rovnosti se říká *analytické vyjádření* semilineární formy f vzhledem k bázi N (srovnej s příkladem 22.2(i)).

Součet dvou semilineárních forem a násobek semilineární formy komplexním číslem jsou opět semilineární formy. Množina všech semilineárních forem na komplexním vektorovém prostoru V tvoří komplexní vektorový prostor.

22.6. Definice. Nechť V je komplexní vektorový prostor. Vektorový prostor V^\sim všech semilineárních forem na prostoru V budeme nazývat *semiduálním prostorem* k prostoru V .

22.7. Věta. *Jestliže má komplexní vektorový prostor V konečnou dimenzi, pak se dimenze prostorů V a V^\sim rovnají.*

22.8. Definice. Říkáme, že báze $\{f_1, \dots, f_n\}$ prostoru V^\sim je *semiduální* k bázi $\{v_1, \dots, v_n\}$ prostoru V , jestliže pro každé $i, j = 1, \dots, n$ je

$$f_i(v_j) = \delta_{ij}.$$

22.9. Věta. *Ke každé bázi komplexního vektorového prostoru V konečné dimenze existuje právě jediná báze prostoru V^\sim , která je k ní semiduální.*

Na závěr uvedeme dva odstavce, které odpovídají odstavcům 21.15 a 21.16 předchozího paragrafu.

22.15. Poznámka. Provedení semilineární formy $f \in V^\sim$ na vektor $v \in V$ značíme $\langle f, v \rangle$. Symbolem $\langle \cdot, \cdot \rangle$ můžeme označit zobrazení kartézského součinu prostorů V^\sim a V do tělesa komplexních čísel, které každému vektoru $v \in V$ a každé semilineární formě $f \in V^\sim$ přiřazuje komplexní číslo $\langle f, v \rangle = f(v)$. Toto zobrazení má následující vlastnosti:

- (i) $\forall v_1, v_2 \in V \quad \forall f \in V^\sim \quad \langle f, v_1 + v_2 \rangle = \langle f, v_1 \rangle + \langle f, v_2 \rangle,$
- (ii) $\forall v \in V \quad \forall a \in \mathbb{C} \quad \forall f \in V^\sim \quad \langle f, av \rangle = \overline{a} \cdot \langle f, v \rangle,$
- (iii) $\forall v \in V \quad \forall f_1, f_2 \in V^\sim \quad \langle f_1 + f_2, v \rangle = \langle f_1, v \rangle + \langle f_2, v \rangle,$
- (iv) $\forall v \in V \quad \forall a \in \mathbb{C} \quad \forall f \in V^\sim \quad \langle af, v \rangle = a \cdot \langle f, v \rangle.$

První dvě vlastnosti vznikly přepisem faktu, že f je semilineární forma (viz definice 22.1), třetí je přepisem definice součtu dvou semilineárních forem a čtvrtá přepisem definice násobku semilineární formy komplexním číslem. Říkáme, že zobrazení

$$\langle \cdot, \cdot \rangle : V^\sim \times V \longrightarrow \mathbb{C}$$

je lineární v první složce a semilineární v druhé složce.

22.16. Poznámka. Semiduální prostor k prostoru V^\sim značíme $V^{\sim\sim}$. Kanonickým zobrazením prostoru V do prostoru $V^{\sim\sim}$ rozumíme zobrazení Φ , které vektoru $v \in V$ přiřadí takovou semilineární formu $\Phi(v) = v^{\sim\sim}$ na prostoru V^\sim , že pro každé $f \in V^\sim$ je

$$v^{\sim\sim}(f) = f(v) .$$

Kanonické zobrazení Φ je prostý semihomomorfismus; vzájemně jednoznačný je právě tehdy, když má prostor V konečnou dimenzi.

Rovnost, která definuje obraz $v^{\sim\sim}$ vektoru v při kanonickém zobrazení Φ , může být zapsána v tvaru

$$\langle v^{\sim\sim}, f \rangle = \langle f, v \rangle .$$

23. BILINEÁRNÍ A KVADRATICKÉ FORMY

23.1. Definice. Nechť V je vektorový prostor nad tělesem T . *Bilineární formou* na prostoru V budeme rozumět každé zobrazení f kartézského součinu $V \times V$ do tělesa T , pro které platí:

- (i) $\forall x, y, z \in V \quad f(x + y, z) = f(x, z) + f(y, z)$,
- (ii) $\forall x, y \in V \quad \forall a \in T \quad f(ax, y) = a \cdot f(x, y)$,
- (iii) $\forall x, y, z \in V \quad f(x, y + z) = f(x, y) + f(x, z)$,
- (iv) $\forall x, y \in V \quad \forall a \in T \quad f(x, ay) = a \cdot f(x, y)$.

První dvě vlastnosti představují *linearitu* formy f v *první složce*, druhé dvě *linearitu* formy f v *druhé složce*. Definující vlastnosti bilineární formy f je možno shrnout (podobně jako u forem lineárních):

$$\begin{aligned} \forall x, y, z \in V \quad \forall a, b \in T \quad f(ax + by, z) &= a \cdot f(x, z) + b \cdot f(y, z), \\ \forall x, y, z \in V \quad \forall a, b \in T \quad f(x, ay + bz) &= a \cdot f(x, y) + b \cdot f(x, z), \end{aligned}$$

nebo

$$\forall x_1, x_2, y_1, y_2 \in V \quad \forall a, b, c, d \in T$$

$$f(ax_1 + bx_2, cy_1 + dy_2) = ac \cdot f(x_1, y_1) + ad \cdot f(x_1, y_2) + bc \cdot f(x_2, y_1) + bd \cdot f(x_2, y_2).$$

Užitím matematické indukce dostaneme obecnou podmínku:

$$\forall x_1, \dots, x_r, y_1, \dots, y_s \in V \quad \forall a_1, \dots, a_r, b_1, \dots, b_s \in T$$

$$f\left(\sum_{i=1}^r a_i x_i, \sum_{j=1}^s b_j y_j\right) = \sum_{i=1}^r \sum_{j=1}^s a_i b_j \cdot f(x_i, y_j)$$

23.2. Příklady.

(i) Nejjednodušší bilineární formou na vektorovém prostoru V je tzv. *nulová* bilineární forma, která každé dvojici vektorů prostoru V přiřazuje nulový prvek tělesa T . Ostatní bilineární formy na prostoru V se nazývají *nenulové*.

(ii) Jsou-li g_1, g_2 lineární formy na prostoru V , potom zobrazení f , které každé dvojici $(x, y) \in V \times V$ přiřazuje skalár $f(x, y) = g_1(x) \cdot g_2(y)$, je bilineární forma na prostoru V .

(iii) Nechť V je vektorový prostor všech funkcí reálné proměnné, které jsou spojitě na uzavřeném intervalu $\langle a, b \rangle$, nechť k je pevně zvolená funkce dvou reálných proměnných, která je spojitá na intervalu $\langle a, b \rangle \times \langle a, b \rangle$. Zobrazení f , které každým dvěma funkcím $p, q \in V$ přiřazuje reálné číslo

$$f(p, q) = \int_a^b \int_a^b k(x, y)p(x)q(y) dx dy,$$

je bilineární forma na prostoru V . Jestliže je funkce k identicky rovna jedné, je

$$f(p, q) = \int_a^b \int_a^b p(x)q(y) dx dy = \int_a^b p(x) dx \cdot \int_a^b q(y) dy = g(p) \cdot g(q) ;$$

bilineární forma f je zřejmě vytvořena pomocí lineární formy g na prostoru V , která je definovaná rovností

$$g(p) = \int_a^b p(x) dx ,$$

ve smyslu předchozího příkladu (ii).

(iv) Nechť $A = (a_{ij})$ je čtvercová matice řádu n nad tělesem T . Zobrazení f , které každým dvěma vektorům $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ prostoru T^n přiřadí skalár

$$f(x, y) = \sum_{i,j=1}^n a_{ij}x_iy_j = (x_1, \dots, x_n) \cdot A \cdot (y_1, \dots, y_n)^T,$$

je bilineární forma na prostoru T^n .

Nechť V je vektorový prostor nad tělesem T a M jeho báze. Každá bilineární forma na prostoru V (tj. zobrazení množiny $V \times V$ do tělesa T s určitými vlastnostmi) určuje zřejmým způsobem (zúžením) zobrazení množiny $M \times M$ do tělesa T . Následující věta říká, že naopak každé zobrazení množiny $M \times M$ do tělesa T určuje bilineární formu na prostoru V .

23.3. Věta. *Nechť V je vektorový prostor nad tělesem T a M jeho báze. Potom platí:*

- (i) *Každé zobrazení množiny $M \times M$ do tělesa T je možno právě jediným způsobem rozšířit na bilineární formu na prostoru V .*
- (ii) *Každá bilineární forma na prostoru V je jednoznačně určena svými hodnotami na množině $M \times M$.*

Důkaz. Nechť $M = \{v_\alpha; \alpha \in \Lambda\}$ je báze prostoru V a g zobrazení množiny $M \times M$ do tělesa T . Nechť x, y jsou libovolně zvolené vektory prostoru V ; pišme

$$x = \sum_{\alpha \in \Lambda} x_\alpha v_\alpha , \quad y = \sum_{\beta \in \Lambda} y_\beta v_\beta$$

(skoro všechny koeficienty x_α a skoro všechny koeficienty y_β jsou rovny nule, tj. jde o lineární kombinace vektorů báze M zapsané — pokud je množina Λ nekonečná — formálně nekonečnými součty). Pro bilineární formu f , která rozšiřuje zobrazení g , musí být

$$\begin{aligned} f(x, y) &= f\left(\sum_{\alpha \in \Lambda} x_\alpha v_\alpha, \sum_{\beta \in \Lambda} y_\beta v_\beta\right) = \\ &= \sum_{\alpha, \beta \in \Lambda} x_\alpha y_\beta \cdot f(v_\alpha, v_\beta) = \sum_{\alpha, \beta \in \Lambda} x_\alpha y_\beta \cdot g(v_\alpha, v_\beta) . \end{aligned}$$

Je tedy jasné, že jediná možnost, jak rozšířit zobrazení g na bilineární formu f , je položit

$$f(x, y) = \sum_{\alpha, \beta \in \Lambda} x_\alpha y_\beta \cdot g(v_\alpha, v_\beta) . \quad (1)$$

K dokončení důkazu stačí ukázat, že takto definované zobrazení f je opravdu bilineární formou. Jestliže je ještě $x' \in V$,

$$x' = \sum_{\alpha \in \Lambda} x'_\alpha v_\alpha ,$$

a $c \in T$, pak je podle (1)

$$\begin{aligned} f(x + x', y) &= \sum_{\alpha, \beta \in \Lambda} (x_\alpha + x'_\alpha) y_\beta \cdot g(v_\alpha, v_\beta) = \\ &= \sum_{\alpha, \beta \in \Lambda} x_\alpha y_\beta \cdot g(v_\alpha, v_\beta) + \sum_{\alpha, \beta \in \Lambda} x'_\alpha y_\beta \cdot g(v_\alpha, v_\beta) = f(x, y) + f(x', y) , \end{aligned}$$

$$f(cx, y) = \sum_{\alpha, \beta \in \Lambda} (cx_\alpha) y_\beta \cdot g(v_\alpha, v_\beta) = c \cdot \sum_{\alpha, \beta \in \Lambda} x_\alpha y_\beta \cdot g(v_\alpha, v_\beta) = c \cdot f(x, y) .$$

Stejně se dokáže linearita v druhé složce. Zobrazení f definované rovností (1) je tedy bilineární forma rozšiřující zobrazení g .

Druhé tvrzení věty ihned vyplývá z tvrzení prvního. \square

V případě, kdy má vektorový prostor V konečnou dimenzi, sestavujeme hodnoty bilineární formy na množině $M \times M$ do čtvercové matice.

23.4. Definice. Nechť V je vektorový prostor nad tělesem T a $M = \{v_1, \dots, v_n\}$ jeho báze, nechť f je bilineární forma na prostoru V . *Maticí bilineární formy f vzhledem k bázi M* budeme rozumět čtvercovou matici $A = (a_{ij})$ řádu n , která má na místě ij hodnotu formy f v i -tém a j -tém vektoru báze M , tj. pro každé $i, j = 1, \dots, n$ je

$$a_{ij} = f(v_i, v_j) .$$

Z věty 23.3 vyplývá, že každá bilineární forma je jednoznačně určena svou maticí (vzhledem ke zvolené bázi). Následující věta tento fakt ještě upřesňuje a zdůrazňuje.

23.5. Věta. *Nechť V je vektorový prostor dimenze n nad tělesem T a M jeho báze, nechť f je bilineární forma na prostoru V a A čtvercová matice řádu n nad tělesem T . Matice A je maticí formy f vzhledem k bázi M právě tehdy, když pro každé dva vektory $x, y \in V$ je*

$$f(x, y) = \langle x \rangle_M \cdot A \cdot \langle y \rangle_M^T . \quad (2)$$

23.7. Věta. *Nechť V je vektorový prostor konečné dimenze nad tělesem T , nechť M a M' jsou jeho báze a f bilineární forma na prostoru V . Jestliže A je matricí formy f vzhledem k bázi M , potom $B^T AB$ je matricí formy f vzhledem k bázi M' , kde B je matice přechodu od báze M' k bázi M .*

Důkaz. Jestliže je A matricí formy f vzhledem k bázi M , potom podle věty 23.5 platí pro každé dva vektory x, y prostoru V rovnost

$$f(x, y) = \langle x \rangle_M \cdot A \cdot \langle y \rangle_M^T. \quad (2)$$

Jestliže je B matice přechodu od báze M' k bázi M , pak pro transformaci souřadnic vektorů x a y platí (viz 11.7):

$$\begin{aligned} \langle x \rangle_M^T &= B \cdot \langle x \rangle_{M'}^T, & \text{tj.} & \quad \langle x \rangle_M = \langle x \rangle_{M'} \cdot B^T, \\ \langle y \rangle_M^T &= B \cdot \langle y \rangle_{M'}^T. \end{aligned}$$

Dosazením za $\langle x \rangle_M$ a $\langle y \rangle_M^T$ do rovnosti (2) dostáváme, že pro každé dva vektory $x, y \in V$ je

$$f(x, y) = \langle x \rangle_{M'} \cdot B^T \cdot A \cdot B \cdot \langle y \rangle_{M'}^T,$$

a podle věty 23.5 (nyní užíváme opačnou implikaci než na začátku důkazu) je tedy matice $B^T AB$ matricí formy f vzhledem k bázi M' . \square

23.8. Důsledek. *Všechny matice bilineární formy f (vzhledem k různým bázím) mají stejnou hodnotu.*

Důkaz. Tvzení vyplývá z předchozí věty, věty 12.6 a věty 12.26. \square

Právě zjištěná skutečnost nás opravňuje k definici hodnoty a nulity bilineární formy.

23.9. Definice. *Nechť f je bilineární forma na vektorovém prostoru V konečné dimenze. Hodnotí $r(f)$ formy f budeme rozumět hodnotu některé její matice. Nulitou nebo defektem $d(f)$ formy f budeme rozumět doplněk hodnoty $r(f)$ do dimenze prostoru V , tj.*

$$d(f) = \dim V - r(f).$$

Regulárními, resp. singulárními formami budeme rozumět formy, jejichž matice jsou regulární, resp. singulární.

Povšimněme si, že pro bilineární formu platí obdobná rovnost jako pro homomorfismus:

$$\dim V = d(f) + r(f)$$

Pro homomorfismus je tato rovnost důležitým výsledkem (viz 10.18); pro bilineární formu je zatím triviální, neboť uvedený vztah pouze definuje nulitu $d(f)$. V dalším textu však ukážeme (viz 23.12), že číslo $d(f)$, které jsme právě definovali, má hlubší smysl.

Maticí formy f vzhledem k bázi M je matice

$$A = \begin{pmatrix} 1 & 1 & 2 \\ -1 & -2 & 1 \\ -1 & 1 & 2 \end{pmatrix}.$$

Určíme analytické vyjádření a maticí formy f vzhledem k bázi

$$N = \{(1, 0, -1), (1, -1, 0), (1, 1, 1)\}.$$

Maticí přechodu od báze N k bázi M je matice

$$B = \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 1 & 2 & 0 \end{pmatrix}.$$

Maticí formy f vzhledem k bázi N je tedy matice

$$B^T A B = \begin{pmatrix} 2 & 4 & -3 \\ 8 & 2 & -1 \\ 2 & 3 & 1 \end{pmatrix}$$

a analytické vyjádření formy f vzhledem k bázi N je

$$f(x, y) = 2x'_1y'_1 + 4x'_1y'_2 - 3x'_1y'_3 + 8x'_2y'_1 + 2x'_2y'_2 - x'_2y'_3 + 2x'_3y'_1 + 3x'_3y'_2 + x'_3y'_3.$$

23.11. Definice. Nechť f je bilineární forma na prostoru V . *Levým vrcholem* formy f budeme rozumět množinu

$$L(f) = \{x \in V; \forall y \in V \quad f(x, y) = 0\}$$

a *pravým vrcholem* formy f množinu

$$R(f) = \{y \in V; \forall x \in V \quad f(x, y) = 0\}.$$

Užitím linearity formy f v první i druhé složce se snadno zjistí, že levý vrchol $L(f)$ i pravý vrchol $R(f)$ jsou podprostory prostoru V .

23.12. Věta. *Nechť V je vektorový prostor konečné dimenze a f bilineární forma na prostoru V . Jestliže je A maticí formy f vzhledem k bázi M , potom*

- (i) $L(f) = \{x \in V; A^T \cdot \langle x \rangle_M^T = o\}$,
- (ii) $R(f) = \{y \in V; A \cdot \langle y \rangle_M^T = o\}$,
- (iii) $\dim L(f) = \dim R(f) = d(f)$.

Důkaz. (i) Vektor $x \in V$ leží v levém vrcholu formy f právě tehdy, když pro každý vektor $y \in V$ je

$$f(x, y) = \langle x \rangle_M \cdot A \cdot \langle y \rangle_M^T = 0 .$$

To však nastane právě tehdy, když $\langle x \rangle_M \cdot A = o$ neboli $A^T \cdot \langle x \rangle_M^T = o$. Izomorfismus, který každému vektoru prostoru V přiřazuje jeho vektor souřadnic, převádí tedy vrchol $L(f)$ na podprostor všech řešení homogenní soustavy lineárních rovnic s maticí A^T .

(ii) Vektor $y \in V$ leží v pravém vrcholu formy f právě tehdy, když pro každý vektor $x \in V$ je

$$f(x, y) = \langle x \rangle_M \cdot A \cdot \langle y \rangle_M^T = 0 ;$$

to je ekvivalentní s rovností $A \cdot \langle y \rangle_M^T = o$. Vrchol $R(f)$ je tedy izomorfně zobrazen na podprostor všech řešení homogenní soustavy lineárních rovnic s maticí A .

(iii) Protože mají matice A a A^T stejnou hodnotu, je

$$\dim L(f) = \dim R(f) = \dim V - r(A) = d(f) .$$

Regulární formy jsou tedy ty formy, které mají triviální vrcholy.

23.13. Příklady.

(i) Bilineární forma f z příkladu 23.10(i) má triviální vrcholy, je regulární. Rovněž bilineární forma z příkladu 23.10(ii) je regulární.

(ii) Bilineární forma f na prostoru \mathbb{R}^4 má vzhledem ke kanonické bázi analytické vyjádření

$$f(x, y) = x_1y_1 + 2x_1y_2 - x_1y_3 + 2x_2y_1 + x_2y_2 + x_2y_3 + 2x_2y_4 + \\ + x_3y_1 - x_3y_2 + 2x_3y_3 + 2x_3y_4 + 3x_4y_1 + 3x_4y_2 + 2x_4y_4 .$$

Pravý vrchol $R(f)$, resp. levý vrchol $L(f)$ formy f získáme řešením homogenní soustavy lineárních rovnic s maticí

$$\begin{pmatrix} 1 & 2 & -1 & 0 \\ 2 & 1 & 1 & 2 \\ 1 & -1 & 2 & 2 \\ 3 & 3 & 0 & 2 \end{pmatrix}, \quad \text{resp.} \quad \begin{pmatrix} 1 & 2 & 1 & 3 \\ 2 & 1 & -1 & 3 \\ -1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 2 \end{pmatrix} .$$

Odtud

$$R(f) = [(-4, 2, 0, 3), (-1, 1, 1, 0)] \quad \text{a} \quad L(f) = [(-1, 1, -1, 0), (1, 1, 0, -1)] .$$

23.14. Poznámka. Označme $\mathbb{B}(V)$ množinu všech bilineárních forem na prostoru V . Tato množina je pro každý vektorový prostor V neprázdná, neboť vždy obsahuje nulovou bilineární formu. Přírozeným způsobem je možno definovat součet dvou forem a násobek formy skalárem. Pro $f, g \in \mathbb{B}(V)$, $a \in T$ a každé $x, y \in V$ položme

$$(f + g)(x, y) = f(x, y) + g(x, y), \quad (af)(x, y) = a \cdot f(x, y).$$

Snadno se ověří, že zobrazení $f + g$ i zobrazení af jsou bilineární formy na prostoru V , tj. $f + g \in \mathbb{B}(V)$, $af \in \mathbb{B}(V)$. Zcela rutinním způsobem je možno prověřit, že právě definované operace mají všechny vlastnosti operací vektorového prostoru, tj. že množina $\mathbb{B}(V)$ je vektorovým prostorem nad tělesem T .

Ke stejnému zjištění můžeme dojít i jiným způsobem. Každá bilineární forma na prostoru V je prvkem vektorového prostoru $T^{V \times V}$ všech zobrazení množiny $V \times V$ do tělesa T (viz příklad 7.8(ix)) a výše definované operace (součet bilineárních forem a násobek bilineární formy skalárem) jsou zúžením operací prostoru $T^{V \times V}$ na podmnožinu $\mathbb{B}(V)$. Množina $\mathbb{B}(V)$ je vzhledem k těmto operacím uzavřena a je tedy podprostorem prostoru $T^{V \times V}$.

23.15. Definice. Nechť f je bilineární forma na vektorovém prostoru V . Forma f se nazývá *symetrická*, resp. *antisymetrická*, jestliže pro každé dva vektory $x, y \in V$ je

$$f(x, y) = f(y, x), \quad \text{resp.} \quad f(x, y) = -f(y, x).$$

Množinu všech symetrických, resp. antisymetrických forem na prostoru V označme symbolem $\mathbb{S}(V)$, resp. $\mathbb{A}(V)$. Nulová bilineární forma je současně symetrická i antisymetrická. Snadno se ukáže, že součet dvou symetrických (antisymetrických) forem je opět symetrická (antisymetrická) forma a že násobek symetrické (antisymetrické) formy libovolným skalárem je opět symetrická (antisymetrická) forma. Množiny $\mathbb{S}(V)$ a $\mathbb{A}(V)$ jsou tedy podprostory prostoru $\mathbb{B}(V)$.

Maticе symetrických, resp. antisymetrických forem na vektorovém prostoru konečné dimenze jsou zřejmě symetrické, resp. antisymetrické. Snadno se ukáže, že je-li naopak matice formy f vzhledem k nějaké bázi M symetrická, resp. antisymetrická, je forma f symetrická, resp. antisymetrická.

Levý a pravý vrchol symetrické (antisymetrické) bilineární formy zřejmě splývají; proto mluvíme pouze o *vrcholu* symetrické (antisymetrické) bilineární formy.

23.16. Věta. Nechť V je vektorový prostor dimenze n nad tělesem T . Prostor $\mathbb{B}(V)$ je izomorfní s prostorem $T^{n \times n}$, jeho dimenze je n^2 .

Důkaz. Zvolme libovolnou bázi M prostoru V a přiřadme každé formě $f \in \mathbb{B}(V)$ její matici vzhledem k bázi M . Získáme bijekci prostoru $\mathbb{B}(V)$ na prostor $T^{n \times n}$ (viz 23.3 a 23.5). Součtu forem přitom odpovídá součet jejich matic a skalárnímu násobku formy odpovídá též násobek její matice. Prostory $\mathbb{B}(V)$ a $T^{n \times n}$ jsou proto izomorfní a mají tedy stejnou dimenzi. \square

23.17. Věta. *Nechť V je vektorový prostor nad tělesem T a nechť $\text{char } T \neq 2$. Potom platí:*

- (i) *Vektorový prostor $\mathbb{B}(V)$ je direktním součtem svých podprostorů $\mathbb{S}(V)$ a $\mathbb{A}(V)$, tj.*

$$\mathbb{B}(V) = \mathbb{S}(V) \oplus \mathbb{A}(V) .$$

- (ii) *Jestliže $\dim V = n$, potom existuje izomorfismus prostoru $\mathbb{B}(V)$ na prostor $T^{n \times n}$, který převádí direktní rozklad*

$$\mathbb{B}(V) = \mathbb{S}(V) \oplus \mathbb{A}(V)$$

na direktní rozklad

$$T^{n \times n} = \mathbb{S}(T^{n \times n}) \oplus \mathbb{A}(T^{n \times n}) ;$$

dále je

$$\dim \mathbb{S}(V) = \frac{n(n+1)}{2} \quad a \quad \dim \mathbb{A}(V) = \frac{n(n-1)}{2} .$$

Důkaz. Ke každé formě $f \in \mathbb{B}(V)$ definujeme formy $f_s, f_a \in \mathbb{B}(V)$ takto:

$$f_s(x, y) = \frac{1}{2} \cdot (f(x, y) + f(y, x)) , \quad f_a(x, y) = \frac{1}{2} \cdot (f(x, y) - f(y, x)) .$$

Zřejmě je forma f_s symetrická, forma f_a antisymetrická a $f = f_s + f_a$. Je tedy $\mathbb{B}(V) = \mathbb{S}(V) + \mathbb{A}(V)$.

Jestliže je forma f současně symetrická i antisymetrická, potom je pro každé dva vektory $x, y \in V$

$$f(x, y) = f(y, x) \quad a \quad f(x, y) = -f(y, x) ,$$

odtud $f(y, x) = -f(y, x)$ a $2f(y, x) = 0$. Proto je tedy $f(y, x) = 0$ pro každé dva vektory $x, y \in V$, forma f je nulová a $\mathbb{S}(V) \cap \mathbb{A}(V) = O$. Vektorový prostor $\mathbb{B}(V)$ je tedy direktním součtem svých podprostorů $\mathbb{S}(V)$ a $\mathbb{A}(V)$.

Poznamenejme, že jsme dvakrát užili toho, že $\text{char } T \neq 2$; v první části důkazu při definici forem f_s a f_a , kde $\frac{1}{2}$ je inverzním prvkem k nenulovému prvku $2 = 1 + 1$ tělesa T , a v druhé části důkazu při krácení nenulovým prvkem 2. Je-li $\text{char } T = 2$, pak tvrzení (i) neplatí; symetrické a antisymetrické formy na prostoru V splývají, neboť pro každý prvek $a \in T$ je $2a = 0$ neboli $a = -a$.

(ii) Přiřadíme-li každé formě $f \in \mathbb{B}(V)$ její matici vzhledem k pevně zvolené bázi M prostoru V , získáme stejně jako v 23.16 izomorfismus prostoru $\mathbb{B}(V)$ na

prostor $T^{n \times n}$. Při tomto izomorfismu odpovídají symetrické, resp. antisymetrické formy symetrickým, resp. antisymetrickým maticím, takže rozklad

$$\mathbb{B}(V) = \mathbb{S}(V) \oplus \mathbb{A}(V)$$

přechází v rozklad

$$T^{n \times n} = \mathbb{S}(T^{n \times n}) \oplus \mathbb{A}(T^{n \times n}) .$$

Ostatní je důsledkem věty 10.22. \square

Každou bilineární formu f na vektorovém prostoru V nad tělesem T , pro které $\text{char } T \neq 2$, je tedy možno právě jediným způsobem vyjádřit jako součet symetrické formy f_s a antisymetrické formy f_a . Tyto formy se někdy nazývají *symetrická část* a *antisymetrická část* formy f . V praktických příkladech získáme rozklad formy f na symetrickou a antisymetrickou část rozkladem její matice (užíváme tak vlastně tvrzení předchozí věty).

23.18. Příklad. Bilineární forma na vektorovém prostoru \mathbb{R}^4 je dána vzhledem ke kanonické bázi analytickým vyjádřením

$$\begin{aligned} f(x, y) = & x_1y_1 + 2x_1y_2 + 3x_1y_3 + 2x_1y_4 + x_2y_1 - x_2y_2 + 2x_2y_3 + \\ & + 2x_3y_2 + x_3y_3 + 3x_3y_4 + 2x_4y_1 + x_4y_2 + 2x_4y_3 - x_4y_4 . \end{aligned}$$

Vyjádříme-li matici formy f vzhledem ke kanonické bázi jako součet symetrické a antisymetrické matice, získáme současně rozklad formy f na symetrickou a antisymetrickou část:

$$\begin{pmatrix} 1 & 2 & 3 & 2 \\ 1 & -1 & 2 & 0 \\ 0 & 2 & 1 & 3 \\ 2 & 1 & 2 & -1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{3}{2} & \frac{3}{2} & 2 \\ \frac{3}{2} & -1 & 2 & \frac{1}{2} \\ \frac{3}{2} & 2 & 1 & \frac{5}{2} \\ 2 & \frac{1}{2} & \frac{5}{2} & -1 \end{pmatrix} + \begin{pmatrix} 0 & \frac{1}{2} & \frac{3}{2} & 0 \\ -\frac{1}{2} & 0 & 0 & -\frac{1}{2} \\ -\frac{3}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 \end{pmatrix}$$

Tedy

$$f = f_s + f_a ,$$

kde formy f_s a f_a jsou dány svým analytickým vyjádřením vzhledem ke kanonické bázi:

$$\begin{aligned} f_s(x, y) = & x_1y_1 + \frac{3}{2}x_1y_2 + \frac{3}{2}x_1y_3 + 2x_1y_4 + \frac{3}{2}x_2y_1 - x_2y_2 + 2x_2y_3 + \frac{1}{2}x_2y_4 + \\ & + \frac{3}{2}x_3y_1 + 2x_3y_2 + x_3y_3 + \frac{5}{2}x_3y_4 + 2x_4y_1 + \frac{1}{2}x_4y_2 + \frac{5}{2}x_4y_3 - x_4y_4 , \\ f_a(x, y) = & \frac{1}{2}x_1y_2 + \frac{3}{2}x_1y_3 - \frac{1}{2}x_2y_1 - \frac{1}{2}x_2y_4 - \frac{3}{2}x_3y_1 + \frac{1}{2}x_3y_4 + \frac{1}{2}x_4y_2 - \frac{1}{2}x_4y_3 . \end{aligned}$$

23.19. Definice. Nechť V je vektorový prostor konečné dimenze nad tělesem T a f symetrická bilineární forma na prostoru V . Budeme říkat, že báze N prostoru V je *polární* vůči f , jestliže matice formy f vzhledem k bázi N je diagonální.

Analytické vyjádření formy f vzhledem k bázi N , která je polární vůči f , je tedy

$$f(x, y) = a_1x_1y_1 + a_2x_2y_2 + \dots + a_nx_ny_n ;$$

přitom je $n = \dim V$ a hodnost formy f je rovna počtu nenulových koeficientů tohoto vyjádření.

23.20. Věta. *Nechť V je vektorový prostor konečné dimenze nad tělesem T , nechť $\text{char } T \neq 2$. Potom ke každé symetrické bilineární formě f na prostoru V existuje báze prostoru V , která je vůči f polární.*

Důkaz. Zvolme libovolnou bázi M prostoru V . Jestliže je f symetrická bilineární forma na prostoru V a A její matice vzhledem k bázi M , potom je matice A symetrická a podle věty 12.28 k ní existuje regulární matice B taková, že matice $B^T A B$ je diagonální. Jestliže je N taková báze prostoru V , že B je maticí přechodu od N k M , pak podle věty 23.7 má forma f vzhledem k bázi N diagonální matici $B^T A B$, tj. báze N je polární vůči f . \square

Je-li A nenulová antisymetrická matice a B regulární matice, potom je matice $B^T A B$ opět nenulová antisymetrická matice a nemůže být proto diagonální. K nenulové antisymetrické formě f tedy nemůže existovat báze prostoru V , vzhledem ke které by matice formy f byla diagonální.

Jestliže $f = f_s + f_a$ je bilineární forma a N báze prostoru V , která je polární vůči formě f_s , potom matice formy f vzhledem k bázi N je součtem diagonální a antisymetrické matice. Odtud vyplývá, že má smysl definovat pojem polární báze pouze vůči symetrickým bilineárním formám.

23.21. Příklad. Symetrická bilineární forma na vektorovém prostoru \mathbb{R}^4 je dána vzhledem k bázi M analytickým vyjádřením

$$f(x, y) = x_1y_1 + x_1y_2 + 3x_1y_3 - x_1y_4 + x_2y_1 + 2x_2y_2 + x_2y_3 + \\ + 3x_3y_1 + x_3y_2 + 2x_3y_3 + x_3y_4 - x_4y_1 + x_4y_3 + x_4y_4 .$$

Najdeme bázi N prostoru \mathbb{R}^4 , která je vůči f polární. Matici A formy f vzhledem k bázi M budeme symetrickými úpravami převádět na diagonální tvar D a současně sledovat prováděné řádkové elementární úpravy, tj. najdeme matici B , pro kterou $D = B^T A B$:

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 3 & -1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 2 & 1 & 0 & 0 & 1 & 0 \\ -1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 1 & -1 & 1 & 0 & 0 \\ 0 & -2 & -7 & 4 & -3 & 0 & 1 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 & 0 & 1 \end{array} \right) \rightsquigarrow$$

$$\begin{aligned}
& \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -11 & 6 & -5 & 2 & 1 & 0 \\ 0 & 0 & 6 & -1 & 2 & -1 & 0 & 1 \end{array} \right) \rightsquigarrow \\
& \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 6 & 2 & -1 & 0 & 1 \\ 0 & 0 & 6 & -11 & -5 & 2 & 1 & 0 \end{array} \right) \rightsquigarrow \\
& \rightsquigarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 2 & -1 & 0 & 1 \\ 0 & 0 & 0 & 25 & 7 & -4 & 1 & 6 \end{array} \right) = (D | B^T)
\end{aligned}$$

Našli jsme tedy bázi $N = \{v_1, v_2, v_3, v_4\}$, která je polární vůči formě f , a analytické vyjádření formy f vzhledem k této bázi N . Je

$$\begin{aligned}
\langle v_1 \rangle_M &= (1, 0, 0, 0), & \langle v_2 \rangle_M &= (-1, 1, 0, 0), \\
\langle v_3 \rangle_M &= (2, -1, 0, 1), & \langle v_4 \rangle_M &= (7, -4, 1, 6),
\end{aligned}$$

$$f(x, y) = x'_1 y'_1 + x'_2 y'_2 - x'_3 y'_3 + 25x'_4 y'_4,$$

neboť matice B je maticí přechodu od báze N k bázi M a matice D je maticí formy f vzhledem k bázi N .

23.22. Poznámka. Nechť f je bilineární forma na vektorovém prostoru V nad tělesem T a necht' $v \in V$ je pevně zvolený vektor. Zobrazení v^* prostoru V do tělesa T definované rovností $v^*(x) = f(v, x)$ je lineární forma na prostoru V (tj. $v^* \in V^*$), neboť bilineární forma f je lineární ve druhé složce. Pro každé $x_1, x_2 \in V$ je totiž

$$v^*(x_1 + x_2) = f(v, x_1 + x_2) = f(v, x_1) + f(v, x_2) = v^*(x_1) + v^*(x_2)$$

a pro každé $x \in V$ a $a \in T$ je

$$v^*(ax) = f(v, ax) = a \cdot f(v, x) = a \cdot v^*(x).$$

Zobrazení f_L prostoru V do prostoru V^* definované rovností $f_L(v) = v^*$ je homomorfismus, neboť bilineární forma f je lineární i v první složce. Pro každé $v_1, v_2 \in V$ je totiž

$$(v_1 + v_2)^*(x) = f(v_1 + v_2, x) = f(v_1, x) + f(v_2, x) = v_1^*(x) + v_2^*(x) = (v_1^* + v_2^*)(x)$$

a pro každé $v \in V$ a $a \in T$ je

$$(av)^*(x) = f(av, x) = a \cdot f(v, x) = a \cdot v^*(x) = (a \cdot v^*)(x),$$

takže

$$(v_1 + v_2)^* = v_1^* + v_2^* , \quad (av)^* = a \cdot v^* ,$$

neboli

$$f_L(v_1 + v_2) = f_L(v_1) + f_L(v_2) , \quad f_L(av) = a \cdot f_L(v) .$$

Vzhledem k označení, které jsme zavedli v 21.15, je pro každé $v, x \in V$

$$\langle x, f_L(v) \rangle = \langle x, v^* \rangle = v^*(x) = f(v, x) .$$

Homomorfismus f_L se někdy nazývá *levý homomorfismus* prostoru V do prostoru V^* určený bilineární formou f . Jádrem tohoto homomorfismu je zřejmě levý vrchol bilineární formy f , tj.

$$\text{Ker } f_L = L(f) .$$

Zobrazení L prostoru $\mathbb{B}(V)$ do prostoru $\text{Hom}(V, V^*)$, které formě $f \in \mathbb{B}(V)$ přiřadí levý homomorfismus f_L určený touto formou, je monomorfismus. Pro každé $f, f' \in \mathbb{B}(V)$, $a \in T$ a $v, x \in V$ je totiž:

$$\begin{aligned} \langle x, (f + f')_L(v) \rangle &= (f + f')(v, x) = f(v, x) + f'(v, x) = \\ &= \langle x, f_L(v) \rangle + \langle x, f'_L(v) \rangle = \langle x, (f_L + f'_L)(v) \rangle , \end{aligned}$$

$$\langle x, (af)_L(v) \rangle = (af)(v, x) = a \cdot f(v, x) = a \cdot \langle x, f_L(v) \rangle = \langle x, (a \cdot f_L)(v) \rangle ,$$

takže

$$(f + f')_L(v) = (f_L + f'_L)(v) , \quad (af)_L(v) = (a \cdot f_L)(v) ,$$

neboli

$$(f + f')_L = f_L + f'_L , \quad (af)_L = a \cdot f_L .$$

Dále je $f_L = o$ právě tehdy, když je $\text{Ker } f_L = V$ a tedy $f = o$ a L je monomorfismus.

Nechť V je prostor konečné dimenze. Jestliže je f regulární bilineární forma na prostoru V , potom je f_L izomorfismus prostoru V na prostor V^* ; ke každé lineární formě $g \in V^*$ tedy existuje jednoznačně určený vektor $v \in V$ takový, že $g = v^*$, tj. pro každé $x \in V$ je $\langle x, g \rangle = f(v, x)$. Zobrazení L je izomorfismus prostoru $\mathbb{B}(V)$ na prostor $\text{Hom}(V, V^*)$, tj. ke každému homomorfismu h prostoru V do prostoru V^* existuje právě jediná bilineární forma f na prostoru V , pro kterou $f_L = h$, tj. pro každé $v, x \in V$ je $\langle x, h(v) \rangle = f(v, x)$.

23.23. Poznámka. Úvahy předchozí poznámky 23.22 můžeme snadno modifikovat.

Nechť f je bilineární forma na vektorovém prostoru V nad tělesem T a $v \in V$ je pevně zvolený vektor. Zobrazení v^* prostoru V do tělesa T definované rovností

$v^*(x) = f(x, v)$ je lineární formou na prostoru V , neboť bilineární forma f je lineární v první složce. Zobrazení f_R prostoru V do prostoru V^* definované rovností $f_R(v) = v^*$ je homomorfismus, neboť forma f je lineární i ve druhé složce. Pro každé $v, x \in V$ je

$$\langle x, f_R(v) \rangle = f(x, v) .$$

Homomorfismus f_R se nazývá *pravý homomorfismus* prostoru V do prostoru V^* určený bilineární formou f . Jeho jádrem je pravý vrchol formy f , tj.

$$\text{Ker } f_R = R(f) .$$

Zobrazení R prostoru $\mathbb{B}(V)$ do prostoru $\text{Hom}(V, V^*)$, které každé formě $f \in \mathbb{B}(V)$ přiřadí pravý homomorfismus f_R určený formou f , je monomorfismus.

Jestliže má prostor V konečnou dimenzi a $f \in \mathbb{B}(V)$ je regulární, potom je f_R izomorfismus prostoru V na prostor V^* a R izomorfismus prostoru $\mathbb{B}(V)$ na prostor $\text{Hom}(V, V^*)$.

Pomocí bilineárních forem jsou definovány formy kvadratické.

23.24. Definice. Nechť V je vektorový prostor nad tělesem T . *Kvadratickou formou* na prostoru V budeme rozumět každé zobrazení q prostoru V do tělesa T , ke kterému existuje bilineární forma f taková, že pro každý vektor $v \in V$ je $q(v) = f(v, v)$; budeme říkat, že kvadratická forma q je *vytvořena bilineární formou* f .

23.25. Příklady.

(i) Nejjednodušší kvadratickou formou na prostoru V je tzv. *nulová* kvadratická forma, která každému vektoru $v \in V$ přiřazuje nulový prvek tělesa T . Je vytvořena nulovou bilineární formou na prostoru V .

(ii) Jsou-li g_1, g_2 lineární formy na prostoru V , potom zobrazení q , které vektoru $v \in V$ přiřazuje skalár $q(v) = g_1(v) \cdot g_2(v)$, je kvadratická forma na prostoru V . Srovnej s příkladem 23.2(ii).

(iii) Nechť V je vektorový prostor všech reálných funkcí spojitých na intervalu $\langle a, b \rangle$ a necht' k je reálná funkce dvou reálných proměnných, která je spojitá na intervalu $\langle a, b \rangle \times \langle a, b \rangle$. Zobrazení, které každé funkci $p \in V$ přiřazuje reálné číslo

$$q(p) = \int_a^b \int_a^b k(x, y)p(x)p(y) dx dy ,$$

je kvadratická forma na prostoru V . Srovnej s příkladem 23.2(iii).

(iv) Nechť $A = (a_{ij})$ je čtvercová matice řádu n nad tělesem T . Zobrazení, které vektoru $x = (x_1, \dots, x_n) \in T^n$ přiřadí skalár

$$q(x) = \sum_{i,j=1}^n a_{ij}x_i x_j = (x_1, \dots, x_n) \cdot A \cdot (x_1, \dots, x_n)^T ,$$

je kvadratická forma na prostoru T^n . Srovnej s příkladem 23.2(iv).

23.26. Poznámka. Označme $\mathbb{Q}(V)$ množinu všech kvadratických forem na prostoru V . Tato množina je pro každý vektorový prostor V neprázdná, neboť vždy obsahuje nulovou kvadratickou formu. Přirozeným způsobem je možno definovat součet dvou kvadratických forem a násobek kvadratické formy skalárem. Pro každé $q_1, q_2, q \in \mathbb{Q}(V)$, $a \in T$ a $x \in V$ klademe

$$(q_1 + q_2)(x) = q_1(x) + q_2(x) \quad \text{a} \quad (aq)(x) = a \cdot q(x) .$$

Jsou-li f_1, f_2, f bilineární formy, které po řadě vytvářejí kvadratické formy q_1, q_2, q , pak bilineární forma $f_1 + f_2$, resp. af vytváří kvadratickou formu $q_1 + q_2$, resp. aq , neboť

$$(q_1 + q_2)(x) = q_1(x) + q_2(x) = f_1(x, x) + f_2(x, x) = (f_1 + f_2)(x, x) ,$$

$$(aq)(x) = a \cdot q(x) = a \cdot f(x, x) = (af)(x, x) .$$

Snadno se ověří, že sčítání kvadratických forem i násobení kvadratické formy skalárem jsou operace, které mají všechny vlastnosti operací vektorového prostoru, tj. množina $\mathbb{Q}(V)$ je vektorovým prostorem nad tělesem T .

Poznamenejme ještě, že každá kvadratická forma na prostoru V je prvkem vektorového prostoru T^V všech zobrazení množiny V do tělesa T (viz příklad 7.8(ix)) a výše definované operace jsou zúžením operací prostoru T^V na jeho podmnožinu $\mathbb{Q}(V)$. Množina $\mathbb{Q}(V)$ je vzhledem k těmto operacím uzavřená a je tedy podprostorem prostoru T^V .

23.27. Věta. *Nechť V je vektorový prostor nad tělesem T a nechť $\text{char } T \neq 2$. Zobrazení Φ , které každé bilineární formě f na prostoru V přiřazuje kvadratickou formu vytvořenou formou f , je epimorfismus vektorového prostoru $\mathbb{B}(V)$ na vektorový prostor $\mathbb{Q}(V)$. Jádrem epimorfismu Φ je podprostor $\mathbb{A}(V)$. Zúžení epimorfismu Φ na podprostor $\mathbb{S}(V)$ je izomorfismus prostoru $\mathbb{S}(V)$ na prostor $\mathbb{Q}(V)$.*

Důkaz. V předchozím odstavci jsme viděli, že pro formy $f_1, f_2, f \in \mathbb{B}(V)$ a skalár $a \in T$ je

$$\Phi(f_1 + f_2) = \Phi(f_1) + \Phi(f_2) \quad \text{a} \quad \Phi(af) = a \cdot \Phi(f) .$$

Zobrazení Φ je tedy homomorfismus; z definice 23.24 vyplývá, že jde o epimorfismus. (K prověření těchto faktů jsme nepotřebovali předpoklad $\text{char } T \neq 2$.)

Jestliže $f \in \text{Ker } \Phi$, potom pro každý vektor $x \in V$ je $f(x, x) = 0$. Pro libovolně zvolené vektory $u, v \in V$ je potom

$$0 = f(u + v, u + v) = f(u, u) + f(u, v) + f(v, u) + f(v, v) = f(u, v) + f(v, u) ,$$

odtud $f(u, v) = -f(v, u)$, tj. forma f je antisymetrická. Jestliže je naopak forma f antisymetrická, pak pro každý vektor $x \in V$ je $f(x, x) = -f(x, x)$, tj. $f(x, x) = 0$ (neboť $\text{char } T \neq 2$) a $f \in \text{Ker } \Phi$. Dokázali jsme tedy, že $\text{Ker } \Phi = \mathbb{A}(V)$. Protože je

navíc $\mathbb{A}(V) \cap \mathbb{S}(V) = O$ (neboť $\text{char } T \neq 2$ — viz 23.17), je zúžení epimorfismu Φ na podprostor $\mathbb{S}(V)$ monomorfismus. Navíc je kvadratická forma vytvořená bilineární formou f vytvořena též symetrickou částí formy f , takže uvažované zúžení je dokonce izomorfismus. Je-li totiž $f = f_s + f_a$, kde $f_s \in \mathbb{S}(V)$ a $f_a \in \mathbb{A}(V)$, potom je podle předešlého

$$\Phi(f) = \Phi(f_s) + \Phi(f_a) = \Phi(f_s) . \quad \square$$

Nechť V je vektorový prostor dimenze n nad tělesem T , M jeho báze a q kvadratická forma na prostoru V vytvořená symetrickou bilineární formou f . *Maticí kvadratické formy q vzhledem k bázi M* budeme rozumět matici formy f vzhledem k téže bázi M . Označíme-li tuto matici $A = (a_{ij})$, potom je pro každý vektor $x \in V$

$$q(x) = \langle x \rangle_M \cdot A \cdot \langle x \rangle_M^T .$$

Po provedení maticového násobení přejde tato rovnost v tzv. *analytické vyjádření* kvadratické formy q vzhledem k bázi M :

$$\begin{aligned} q(x) = \sum_{i,j=1}^n a_{ij}x_i x_j = & a_{11}x_1^2 + 2a_{12}x_1x_2 + \dots + 2a_{1n}x_1x_n + \\ & + a_{22}x_2^2 + \dots + 2a_{2n}x_2x_n + \\ & \dots\dots\dots \\ & + a_{nn}x_n^2 . \end{aligned}$$

Jestliže je A matice kvadratické formy q vzhledem k bázi M , potom maticí formy q vzhledem k bázi M' je matice $B^T A B$, kde B je matice přechodu od báze M' k bázi M .

Hodnotí, resp. *nulitou* (nebo *defektem*) kvadratické formy q rozumíme hodnotu, resp. nulitu symetrické bilineární formy f , která kvadratickou formu q vytváří; rozlišujeme *regulární* a *singulární* kvadratické formy. *Vrcholem* kvadratické formy q rozumíme vrchol symetrické bilineární formy f , která formu q vytváří.

Nechť V je vektorový prostor konečné dimenze nad tělesem T a q kvadratická forma na prostoru V . Budeme říkat, že báze N prostoru V je *polární* vůči q , jestliže matice formy q vzhledem k bázi N je diagonální.

Analytické vyjádření kvadratické formy q vzhledem k bázi N , která je vůči q polární, je tedy

$$q(x) = a_1x_1^2 + a_2x_2^2 + \dots + a_nx_n^2 ;$$

přitom je $n = \dim V$ a hodnota formy q je rovna počtu nenulových koeficientů tohoto vyjádření.

Víme, že každá lineární forma na prostoru V je určena svými hodnotami v libovolné bázi prostoru V . Pro kvadratickou formu obdobné tvrzení neplatí. Hodnotami kvadratické formy q v bázi M vektorového prostoru V konečné dimenze je

totiž určena pouze hlavní diagonála matice formy q vzhledem k bázi M a nikoli celá tato matice. Každá kvadratická forma q je však určena svými hodnotami v libovolné bázi, která je vůči q polární; matice formy q vzhledem k takovéto bázi je totiž diagonální.

Nechť q je kvadratická forma na prostoru V , která je vytvořena symetrickou bilineární formou f . Množina

$$N(q) = \{v \in V; q(v) = 0\}$$

je zřejmě uzavřena vzhledem k násobení skalárem; není však uzavřena vzhledem ke sčítání vektorů. Jestliže je totiž $v_1, v_2 \in N(q)$, je

$$q(v_1 + v_2) = q(v_1) + 2f(v_1, v_2) + q(v_2) = 2f(v_1, v_2),$$

takže nemusí být $q(v_1 + v_2) = 0$. Množina $N(q)$ zřejmě obsahuje vrchol formy q .

23.28. Příklad. Kvadratická forma q na prostoru \mathbb{R}^3 je dána analytickým vyjádřením vzhledem ke kanonické bázi:

$$q(x) = x_1^2 + 2x_1x_2 + 4x_1x_3 + 3x_2^2 + x_2x_3 + x_3^2$$

Maticí formy q vzhledem ke kanonické bázi je matice

$$\begin{pmatrix} 1 & 1 & 2 \\ 1 & 3 & \frac{1}{2} \\ 2 & \frac{1}{2} & 1 \end{pmatrix}.$$

Kvadratická forma q je vytvořena symetrickou bilineární formou f , jejíž analytické vyjádření vzhledem ke kanonické bázi je

$$f(x, y) = x_1y_1 + x_1y_2 + 2x_1y_3 + x_2y_1 + 3x_2y_2 + \frac{1}{2}x_2y_3 + 2x_3y_1 + \frac{1}{2}x_3y_2 + x_3y_3.$$

Standardním způsobem nalezneme bázi N prostoru \mathbb{R}^3 , která je polární vůči formě q :

$$\begin{aligned} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & \frac{1}{2} & 0 & 1 & 0 \\ 2 & \frac{1}{2} & 1 & 0 & 0 & 1 \end{array} \right) &\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & -3 & -1 & 1 & 0 \\ 0 & -3 & -12 & -4 & 0 & 2 \end{array} \right) \rightsquigarrow \\ &\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -1 & 1 & 0 \\ 0 & 0 & -66 & -11 & 3 & 4 \end{array} \right) \end{aligned}$$

Nalezená báze $N = \{(1, 0, 0), (-1, 1, 0), (-11, 3, 4)\}$ je polární vůči kvadratické formě q ; analytické vyjádření formy q vzhledem k bázi N je

$$q(x) = \xi_1^2 + 2\xi_2^2 - 66\xi_3^2.$$

24. SESKVILINEÁRNÍ A KVADRATICKÉ FORMY NA KOMPLEXNÍCH PROSTORECH

V teorii komplexních vektorových prostorů se často místo bilineárních forem studují tzv. seskvilineární formy. Jejich teorii je možno vyložit paralelně k teorii bilineárních forem, která je obsažena v předchozím paragrafu.

24.1. Definice. Nechť V je komplexní vektorový prostor. *Seskvilineární formou* na prostoru V budeme rozumět každé zobrazení f kartézského součinu $V \times V$ do tělesa \mathbb{C} , pro které platí:

- (i) $\forall x, y, z \in V \quad f(x + y, z) = f(x, z) + f(y, z)$,
- (ii) $\forall x, y \in V \quad \forall a \in \mathbb{C} \quad f(ax, y) = a \cdot f(x, y)$,
- (iii) $\forall x, y, z \in V \quad f(x, y + z) = f(x, y) + f(x, z)$,
- (iv) $\forall x, y \in V \quad \forall a \in \mathbb{C} \quad f(x, ay) = \bar{a} \cdot f(x, y)$.

Seskvilineární forma je tedy *lineární v první složce* a *semilineární v druhé složce*.

Užitím matematické indukce dostaneme pro seskvilineární formu obecnou podmínku:

$$\forall x_1, \dots, x_r, y_1, \dots, y_s \in V \quad \forall a_1, \dots, a_r, b_1, \dots, b_s \in \mathbb{C}$$

$$f\left(\sum_{i=1}^r a_i x_i, \sum_{j=1}^s b_j y_j\right) = \sum_{i=1}^r \sum_{j=1}^s a_i \bar{b}_j \cdot f(x_i, y_j).$$

24.2. Příklady.

(i) Zobrazení, které každé dvojici vektorů prostoru V přiřazuje nulu, je tzv. *nulová* seskvilineární forma. Ostatní seskvilineární formy na prostoru V se nazývají *nenulové*.

(ii) Je-li g_1 lineární a g_2 semilineární forma na prostoru V , potom zobrazení f , které každé dvojici $(x, y) \in V \times V$ přiřadí číslo $f(x, y) = g_1(x) \cdot g_2(y)$, je seskvilineární forma na prostoru V . Srovnej s příkladem 23.2(ii).

(iii) Nechť $A = (a_{ij})$ je komplexní čtvercová matice řádu n . Zobrazení f , které každým dvěma vektorům $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ prostoru \mathbb{C}^n přiřadí skalár

$$f(x, y) = \sum_{i,j=1}^n a_{ij} x_i \bar{y}_j = (x_1, \dots, x_n) \cdot A \cdot (\bar{y}_1, \dots, \bar{y}_n)^T,$$

je seskvilineární forma na prostoru \mathbb{C}^n .

Teorii bilineárních a kvadratických forem z předchozího paragrafu budeme nyní modifikovat pro seskvilineární formy; tomu bude odpovídat i číslování většiny odstavců. Všechny důkazy je možno provést stejně, je však třeba dávat pozor na čtvrtou vlastnost z definice 24.1. Jen v několika odstavcích (24.13, 24.15, 24.17, 24.26, 24.27, 24.28) se výsledky tohoto paragrafu výrazněji odlišují od výsledků paragrafu předchozího.

24.3. Věta. *Nechť V je komplexní vektorový prostor a M jeho báze. Každá seskvilineární forma na prostoru V určuje přirozeným způsobem zobrazení množiny $M \times M$ do tělesa \mathbb{C} . Naopak každé zobrazení množiny $M \times M$ do tělesa \mathbb{C} je možno právě jediným způsobem rozšířit na seskvilineární formu na prostoru V . Každá seskvilineární forma na prostoru V je jednoznačně určena svými hodnotami na množině $M \times M$. \square*

24.4. Definice. *Nechť V je komplexní vektorový prostor dimenze n a nechť $M = \{v_1, \dots, v_n\}$ je jeho báze. Nechť f je seskvilineární forma na prostoru V . Maticí seskvilineární formy f vzhledem k bázi M budeme rozumět čtvercovou matici řádu n , která má na místě ij hodnotu formy f v i -tém a j -tém vektoru báze M , tj. komplexní číslo $f(v_i, v_j)$.*

24.5. Věta. *Nechť V je komplexní vektorový prostor dimenze n a M jeho báze. Nechť f je seskvilineární forma na prostoru V . Komplexní matice A řádu n je maticí formy f vzhledem k bázi M právě tehdy, když pro každé $x, y \in V$ je*

$$f(x, y) = \langle x \rangle_M \cdot A \cdot \overline{\langle y \rangle_M}^T. \quad \square$$

24.6. Poznámka. *Pišme $\langle x \rangle_M = (x_1, \dots, x_n)$, $\langle y \rangle_M = (y_1, \dots, y_n)$, $A = (a_{ij})$; rovnost uvedená ve větě 24.5 přejde v rovnost*

$$f(x, y) = \sum_{i,j=1}^n a_{ij} x_i \overline{y_j},$$

kteřá se nazývá *analytické vyjádření seskvilineární formy f vzhledem k bázi M* .

24.7. Věta. *Nechť V je komplexní vektorový prostor konečné dimenze, M a M' jeho báze a f seskvilineární forma na prostoru V . Jestliže A je maticí formy f vzhledem k bázi M , potom $B^T A \overline{B}$ je maticí formy f vzhledem k bázi M' , kde B je matice přechodu od báze M' k bázi M . \square*

24.8. Důsledek. *Všechny matice seskvilineární formy f (vzhledem k různým bázím) mají stejnou hodnotu. \square*

24.9. Definice. *Hodností $r(f)$ seskvilineární formy f na komplexním vektorovém prostoru V konečné dimenze budeme rozumět hodnotu některé její matice. Nulitou nebo defektem $d(f)$ formy f budeme rozumět doplněk hodnoty $r(f)$ do dimenze prostoru V , tj. $d(f) = \dim V - r(f)$. Regulárními, resp. singulárními formami budeme rozumět ty formy, jejichž matice jsou regulární, resp. singulární.*

24.10. Příklad. *Seskvilineární forma f na prostoru $V = \mathbb{C}^3$ je dána analytickým vyjádřením vzhledem ke kanonické bázi prostoru V :*

$$f(x, y) = x_1 \overline{y_1} + 2x_1 \overline{y_2} + ix_1 \overline{y_3} + x_2 \overline{y_2} - ix_2 \overline{y_3} + x_3 \overline{y_1} + ix_3 \overline{y_2}$$

Maticí formy f vzhledem ke kanonické bázi prostoru V je tedy matice

$$A = \begin{pmatrix} 1 & 2 & i \\ 0 & 1 & -i \\ 1 & i & 0 \end{pmatrix}.$$

Máme-li určit analytické vyjádření formy f vzhledem k bázi

$$N = \{(1, 0, i), (1, i, 0), (i, 0, 0)\},$$

najdeme matici přechodu od báze N ke kanonické bázi prostoru V , označíme ji B a pak vypočteme matici $A' = B^T A \bar{B}$, ve které jsou koeficienty analytického vyjádření formy f vzhledem k bázi N :

$$B = \begin{pmatrix} 1 & 1 & i \\ 0 & i & 0 \\ i & 0 & 0 \end{pmatrix}, \quad A' = \begin{pmatrix} 2+i & 1 & 1-i \\ 2-i & 2-2i & -i \\ 2i & 2+i & 1 \end{pmatrix}.$$

Analytické vyjádření formy f vzhledem k bázi N je tedy

$$\begin{aligned} f(x, y) &= (2+i)x'_1\bar{y}'_1 + x'_1\bar{y}'_2 + (1-i)x'_1\bar{y}'_3 + \\ &+ (2-i)x'_2\bar{y}'_1 + (2-2i)x'_2\bar{y}'_2 - ix'_2\bar{y}'_3 + 2ix'_3\bar{y}'_1 + (2+i)x'_3\bar{y}'_2 + x'_3\bar{y}'_3. \end{aligned}$$

Forma f je regulární, neboť matice A (resp. $A' = B^T A \bar{B}$) je regulární.

Pokud bychom chtěli naopak přejít od analytického vyjádření vzhledem k bázi N k analytickému vyjádření vzhledem ke kanonické bázi, použili bychom matici C přechodu od kanonické báze k bázi N :

$$C = B^{-1} = \begin{pmatrix} 0 & 0 & -i \\ 0 & -i & 0 \\ -i & 1 & 1 \end{pmatrix}, \quad A = C^T A \bar{C} = \begin{pmatrix} 1 & 2 & i \\ 0 & 1 & -i \\ 1 & i & 0 \end{pmatrix}.$$

24.11. Definice. *Levým, resp. pravým vrcholem* seskvilineární formy f na komplexním vektorovém prostoru V budeme rozumět množinu

$$L(f) = \{x \in V; \forall y \in V \quad f(x, y) = 0\},$$

resp.

$$R(f) = \{y \in V; \forall x \in V \quad f(x, y) = 0\}.$$

Levý i pravý vrchol formy f jsou podprostory prostoru V .

24.12. Věta. Jestliže je f seskvilineární forma na komplexním prostoru V konečné dimenze a A její matice vzhledem k bázi M , potom je

$$L(f) = \{x \in V; A^T \cdot \langle x \rangle_M^T = o\}, \quad R(f) = \{y \in V; \overline{A} \cdot \langle y \rangle_M^T = o\}.$$

Levý i pravý vrchol mají stejnou dimenzi, která je rovna nulitě $d(f)$ formy f . \square

24.13. Lemma. Nechť f je seskvilineární forma na komplexním vektorovém prostoru V . Potom pro každé dva vektory $x, y \in V$ je

$$f(x, y) = \frac{1}{4} \cdot (f(x+y, x+y) - f(x-y, x-y) + i \cdot f(x+iy, x+iy) - i \cdot f(x-iy, x-iy)),$$

$$f(y, x) = \frac{1}{4} \cdot (f(x+y, x+y) - f(x-y, x-y) - i \cdot f(x+iy, x+iy) + i \cdot f(x-iy, x-iy)).$$

Každá seskvilineární forma na komplexním prostoru V je určena svými hodnotami na množině $\Delta_V = \{(v, v); v \in V\}$.

Důkaz. Pro vektory $x, y \in V$ platí:

$$\begin{aligned} f(x+y, x+y) &= f(x, x) + f(x, y) + f(y, x) + f(y, y), \\ f(x-y, x-y) &= f(x, x) - f(x, y) - f(y, x) + f(y, y), \\ f(x+iy, x+iy) &= f(x, x) - if(x, y) + if(y, x) + f(y, y), \\ f(x-iy, x-iy) &= f(x, x) + if(x, y) - if(y, x) + f(y, y). \end{aligned}$$

Vynásobíme-li tyto čtyři rovnosti po řadě čísly $1, -1, i, -i$, resp. $1, -1, -i, i$, sečteme a vydělíme čtyřmi, dostaneme výše uvedená vyjádření pro $f(x, y)$ a $f(y, x)$.

Druhé tvrzení je důsledkem prvního. \square

Tvrzení obdobné lemmatu 24.13 neplatí pro obecné bilineární formy, ale pouze pro symetrické bilineární formy. Je-li f bilineární forma na vektorovém prostoru V nad tělesem T , potom pro ni platí první dvě rovnosti z důkazu lemmatu 24.13; jejich odečtením získáme rovnost

$$2 \cdot f(x, y) + 2 \cdot f(y, x) = f(x+y, x+y) - f(x-y, x-y).$$

Jestliže je f navíc symetrická a $\text{char } T \neq 2$, potom je

$$f(x, y) = \frac{1}{4} \cdot (f(x+y, x+y) - f(x-y, x-y)).$$

Každá symetrická bilineární forma na vektorovém prostoru V nad tělesem T , kde $\text{char } T \neq 2$, je proto jednoznačně určena svými hodnotami na množině Δ_V .

24.14. Poznámka. Označme $\mathbb{B}_s(V)$ množinu všech seskvilineárních forem na komplexním prostoru V (index s je od slova seskvilineární). Tato množina je neprázdná; přirozeným způsobem definujeme součet seskvilineárních forem a násobek seskvilineární formy komplexním číslem; pro $f, g \in \mathbb{B}_s(V)$, $a \in \mathbb{C}$ a $x, y \in V$ klademe:

$$(f + g)(x, y) = f(x, y) + g(x, y) \quad \text{a} \quad (af)(x, y) = a \cdot f(x, y) .$$

Zřejmě je $f + g \in \mathbb{B}_s(V)$, $af \in \mathbb{B}_s(V)$; snadno se ověří, že $\mathbb{B}_s(V)$ je komplexním vektorovým prostorem. Tento prostor je podprostorem prostoru $\mathbb{C}^{V \times V}$.

Důležitou roli hrají pro komplexní vektorové prostory tzv. hermitovské seskvilineární formy. Do jisté míry svým významem odpovídají symetrickým bilineárním formám na obecných vektorových prostorech.

24.15. Definice. Seskvilineární forma f na komplexním vektorovém prostoru V se nazývá *hermitovská*, jestliže pro každé dva vektory $x, y \in V$ je

$$f(x, y) = \overline{f(y, x)} .$$

Ukážeme, že seskvilineární forma f na komplexním vektorovém prostoru konečné dimenze je hermitovská právě tehdy, když její matice vzhledem k nějaké bázi je hermitovská.

Nechť $M = \{v_1, \dots, v_n\}$ je báze prostoru V a $A = (a_{ij})$ matice seskvilineární formy f vzhledem k bázi M . Je tedy

$$f(x, y) = \sum_{i,j=1}^n a_{ij} x_i \bar{y}_j ,$$

kde $\langle x \rangle_M = (x_1, \dots, x_n)$, $\langle y \rangle_M = (y_1, \dots, y_n)$. Je-li f hermitovská, je

$$a_{ij} = f(v_i, v_j) = \overline{f(v_j, v_i)} = \bar{a}_{ji} ,$$

tj. matice A je hermitovská. Je-li naopak A hermitovská, je

$$\overline{f(y, x)} = \overline{\sum_{i,j=1}^n a_{ji} y_j \bar{x}_i} = \sum_{i,j=1}^n \bar{a}_{ji} x_i \bar{y}_j = \sum_{i,j=1}^n a_{ij} x_i \bar{y}_j = f(x, y)$$

a forma f je hermitovská.

24.16. Věta. Jestliže je V komplexní vektorový prostor dimenze n , potom je prostor $\mathbb{B}_s(V)$ izomorfní s prostorem $\mathbb{C}^{n \times n}$ a $\dim \mathbb{B}_s(V) = n^2$. \square

Při izomorfismu prostoru $\mathbb{B}_s(V)$ na prostor $\mathbb{C}^{n \times n}$, který každé seskvilineární formě přiřazuje její matici vzhledem k nějaké pevně zvolené bázi, odpovídají hermitovským formám hermitovské matice. Stejně jako hermitovské matice netvoří podprostor v $\mathbb{C}^{n \times n}$, netvoří ani hermitovské formy podprostor v $\mathbb{B}_s(V)$. Součet dvou hermitovských forem je opět forma hermitovská, reálný násobek hermitovské formy je hermitovská forma; komplexní násobek hermitovské formy však už hermitovskou formou být nemusí (viz 7.8(vi)).

24.17. Věta. *Seskvilineární forma f na komplexním vektorovém prostoru V je hermitovská právě tehdy, když pro každý vektor $v \in V$ je $f(v, v)$ reálné číslo.*

Důkaz. Jestliže je forma f hermitovská, potom je $f(v, v) = \overline{f(v, v)}$, tj. pro každé $v \in V$ je $f(v, v)$ reálné číslo. Jestliže je naopak tato podmínka splněna, je podle lemmatu 24.13 $f(u, v) = \overline{f(v, u)}$. \square

24.18. Příklad. Seskvilineární forma f na prostoru \mathbb{C}^2 je dána analytickým vyjádřením vzhledem ke kanonické bázi:

$$f(x, y) = 3x_1\bar{y}_1 + (1+i)x_1\bar{y}_2 + (1-i)x_2\bar{y}_1 + 2x_2\bar{y}_2$$

Maticí formy f vzhledem ke kanonické bázi je matice

$$A = \begin{pmatrix} 3 & 1+i \\ 1-i & 2 \end{pmatrix}.$$

Forma f je hermitovská, neboť $f(x, y) = \overline{f(y, x)}$, jak se snadno přesvědčíme. Skutečnost, že je forma f hermitovská, je však ihned vidět z její matice (viz poznámka za definicí 24.15). Analytické vyjádření a matici A' formy f vzhledem k bázi $M = \{(1, i), (i, 1)\}$ snadno zjistíme pomocí matice přechodu B od báze M ke kanonické bázi:

$$B = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \quad A' = B^T A \bar{B} = \begin{pmatrix} 7 & 2-i \\ 2+i & 3 \end{pmatrix}.$$

Analytické vyjádření formy f vzhledem k bázi M je

$$f(x, y) = 7x'_1\bar{y}'_1 + (2-i)x'_1\bar{y}'_2 + (2+i)x'_2\bar{y}'_1 + 3x'_2\bar{y}'_2.$$

24.19. Definice. Nechť V je komplexní vektorový prostor konečné dimenze a f je hermitovská seskvilineární forma na prostoru V . Budeme říkat, že báze N prostoru V je *polární* vůči f , jestliže matice formy f vzhledem k bázi N je diagonální.

24.20. Věta. *Ke každé hermitovské seskvilineární formě na prostoru V existuje báze prostoru V , která je polární vůči f .* \square

24.21. Příklad. Hermitovská seskvilineární forma f na prostoru \mathbb{C}^3 je dána analytickým vyjádřením vzhledem ke kanonické bázi:

$$f(x, y) = x_1\bar{y}_1 + ix_1\bar{y}_2 + x_1\bar{y}_3 - ix_2\bar{y}_1 + (1+i)x_2\bar{y}_3 + x_3\bar{y}_1 + (1-i)x_3\bar{y}_2 + x_3\bar{y}_3$$

Maticí formy f vzhledem ke kanonické bázi je tedy hermitovská matice

$$A = \begin{pmatrix} 1 & i & 1 \\ -i & 0 & 1+i \\ 1 & 1-i & 1 \end{pmatrix}.$$

Najdeme bázi prostoru \mathbb{C}^3 , která je vůči formě f polární, a příslušné analytické vyjádření formy f :

$$\begin{aligned} \left(\begin{array}{ccc|ccc} 1 & i & 1 & 1 & 0 & 0 \\ -i & 0 & 1+i & 0 & 1 & 0 \\ 1 & 1-i & 1 & 0 & 0 & 1 \end{array} \right) &\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1+2i & i & 1 & 0 \\ 0 & 1-2i & 0 & -1 & 0 & 1 \end{array} \right) \rightsquigarrow \\ &\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & i & 1 & 0 \\ 0 & 0 & 5 & 1+i & 1-2i & 1 \end{array} \right) \end{aligned}$$

Od matice $(A|E)$ jsme dospěli k matici $(D|B^T)$, kde $D = B^T A \bar{B}$. Matice B je přitom maticí přechodu od nějaké báze N ke kanonické bázi. Nalezli jsme tedy bázi $N = \{(1, 0, 0), (i, 1, 0), (1+i, 1-2i, 1)\}$, která je vůči f polární, a analytické vyjádření formy f vzhledem k bázi N :

$$f(x, y) = x'_1 \bar{y}'_1 - x'_2 \bar{y}'_2 + 5x'_3 \bar{y}'_3$$

Forma f je zřejmě regulární.

24.22. Poznámka. Nechť f je seskvilineární forma na komplexním prostoru V . Ke každému vektoru $v \in V$ je zobrazení v^* prostoru V do tělesa \mathbb{C} definované rovností

$$v^*(x) = f(x, v)$$

lineární formou na prostoru V , neboť seskvilineární forma f je lineární v první složce. Zobrazení f_R prostoru V do duálního prostoru V^* definované rovností $f_R(v) = v^*$ je semihomomorfismus (viz 22.1), neboť seskvilineární forma f je semilineární v druhé složce. Pro každé $x, v \in V$ je $\langle x, f_R(v) \rangle = f(x, v)$. Jádrem semihomomorfismu f_R je pravý vrchol formy f , tj. $\text{Ker } f_R = R(f)$.

Jestliže V je prostor konečné dimenze a f regulární seskvilineární forma na prostoru V , potom je f_R vzájemně jednoznačný semihomomorfismus prostoru V na prostor V^* ; ke každé lineární formě $g \in V^*$ tedy existuje jednoznačně určený vektor $v \in V$ takový, že $g = v^*$, tj. pro každé $x \in V$ je $\langle x, g \rangle = f(x, v)$.

24.23. Poznámka. Podobně je ke každému vektoru $v \in V$ zobrazení v^\sim prostoru V do tělesa \mathbb{C} definované rovností

$$v^\sim(x) = f(v, x)$$

semilineární formou na prostoru V , neboť seskvilineární forma f je semilineární ve druhé složce. Zobrazení f_L prostoru V do semiduálního prostoru V^\sim definované rovností $f_L(v) = v^\sim$ je homomorfismus, neboť seskvilineární forma f je lineární v první složce. Pro každé $v, x \in V$ je $\langle f_L(v), x \rangle = f(v, x)$. Jádrem homomorfismu f_L je levý vrchol formy f , tj. platí rovnost $\text{Ker } f_L = L(f)$.

Jestliže V je prostor konečné dimenze a f regulární seskvilineární forma na V , potom je f_L izomorfismus prostoru V na semidualem prostoru V^\sim ; ke každé seskvilineární formě $g \in V^\sim$ tedy existuje jednoznačně určený vektor $v \in V$ takový, že $g = v^\sim$, tj. pro každé $x \in V$ je $\langle g, x \rangle = f(v, x)$.

Na komplexních vektorových prostorech můžeme uvažovat jednak kvadratické formy, které jsou vytvářeny bilineárními formami způsobem popsaným v předchozím paragrafu (viz definice 23.24), jednak kvadratické formy, které jsou obdobným způsobem vytvářeny seskvilineárními formami. Vzhledem k tomu, že oba tyto druhy zobrazení jsou nazývány kvadratickými formami, hovoří se někdy pro rozlišení o *kvadratických formách prvního druhu* a o *kvadratických formách druhého druhu*. Kvadratické formy druhého druhu budeme vyšetřovat v následujících odstavcích.

24.24. Definice. Nechť V je komplexní vektorový prostor. Zobrazení q prostoru V do tělesa komplexních čísel se nazývá *kvadratická forma druhého druhu*, jestliže existuje taková seskvilineární forma f na prostoru V , že pro každý vektor $v \in V$ je $q(v) = f(v, v)$; budeme říkat, že kvadratická forma q je *vytvořena seskvilineární formou f* .

24.25. Příklady.

(i) Nejjednodušší kvadratickou formou druhého druhu na komplexním prostoru V je tzv. *nulová kvadratická forma*, která každému vektoru $v \in V$ přiřazuje nulový prvek tělesa T . Je vytvořena nulovou seskvilineární formou na prostoru V .

(ii) Je-li g_1 lineární a g_2 semilineární forma na komplexním prostoru V , potom zobrazení q , které vektoru $v \in V$ přiřazuje skalár $q(v) = g_1(v) \cdot g_2(v)$, je kvadratická forma druhého druhu na prostoru V .

(iii) Nechť $A = (a_{ij})$ je komplexní čtvercová matice řádu n . Zobrazení, které vektoru $x = (x_1, \dots, x_n) \in \mathbb{C}^n$ přiřadí komplexní číslo

$$q(x) = \sum_{i,j=1}^n a_{ij} x_i \bar{x}_j = (x_1, \dots, x_n) \cdot A \cdot (\bar{x}_1, \dots, \bar{x}_n)^T,$$

je kvadratická forma druhého druhu na prostoru \mathbb{C}^n .

Množinu všech kvadratických forem druhého druhu na komplexním prostoru V značíme $Q_s(V)$ (index s je od slova seskvilineární).

V předchozím paragrafu jsme viděli, že jestliže $\text{char } T \neq 2$, potom je každá kvadratická forma prvního druhu $f \in Q(V)$ vytvořena více bilineárními formami, z nichž právě jediná je symetrická. U komplexních prostorů a kvadratických forem druhého druhu je situace jiná.

24.26. Věta. *Nechť V je komplexní vektorový prostor. Potom platí:*

- (i) *Množina $Q_s(V)$ všech kvadratických forem druhého druhu na prostoru V je podprostorem vektorového prostoru \mathbb{C}^V .*
- (ii) *Zobrazení Φ , které každé seskvilineární formě f na prostoru V přiřazuje kvadratickou formu vytvořenou formou f , je izomorfismus vektorového prostoru $B_s(V)$ na vektorový prostor $Q_s(V)$. Jestliže je $\dim V = n$, potom je $\dim Q_s(V) = n^2$.*

Důkaz. Snadno se ukáže, že součet dvou kvadratických forem a násobek kvadratické formy jsou opět kvadratické formy. Jestliže kvadratické formy q, q_1, q_2 jsou vytvořeny seskvilineárními formami f, f_1, f_2 , potom je

$$(q_1 + q_2)(x) = q_1(x) + q_2(x) = f_1(x, x) + f_2(x, x) = (f_1 + f_2)(x, x) ,$$

$$(aq)(x) = a \cdot q(x) = a \cdot f(x, x) = (af)(x, x) ,$$

tj. $q_1 + q_2$, resp. aq je kvadratická forma vytvořená seskvilineární formou $f_1 + f_2$, resp. af . Zapišeme-li tato fakta pomocí výše definovaného zobrazení Φ , dostáváme rovnosti

$$\Phi(f_1 + f_2) = \Phi(f_1) + \Phi(f_2) , \quad \Phi(af) = a \cdot \Phi(f) ,$$

takže Φ je homomorfismus. Jestliže $\Phi(f) = q$, potom podle lemmatu 24.13 je pro libovolné vektory $x, y \in V$

$$f(x, y) = \frac{1}{4} \cdot (q(x + y) - q(x - y) + i \cdot q(x + iy) - i \cdot q(x - iy)) .$$

Forma f je tedy jednoznačně určena formou q a homomorfismus Φ je izomorfismus. \square

Dokázali jsme, že kvadratická forma q na komplexním vektorovém prostoru jednoznačně určuje seskvilineární formu, kterou je vytvořena.

24.27. Definice. Kvadratická forma na komplexním vektorovém prostoru se nazývá *hermitovská*, je-li vytvořena hermitovskou seskvilineární formou.

Z věty 24.17 ihned vyplývá následující tvrzení.

24.28. Věta. *Kvadratická forma na komplexním vektorovém prostoru je hermitovská právě tehdy, když nabývá pouze reálných hodnot.* \square

Nechť V je komplexní vektorový prostor dimenze n a M jeho báze, nechť q je kvadratická forma na prostoru V vytvořená seskvilineární formou f . Maticí kvadratické formy q vzhledem k bázi M budeme rozumět matici formy f vzhledem k bázi M . Označíme-li tuto matici A , potom je pro každý vektor $x \in V$

$$q(x) = \langle x \rangle_M \cdot A \cdot \overline{\langle x \rangle_M}^T .$$

25. HERMITOVSKÉ A SYMETRICKÉ FORMY

Hermitovské seskvilineární formy na komplexních vektorových prostorech odpovídají svým významem symetrickým bilineárním formám na reálných vektorových prostorech. Některé výsledky týkající se hermitovských a symetrických forem můžeme vyložit současně. Definice a věty tohoto paragrafu zformulujeme ve dvou verzích — jak pro hermitovské, tak pro symetrické formy. Všechny důkazy však budeme provádět jen pro hermitovské seskvilineární formy; vynecháním pruhů znázorňujících komplexně sdružená čísla tyto důkazy přejdou v důkazy pro symetrické bilineární formy.

Na komplexním vektorovém prostoru V jsou hermitovské seskvilineární formy charakterizovány tím, že jejich hodnoty na množině $\Delta_V = \{(v, v); v \in V\}$ jsou reálné (viz 24.17). Ze všech seskvilineárních forem má tedy smysl jen hermitovské formy klasifikovat podle toho, zda na množině Δ_V nabývají pouze kladných, záporných, nezáporných či nekladných hodnot.

Jestliže f je bilineární forma na reálném vektorovém prostoru V , potom pro každý vektor $v \in V$ je $f(v, v) = f_s(v, v)$, kde f_s je symetrická část formy f . Každá bilineární forma tedy nabývá na množině Δ_V stejných hodnot jako její symetrická část. Stačí tedy ze všech bilineárních forem jen symetrické formy rozlišovat podle toho, zda na množině Δ_V nabývají pouze kladných, záporných, nezáporných či nekladných hodnot.

25.1. Definice. Hermitovská seskvilineární forma f na komplexním (symetrická bilineární forma na reálném) vektorovém prostoru V se nazývá

- *pozitivně semidefinitní*, resp. *negativně semidefinitní*, jestliže pro každý vektor $v \in V$ je $f(v, v) \geq 0$, resp. $f(v, v) \leq 0$;
- *pozitivně definitní*, resp. *negativně definitní*, jestliže pro každý nenulový vektor $v \in V$ je $f(v, v) > 0$, resp. $f(v, v) < 0$;
- *indefinitní*, jestliže existují vektory $x, y \in V$ takové, že $f(x, x) < 0 < f(y, y)$.

Každá pozitivně definitní forma je zřejmě pozitivně semidefinitní a podobně každá negativně definitní forma je negativně semidefinitní.

25.2. Definice. Nechť V je komplexní (reálný) vektorový prostor konečné dimenze, N jeho báze a f hermitovská seskvilineární (symetrická bilineární) forma na prostoru V . Jestliže analytické vyjádření formy f vzhledem k bázi N má tvar

$$f(x, y) = x_1 \bar{y}_1 + \cdots + x_p \bar{y}_p - x_{p+1} \bar{y}_{p+1} - \cdots - x_{p+n} \bar{y}_{p+n} ,$$

kde $0 \leq p$, $0 \leq n$, $p+n \leq \dim V$, pak říkáme, že báze N prostoru V je *normální vůči f* a uvedené analytické vyjádření nazýváme *normálním tvarem* formy f .

Matice formy f vzhledem k bázi N je tedy diagonální a na diagonále má po řadě p jedniček, n minus jedniček a $\dim V - p - n$ nul. Báze N prostoru V je tedy polární vůči f (viz definice 23.19 a 24.19). Poznamenejme, že ne každá báze, která je vůči f polární, je vůči f normální.

25.3. Věta. *Ke každé hermitovské seskvilineární (symetrické bilineární) formě na komplexním (reálném) vektorovém prostoru V konečné dimenze existuje báze prostoru V , která je vůči ní normální.*

Důkaz. Nechť f je hermitovská forma na komplexním prostoru V a M nějaká jeho báze. Matice A formy f vzhledem k bázi M je hermitovská a proto podle věty 12.30 existuje regulární matice B taková, že matice $B^T A \bar{B}$ je reálná diagonální matice, která má na hlavní diagonále po řadě jedničky, minus jedničky a nuly (je-li na místě ii nenulové číslo a , vynásobíme i -tý řádek a i -tý sloupec číslem $\frac{1}{\sqrt{|a|}}$).

Nechť N je taková báze prostoru V , že matice B je maticí přechodu od báze N k bázi M . Podle věty 24.7 má forma f vzhledem k bázi N matici $B^T A \bar{B}$, tj. báze N je normální vůči formě f . \square

Poznamenejme, že při předchozím důkazu bylo možno vyjít z báze, která je vůči formě f polární, vhodnými skaláry vynásobit vektory této báze a případně změnit jejich pořadí.

Důkaz předchozí věty dává spolu s důkazem věty 12.30, resp. 12.28 konkrétní návod, jak najít normální tvar dané hermitovské, resp. symetrické formy a bázi, která je vůči ní normální.

25.4. Sylvesterův zákon setrvačnosti. *Normální tvar hermitovské seskvilineární (symetrické bilineární) formy f na komplexním (reálném) vektorovém prostoru V konečné dimenze je invariantní, tj. nezávisí na konkrétní volbě báze, která je vůči formě f normální.*

Důkaz. Je třeba dokázat, že ve všech normálních tvarech formy f je stejný počet jedniček, stejný počet minus jedniček a stejný počet nul. Nechť tedy $\dim V = k$ a nechť

$$N = \{v_1, \dots, v_k\} \quad \text{a} \quad M = \{w_1, \dots, w_k\}$$

jsou dvě báze prostoru V , které jsou normální vůči f . Nechť

$$f(x, y) = x_1 \bar{y}_1 + \dots + x_p \bar{y}_p - x_{p+1} \bar{y}_{p+1} - \dots - x_{p+n} \bar{y}_{p+n}$$

je normální tvar formy f vzhledem k bázi N ($0 \leq p, 0 \leq n, p+n \leq k$) a

$$f(x, y) = \xi_1 \bar{\eta}_1 + \dots + \xi_r \bar{\eta}_r - \xi_{r+1} \bar{\eta}_{r+1} - \dots - \xi_{r+s} \bar{\eta}_{r+s}$$

je normální tvar formy f vzhledem k bázi M ($0 \leq r, 0 \leq s, r+s \leq k$). Předpokládejme, že $p > r$. Označme

$$V_1 = [v_1, \dots, v_p] \quad \text{a} \quad V_2 = [w_{r+1}, \dots, w_k].$$

Podle věty o dimenzích spojení a průniku dvou podprostorů (s přihlédnutím k předpokladu $p > r$) je

$$\dim(V_1 \cap V_2) + \dim(V_1 + V_2) = \dim V_1 + \dim V_2 = p + k - r > k = \dim V,$$

takže $V_1 \cap V_2$ je netriviální podprostor prostoru V ; existuje tedy nenulový vektor $z \in V_1 \cap V_2$. Jestliže

$$\langle z \rangle_N = (z_1, \dots, z_k) \quad \text{a} \quad \langle z \rangle_M = (\zeta_1, \dots, \zeta_k),$$

potom podle definice podprostorů V_1 a V_2 je

$$z_{p+1} = \dots = z_k = 0 \quad \text{a} \quad \zeta_1 = \dots = \zeta_r = 0.$$

Dosažením souřadnic vektoru z do obou výše uvedených normálních tvarů formy f dostaneme:

$$f(z, z) = \sum_{i=1}^p |z_i|^2 > 0 \quad \text{a} \quad f(z, z) = - \sum_{i=r+1}^{r+s} |\zeta_i|^2 \leq 0$$

(ve druhém případě nedostaneme ostrou nerovnost, neboť nenulový koeficient ζ_i může existovat až pro $i > r + s$). Předpoklad $p > r$ tedy vede ke sporu; z hlediska symetrie nemůže být ani $p < r$. Je tedy $p = r$, tj. oba normální tvary formy f mají stejný počet kladných členů. Mají však i stejný počet záporných členů, neboť číslo $p + n$ i číslo $r + s$ je rovno hodnotě formy f . \square

Nechť f je hermitovská (symetrická) forma na komplexním (reálném) vektorovém prostoru V konečné dimenze. Označme $p(f)$, resp. $n(f)$ počet kladných, resp. záporných koeficientů v normálním tvaru formy f . Podle Sylvesterova zákona setrvačnosti jsou tato čísla nezávislá na volbě báze, která je normální vůči f . Tento fakt umožňuje vyslovit následující definici.

25.5. Definice. Nechť V je komplexní (reálný) vektorový prostor konečné dimenze a f hermitovská seskvilineární (symetrická bilineární) forma na prostoru V . *Signaturou* formy f budeme rozumět trojici $(p(f), n(f), d(f))$, kde $p(f)$, resp. $n(f)$ je počet kladných, resp. záporných koeficientů v normálním tvaru formy f a $d(f)$ je nulita formy f .

Zřejmě je

$$p(f) + n(f) + d(f) = \dim V \quad \text{a} \quad p(f) + n(f) = r(f).$$

Poznamenejme, že signaturu formy f zjistíme už z jejího analytického vyjádření vzhledem k bázi, která je vůči f polární, neboť přechodem k normálnímu tvaru se již počet kladných, záporných a nulových koeficientů nemění.

Stanovením signatury zjistíme nejen to, zda daná hermitovská (symetrická) forma je regulární či singulární, ale i to, zda je pozitivně či negativně definitní, resp. semidefinitní nebo indefinitní.

25.6. Věta. Hermitovská seskvilineární (symetrická bilineární) forma f na komplexním (reálném) vektorovém prostoru V dimenze k je

- pozitivně definitní, právě když $p(f) = k$ (tj. $n(f) = d(f) = 0$),
- negativně definitní, právě když $n(f) = k$ (tj. $p(f) = d(f) = 0$),
- pozitivně semidefinitní, právě když $n(f) = 0$ (tj. $p(f) + d(f) = k$),
- negativně semidefinitní, právě když $p(f) = 0$ (tj. $n(f) + d(f) = k$),
- indefinitní, právě když $p(f) > 0$ a $n(f) > 0$.

Důkaz. Vyjádříme-li formu f v normálním tvaru, jsou všechny uvedené ekvivalence zřejmé. \square

Každá pozitivně (negativně) definitní hermitovská seskvilineární, resp. symetrická bilineární forma je zřejmě regulární. Regulární forma však může být také indefinitní ($p(f) \neq 0$, $n(f) \neq 0$, $d(f) = 0$).

Pro symetrické bilineární formy na vektorovém prostoru nad obecným tělesem T nemá pojem signatury smysl. Těleso T by muselo být uspořádané, tj. museli bychom umět rozlišit kladné a záporné prvky, podobně jako v tělese reálných čísel. Vzhledem k tomu, že každé uspořádané těleso má charakteristiku nula², není možno signaturu definovat pro symetrické bilineární formy na prostorech nad konečnými tělesy.

Pro symetrické bilineární formy na komplexním vektorovém prostoru konečné dimenze nemá pojem signatury smyslu. Symetrickými úpravami můžeme totiž každý nenulový prvek diagonální matice změnit jak na jedničku, tak na minus jedničku. Je-li totiž na místě kk v diagonální matici A jednička (minus jednička), potom po znásobení k -tého řádku a k -tého sloupce komplexní jednotkou i (tj. po symetrické úpravě) dostaneme na místě kk minus jedničku (jedničku). Tento fakt úzce souvisí se skutečností, že těleso komplexních čísel není uspořádaným tělesem; uvědomme si, že komplexní symetrické matice mají na diagonále obecně komplexní čísla.

25.7. Příklady.

(i) Na vektorovém prostoru \mathbb{C}^3 je dána hermitovská seskvilineární forma svým analytickým vyjádřením vzhledem ke kanonické bázi:

$$f(x, y) = x_1\bar{y}_1 + ix_1\bar{y}_2 + (1+i)x_1\bar{y}_3 - ix_2\bar{y}_1 + x_2\bar{y}_3 + (1-i)x_3\bar{y}_1 + x_3\bar{y}_2 + 2x_3\bar{y}_3$$

Vzhledem ke kanonické bázi má tedy forma f matici

$$A = \begin{pmatrix} 1 & i & 1+i \\ -i & 0 & 1 \\ 1-i & 1 & 2 \end{pmatrix}.$$

² Viz např. V. Kořínek: *Základy algebry*, Praha 1956, str. 109, odst. 9,14.

Bázi prostoru \mathbb{C}^3 , která je normální vůči f , najdeme tak, že budeme v matici A provádět hermitovské elementární úpravy a současně budeme v jednotkové matici E zachycovat prováděné řádkové úpravy:

$$\begin{aligned} \left(\begin{array}{ccc|ccc} 1 & i & 1+i & 1 & 0 & 0 \\ -i & 0 & 1 & 0 & 1 & 0 \\ 1-i & 1 & 2 & 0 & 0 & 1 \end{array} \right) &\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & i & 0 & 1 & 0 \\ 0 & -i & 0 & 0 & -1+i & 1 \end{array} \right) &\rightsquigarrow \\ &\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & i & 1 & 0 \\ 0 & 0 & 1 & i & -i & 1 \end{array} \right) &\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & i & -i & 1 \\ 0 & 0 & -1 & i & 1 & 0 \end{array} \right) \end{aligned}$$

Tím jsme matici A převedli hermitovskými úpravami na diagonální matici D , která má na diagonále dvě jedničky a jednu minus jedničku. Současně jsme našli i příslušnou transformační matici B ze vztahu $B^T A \bar{B} = D$:

$$B = \begin{pmatrix} 1 & i & i \\ 0 & -i & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Matice, která po provedených hermitovských úpravách stojí vpravo od matice D , je transformační matice působící na řádky matice A , tj. ta matice, kterou se matice A násobí zleva. Od matice $(A|E)$ jsme tedy uvedenými úpravami dospěli k matici $(D|B^T)$. Násobením snadno ověříme, že je $B^T A \bar{B} = D$:

$$\begin{pmatrix} 1 & 0 & 0 \\ i & -i & 1 \\ i & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & i & 1+i \\ -i & 0 & 1 \\ 1-i & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -i & -i \\ 0 & i & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Báze $N = \{(1, 0, 0), (i, -i, 1), (i, 1, 0)\}$ prostoru \mathbb{C}^3 je tedy normální vůči formě f . Forma f má normální tvar

$$f(x, y) = x'_1 \bar{y}'_1 + x'_2 \bar{y}'_2 - x'_3 \bar{y}'_3,$$

signaturu $(2, 1, 0)$, je indefinitní.

Pokud bychom chtěli zjistit pouze signaturu formy f , resp. její normální tvar, pak stačí převést matici A hermitovskými úpravami na diagonální matici D a není třeba sledovat prováděné řádkové úpravy.

(ii) Na vektorovém prostoru \mathbb{C}^3 je dána hermitovská seskvilineární forma analytickým vyjádřením vzhledem ke kanonické bázi:

$$f(x, y) = x_1 \bar{y}_1 + i x_1 \bar{y}_2 + x_1 \bar{y}_3 - i x_2 \bar{y}_1 + i x_2 \bar{y}_3 + x_3 \bar{y}_1 - i x_3 \bar{y}_2 + 2 x_3 \bar{y}_3$$

Podobně jako v předcházejícím příkladu převedeme matici této formy hermitovskými úpravami na vhodný diagonální tvar:

$$\begin{aligned} & \left(\begin{array}{ccc|ccc} 1 & i & 1 & 1 & 0 & 0 \\ -i & 0 & i & 0 & 1 & 0 \\ 1 & -i & 2 & 0 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 2i & i & 1 & 0 \\ 0 & -2i & 1 & -1 & 0 & 1 \end{array} \right) \rightsquigarrow \\ & \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & i & 1 & 0 \\ 0 & 0 & 5 & 1 & -2i & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & \frac{1}{\sqrt{5}} & \frac{-2i}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ 0 & 0 & -1 & i & 1 & 0 \end{array} \right) \end{aligned}$$

Báze

$$N = \left\{ (1, 0, 0), \left(\frac{1}{\sqrt{5}}, -\frac{2i}{\sqrt{5}}, \frac{1}{\sqrt{5}} \right), (i, 1, 0) \right\}$$

prostoru \mathbb{C}^3 je normální vůči formě f . Forma f má normální tvar

$$f(x, y) = x'_1 \bar{y}'_1 + x'_2 \bar{y}'_2 - x'_3 \bar{y}'_3,$$

signaturu $(2, 1, 0)$, je indefinitní.

(iii) Na vektorovém prostoru \mathbb{C}^3 je dána hermitovská seskvilineární forma analytickým vyjádřením vzhledem ke kanonické bázi:

$$f(x, y) = x_1 \bar{y}_1 + (1 + i)x_1 \bar{y}_2 + 2ix_1 \bar{y}_3 +$$

$$+ (1 - i)x_2 \bar{y}_1 + 3x_2 \bar{y}_2 + (2 + i)x_2 \bar{y}_3 - 2ix_3 \bar{y}_1 + (2 - i)x_3 \bar{y}_2 + 6x_3 \bar{y}_3$$

Potřebujeme-li zjistit pouze signaturu této formy (a nepotřebujeme-li nalézt nějakou normální bázi), upravíme matici formy f hermitovskými úpravami na diagonální tvar:

$$\left(\begin{array}{ccc} 1 & 1 + i & 2i \\ 1 - i & 3 & 2 + i \\ -2i & 2 - i & 6 \end{array} \right) \rightsquigarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & -i \\ 0 & i & 2 \end{array} \right) \rightsquigarrow \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right)$$

Forma f je pozitivně definitní.

Pojmy, které jsme v tomto paragrafu zavedli pro symetrické bilineární, resp. hermitovské seskvilineární formy, a výsledky, které jsme pro ně zformulovali a dokázali, se snadno přenesou a zformulují pro kvadratické formy prvního, resp. druhého druhu. Můžeme tedy hovořit o pozitivně a negativně definitních či semidefinitních kvadratických formách na reálných, resp. komplexních prostorech, o bázích, které jsou vůči kvadratické formě normální, o signatuře kvadratické formy atd.

25.8. Příklady.

(i) Kvadratická forma druhého druhu, která je na prostoru \mathbb{C}^3 dána analytickým vyjádřením vzhledem ke kanonické bázi

$$q(x) = |x_1|^2 + ix_1\bar{x}_2 + (1+i)x_1\bar{x}_3 - ix_2\bar{x}_1 + x_2\bar{x}_3 + (1-i)x_3\bar{x}_1 + x_3\bar{x}_2 + 2|x_3|^2,$$

je vytvořena hermitovskou seskvilineární formou f z příkladu 25.7(i). Její normální tvar je

$$q(x) = |x'_1|^2 + |x'_2|^2 - |x'_3|^2,$$

báze $N = \{(1, 0, 0), (i, -i, 1), (i, 1, 0)\}$ je normální vůči kvadratické formě q ; forma q je indefinitní, její signatura je $(2, 1, 0)$.

(ii) Kvadratická forma druhého druhu, která je na prostoru \mathbb{C}^3 dána analytickým vyjádřením vzhledem ke kanonické bázi

$$q(x) = |x_1|^2 + ix_1\bar{x}_2 + x_1\bar{x}_3 - ix_2\bar{x}_1 + ix_2\bar{x}_3 + x_3\bar{x}_1 - ix_3\bar{x}_2 + 2|x_3|^2,$$

je vytvořena hermitovskou seskvilineární formou f z příkladu 25.7(ii). Její normální tvar je

$$q(x) = |x'_1|^2 + |x'_2|^2 - |x'_3|^2,$$

báze

$$N = \{(1, 0, 0), (\frac{1}{\sqrt{5}}, -\frac{2i}{\sqrt{5}}, \frac{1}{\sqrt{5}}), (i, 1, 0)\}$$

je normální vůči q ; forma q je indefinitní, její signatura je $(2, 1, 0)$.

(iii) Kvadratická forma druhého druhu, která je na prostoru \mathbb{C}^3 dána analytickým vyjádřením vzhledem ke kanonické bázi

$$q(x) = |x_1|^2 + (1+i)x_1\bar{x}_2 + 2ix_1\bar{x}_3 + (1-i)x_2\bar{x}_1 + 3|x_2|^2 + (2+i)x_2\bar{x}_3 - \\ - 2ix_3\bar{x}_1 + (2-i)x_3\bar{x}_2 + 6|x_3|^2,$$

je vytvořena hermitovskou seskvilineární formou f z příkladu 25.7(iii). Její normální tvar je

$$q(x) = |x'_1|^2 + |x'_2|^2 + |x'_3|^2,$$

forma q je pozitivně definitní.

VI. SKALÁRNÍ SOUČIN

26. UNITÁRNÍ PROSTORY

V celé této části knihy (26. – 31. paragraf) budeme písmenem T značit buď těleso \mathbb{R} reálných čísel nebo těleso \mathbb{C} komplexních čísel.

26.1. Definice. Nechť V je vektorový prostor nad tělesem T . *Skalárním součinem* na prostoru V nazveme každé zobrazení f množiny $V \times V$ do tělesa T , které má následující vlastnosti:

- (i) $\forall x, y \in V \quad f(x, y) = \overline{f(y, x)}$,
- (ii) $\forall x, y, z \in V \quad f(x + y, z) = f(x, z) + f(y, z)$,
- (iii) $\forall x, y \in V \quad \forall a \in T \quad f(ax, y) = a \cdot f(x, y)$,
- (iv) $\forall x \in V, \quad x \neq 0 \quad f(x, x) > 0$.

Prostorem se skalárním součinem, resp. *unitárním prostorem* budeme rozumět každý vektorový prostor s nějakým pevně zvoleným skalárním součinem. *Reálným*, resp. *komplexním unitárním prostorem* budeme rozumět unitární prostor nad tělesem reálných, resp. komplexních čísel.

Skalární součin se většinou neoznačuje písmenem. Obraz dvojice $(x, y) \in V \times V$ při skalárním součinu f , tj. číslo $f(x, y) \in T$, budeme v dalším textu značit symbolem $(x|y)$ a nazývat *skalárním součinem vektorů* x, y . Vlastnosti skalárního součinu můžeme pomocí tohoto symbolu přepsat do následujícího tvaru:

- (i) $\forall x, y \in V \quad (x|y) = \overline{(y|x)}$,
- (ii) $\forall x, y, z \in V \quad (x + y|z) = (x|z) + (y|z)$,
- (iii) $\forall x, y \in V \quad \forall a \in T \quad (ax|y) = a \cdot (x|y)$,
- (iv) $\forall x \in V, \quad x \neq 0 \quad (x|x) > 0$.

První vlastnost skalárního součinu znamená, že čísla $(x|y)$ a $(y|x)$ jsou navzájem komplexně sdružená, číslo $(x|x)$ je tedy vždy reálné; podle čtvrté vlastnosti je číslo $(x|x)$ pro nenulový vektor x dokonce kladné.

Pro reálný unitární prostor přejde vlastnost (i) z definice 26.1 v tzv. *symetrii* skalárního součinu

$$\forall x, y \in V \quad (x|y) = (y|x) .$$

Pro komplexní unitární prostor by však symetrie spolu s vlastnostmi (ii), (iii) byla ve sporu s vlastností (iv). Bylo by totiž

$$(x|ay) = (ay|x) = a \cdot (y|x) = a \cdot (x|y) ,$$

odtud by bylo

$$(ax|ay) = a^2 \cdot (x|y) ;$$

pro $x = y$ a $a = i$ by bylo $(ix|ix) = -(x|x)$, což je opravdu ve sporu s vlastností (iv).

26.2. Věta. *Nechť V je unitární prostor. Potom platí:*

- (i) $\forall x \in V \quad (o|x) = (x|o) = 0$,
 - (ii) $\forall x, y, z \in V \quad (x|y+z) = (x|y) + (x|z)$,
 - (iii) $\forall x, y \in V \quad \forall a \in T \quad (x|ay) = \bar{a} \cdot (x|y)$,
 - (iv) $\forall x_1, \dots, x_n, y_1, \dots, y_m \in V \quad \forall a_1, \dots, a_n, b_1, \dots, b_m \in T$
- $$\left(\sum_{k=1}^n a_k x_k \middle| \sum_{j=1}^m b_j y_j \right) = \sum_{k=1}^n \sum_{j=1}^m a_k \bar{b}_j (x_k | y_j) .$$

Důkaz. Z vlastností skalárního součinu uvedených v definici 26.1 vyplývají následující rovnosti:

- (i) $(o|x) = (0x|x) = 0 \cdot (x|x) = 0$, $(x|o) = \overline{(o|x)} = \bar{0} = 0$,
- (ii) $(x|y+z) = \overline{(y+z|x)} = \overline{(y|x) + (z|x)} = \overline{(y|x)} + \overline{(z|x)} = (x|y) + (x|z)$,
- (iii) $(x|ay) = \overline{(ay|x)} = \overline{a \cdot (y|x)} = \bar{a} \cdot \overline{(y|x)} = \bar{a} \cdot (x|y)$.

Rovnost (iv) dostaneme z rovností 26.1(ii), (iii) a 26.2 (ii), (iii) užitím matematické indukce. \square

Z 26.1 a 26.2 vyplývá, že skalární součin na reálném unitárním prostoru je *symetrická pozitivně definitní bilineární forma* a skalární součin na komplexním unitárním prostoru je *hermitovská pozitivně definitní seskvilineární forma*.

Místo skalární součin se často říká *vnitřní součin* a termín skalární součin se rezervuje pro běžný skalární součin vektorů v rovině nebo v prostoru. Někdy se skalárním součinem rozumí zobrazení, které má pouze první tři vlastnosti z definice 26.1; skalární součin definovaný v 26.1 je potom tzv. *pozitivně definitní skalární součin*. Reálný unitární prostor se někdy nazývá eukleidovský prostor a komplexní unitární prostor pouze unitární prostor; někdy se tyto termíny užívají jen pro prostory konečné dimenze.

Nechť V je unitární prostor a W jeho podprostor (jako vektorového prostoru). Zúžením skalárního součinu prostoru V na podprostor W dostáváme skalární součin na podprostoru W , který se tak přirozeným způsobem stává unitárním prostorem. Zvolením skalárního součinu na vektorovém prostoru V se tedy nejen prostor V stane unitárním prostorem, ale i všechny jeho podprostory.

26.3. Příklady.

(i) Skalární součin dvou nenulových vektorů v prostoru (v rovině), které mají počátek v pevně zvoleném bodě, definujeme jako součin jejich délek a kosinu úhlu, který svírají. Skalární součin nulového vektoru s libovolným vektorem klademe rovný nule.

(ii) Na vektorovém prostoru T^n definujeme skalární součin obvyklým způsobem: pro vektory $x = (x_1, \dots, x_n)$ a $y = (y_1, \dots, y_n)$ nechť

$$(x|y) = \sum_{k=1}^n x_k \bar{y}_k .$$

O tomto skalárním součinu budeme hovořit jako o *standardním skalárním součinu*.

(iii) V prostoru všech reálných funkcí spojitých na intervalu $\langle a, b \rangle$ definujeme skalární součin rovností

$$(f|g) = \int_a^b f(x)g(x)dx .$$

Tím je definován skalární součin i na prostoru všech polynomů, resp. na prostoru všech polynomů stupně nejvýše n apod.

(iv) V prostoru komplexních funkcí reálné proměnné, které jsou spojitě na intervalu $\langle a, b \rangle$, definujeme skalární součin rovností

$$(f|g) = \int_a^b f(x)\overline{g(x)}dx .$$

(v) V prostoru $T^{n \times n}$ všech čtvercových matic řádu n definujeme skalární součin rovností

$$(A|B) = \text{tr}(A \cdot \overline{B}^T) .$$

Připomeňme, že $\text{tr} A$ je tzv. *stopa* matice A ; je-li $A = (a_{ij})$ matice řádu n , potom $\text{tr} A = \sum_{k=1}^n a_{kk}$. Tedy

$$(A|B) = \sum_{k=1}^n \sum_{j=1}^n a_{kj} \overline{b_{kj}} .$$

(vi) V prostoru \mathbb{R}^2 je rovností

$$(x|y) = 2x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$$

definován skalární součin. Podobně se prostor \mathbb{R}^3 stane unitárním prostorem, položíme-li např.

$$(x|y) = x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_2 + x_3y_3 .$$

Ve všech výše uvedených příkladech snadno prověříme, že jde o skalární součin.

26.4. Definice. Nechť V je unitární prostor. *Normou* (též *délkou*) vektoru $v \in V$ budeme rozumět reálné číslo $\|v\|$ definované rovností $\|v\| = \sqrt{(v|v)}$. Vektor v se nazývá *normovaný* (též *jednotkový*), jestliže je $\|v\| = 1$.

V rovině nebo prostoru (viz příklad 26.3(i)) je norma vektoru rovna jeho skutečné délce; definice 26.4 tedy koresponduje s naší geometrickou představou.

Uvědomme si, že definice normy vektoru se opírá o čtvrtou vlastnost skalárního součinu: pro každý nenulový vektor $v \in V$ je $(v|v)$ kladné reálné číslo.

Poznamenejme, že zobrazení, které každému vektoru unitárního prostoru V přiřazuje jeho normu, se pouze odmocninou liší od kvadratické formy určené skalárním součinem jako bilineární, resp. seskvilineární formou na prostoru V .

Normu vektoru značíme dvěma dvojicemi svislých čar, abychom odlišili normu vektoru od absolutní hodnoty čísla.

26.5. Věta. *Nechť V je unitární prostor. Potom platí:*

- (i) $\|o\| = 0$,
- (ii) $\forall x \in V, x \neq o \quad \|x\| > 0$,
- (iii) $\forall x \in V \quad \forall a \in T \quad \|ax\| = |a| \cdot \|x\|$,
- (iv) $\forall x \in V, x \neq o \quad \left\| \frac{1}{\|x\|} \cdot x \right\| = 1$,
- (v) $\forall x, y \in V \quad \|x + y\|^2 + \|x - y\|^2 = 2 \cdot \|x\|^2 + 2 \cdot \|y\|^2$.

Důkaz. Tvrzení (i) a (ii) jsou bezprostředními důsledky definice 26.1 a definice 26.4. Z vlastností skalárního součinu a z definice normy dostáváme rovnost

$$\|ax\|^2 = (ax|ax) = a \cdot \bar{a} \cdot (x|x) = |a|^2 \cdot \|x\|^2,$$

ze které vyplývá tvrzení (iii). Tvrzení (iv) je jednoduchým důsledkem tvrzení (iii); vynásobení vektoru převrácenou hodnotou jeho normy se nazývá *normování vektoru*. Dále je

$$\begin{aligned} \|x + y\|^2 &= (x + y|x + y) = (x|x) + (x|y) + (y|x) + (y|y), \\ \|x - y\|^2 &= (x - y|x - y) = (x|x) - (x|y) - (y|x) + (y|y); \end{aligned}$$

sečtením těchto dvou rovností dostaneme rovnost uvedenou v tvrzení (v). \square

V rovině nebo v prostoru (viz příklad 26.3(i)) vynikne geometrický smysl rovnosti (v): součet čtverců nad úhlopříčkami $x + y$, $x - y$ rovnoběžníka se stranami x , y je roven součtu čtverců nad jeho stranami (namalujte si obrázek). Proto se o rovnosti (v) někdy mluví jako o *zákonu rovnoběžníka*.

Poznamenejme, že skalární součin je možno vyjádřit pomocí normy (viz 24.13 a 24.26). Jestliže $T = \mathbb{C}$, potom je

$$(x|y) = \frac{1}{4} \cdot (\|x + y\|^2 - \|x - y\|^2 + i \cdot \|x + iy\|^2 - i \cdot \|x - iy\|^2),$$

je-li $T = \mathbb{R}$, pak je

$$(x|y) = \frac{1}{4} \cdot (\|x + y\|^2 - \|x - y\|^2).$$

26.6. Cauchyova-Schwarzova nerovnost. *Pro každé dva vektory x, y unitárního prostoru platí nerovnost*

$$|(x|y)| \leq \|x\| \cdot \|y\|.$$

Rovnost nastane právě tehdy, když jsou vektory x, y lineárně závislé.

Důkaz. Jestliže je $y = o$, je levá i pravá strana v uvedené nerovnosti rovna nule, tj. platí dokonce rovnost. Předpokládejme, že y je nenulový vektor, a položíme

$$a = \frac{(x|y)}{\|y\|^2}.$$

Podle 26.1 a 26.2 dostáváme:

$$\begin{aligned} 0 \leq (x - ay|x - ay) &= (x|x) - a \cdot (y|x) - \bar{a} \cdot (x|y) + a \cdot \bar{a} \cdot (y|y) = \\ &= \|x\|^2 - a \cdot \overline{(x|y)} - \bar{a} \cdot (x|y) + a \cdot \bar{a} \cdot \|y\|^2. \end{aligned}$$

Po dosazení za a a po vynásobení kladným reálným číslem $\|y\|^2$ dostaneme nerovnost

$$0 \leq \|x\|^2 \cdot \|y\|^2 - (x|y) \cdot \overline{(x|y)} - \overline{(x|y)} \cdot (x|y) + (x|y) \cdot \overline{(x|y)}.$$

Odtud

$$(x|y) \cdot \overline{(x|y)} \leq \|x\|^2 \cdot \|y\|^2,$$

tj.

$$|(x|y)|^2 \leq \|x\|^2 \cdot \|y\|^2.$$

Odmocněním získáme požadovanou rovnost.

Jestliže jsou vektory x, y nezávislé, pak je $x - ay$ nenulový vektor a v předchozím platí všude ostrá nerovnost. Jestliže jsou naopak vektory x, y závislé, tj. např. $x = by$ pro nějaké číslo $b \in T$, potom je

$$|(x|y)| = |(by|y)| = |b| \cdot \|y\| \cdot \|y\| = \|x\| \cdot \|y\|. \quad \square$$

Místo termínu Cauchyova–Schwarzova nerovnost bývají též užívány termíny Cauchyova–Bunjakovského nerovnost, Schwarzova nerovnost apod.

26.7. Důsledky. Pro libovolné dva vektory $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ prostoru T^n platí nerovnost

$$\left| \sum_{k=1}^n x_k \bar{y}_k \right| \leq \sqrt{\sum_{k=1}^n |x_k|^2} \cdot \sqrt{\sum_{k=1}^n |y_k|^2}.$$

Pro libovolné dvě reálné funkce f, g , které jsou spojité na intervalu $\langle a, b \rangle$, platí nerovnost

$$\left| \int_a^b f(x)g(x)dx \right| \leq \sqrt{\int_a^b f(x)^2 dx} \cdot \sqrt{\int_a^b g(x)^2 dx}.$$

Pro libovolné dvě komplexní funkce f, g reálné proměnné, které jsou spojité na intervalu $\langle a, b \rangle$, platí nerovnost

$$\left| \int_a^b f(x)\overline{g(x)} dx \right| \leq \sqrt{\int_a^b |f(x)|^2 dx} \cdot \sqrt{\int_a^b |g(x)|^2 dx}.$$

Pro libovolné dvě matice $A, B \in T^{n \times n}$ je

$$\left| \sum_{j,k=1}^n a_{kj} \bar{b}_{kj} \right| \leq \sqrt{\sum_{j,k=1}^n |a_{kj}|^2} \cdot \sqrt{\sum_{j,k=1}^n |b_{kj}|^2} . \quad \square$$

Nerovnosti uvedené v 26.7 jsou speciálními případy Cauchyovy–Schwarzovy nerovnosti (viz příklady 26.3). Uvádějí se většinou umocněné na druhou.

26.8. Trojúhelníková nerovnost. Pro každé dva vektory x, y unitárního prostoru platí nerovnost

$$\|x + y\| \leq \|x\| + \|y\| .$$

Důkaz. Z definice normy a z vlastností skalárního součinu plyne:

$$\|x + y\|^2 = (x + y|x + y) = (x|x) + (x|y) + (y|x) + (y|y) = \|x\|^2 + 2 \cdot \operatorname{Re}(x|y) + \|y\|^2 ,$$

neboť součet komplexně sdružených čísel je roven dvojnásobku jejich společné reálné části. Podle Cauchyovy–Schwarzovy nerovnosti je však

$$\operatorname{Re}(x|y) \leq |(x|y)| \leq \|x\| \cdot \|y\| ,$$

takže

$$\|x + y\|^2 \leq \|x\|^2 + 2 \cdot \|x\| \cdot \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$$

a po odmocnění dostáváme požadovaný výsledek. \square

26.9. Důsledky. Pro libovolné dva vektory $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ prostoru T^n platí nerovnost

$$\sqrt{\sum_{k=1}^n |x_k + y_k|^2} \leq \sqrt{\sum_{k=1}^n |x_k|^2} + \sqrt{\sum_{k=1}^n |y_k|^2} .$$

Pro libovolné dvě reálné funkce f, g , které jsou spojité na intervalu $\langle a, b \rangle$, platí nerovnost

$$\sqrt{\int_a^b (f(x) + g(x))^2 dx} \leq \sqrt{\int_a^b f(x)^2 dx} + \sqrt{\int_a^b g(x)^2 dx} .$$

Pro libovolné dvě komplexní funkce f, g reálné proměnné, které jsou spojité na intervalu $\langle a, b \rangle$, platí nerovnost

$$\sqrt{\int_a^b |f(x) + g(x)|^2 dx} \leq \sqrt{\int_a^b |f(x)|^2 dx} + \sqrt{\int_a^b |g(x)|^2 dx} .$$

Pro libovolné dvě matice $A, B \in T^{n \times n}$ je

$$\sqrt{\sum_{j,k=1}^n |a_{kj} + b_{kj}|^2} \leq \sqrt{\sum_{j,k=1}^n |a_{kj}|^2} + \sqrt{\sum_{j,k=1}^n |b_{kj}|^2} . \quad \square$$

Nerovnosti uvedené v 26.9 jsou speciálními případy trojúhelníkové nerovnosti (viz příklady 26.3).

26.10. Definice. Necht' V je unitární prostor. Řekneme, že vektory $x, y \in V$ jsou *navzájem ortogonální* (resp. *kolmé*), jestliže je jejich skalární součin roven nule. Podmnožina M prostoru V se nazývá *ortogonální*, jestliže jsou každé dva její různé vektory navzájem ortogonální. Podmnožina M prostoru V se nazývá *ortonormální*, jestliže je ortogonální a každý její vektor je normovaný. *Ortogonální*, resp. *ortonormální bázi* unitárního prostoru budeme rozumět každou bázi tohoto prostoru, která je ortogonální, resp. ortonormální množinou.

Poznamenejme, že nulový vektor je kolmý ke každému vektoru prostoru V a žádný jiný vektor tuto vlastnost nemá. Nulový vektor je rovněž jediným vektorem, který je kolmý sám k sobě. Prázdná množina je podle definice 26.10 ortogonální i ortonormální.

26.11. Příklady.

(i) Dva jednotkové vektory v rovině, které jsou na sebe kolmé (v geometrickém slova smyslu), tvoří ortonormální bázi. Rovněž tři jednotkové vektory v prostoru, které jsou navzájem kolmé, tvoří ortonormální bázi (viz příklad 26.3(i)).

(ii) Kanonická báze prostoru T^n je ortonormální bázi unitárního prostoru T^n se standardním skalárním součinem (viz 26.3(ii)).

V prostoru \mathbb{R}^3 se standardním skalárním součinem

$$(x|y) = x_1y_1 + x_2y_2 + x_3y_3$$

jsou vektory $(1, 2, 3)$ a $(1, 1, -1)$ navzájem ortogonální, skalární součin vektorů $(2, 3, -2)$ a $(1, -1, 3)$ je -7 , takže tyto vektory ortogonální nejsou. Ortogonálními bázemi tohoto prostoru jsou např. báze

$$\{(2, 2, -1), (2, -1, 2), (-1, 2, 2)\} \quad \text{a} \quad \{(1, 1, 1), (1, 0, -1), (1, -2, 1)\},$$

ortonormálními bázemi z nich odvozenými (normujeme vektory) jsou báze

$$\left\{ \frac{1}{3} \cdot (2, 2, -1), \frac{1}{3} \cdot (2, -1, 2), \frac{1}{3} \cdot (-1, 2, 2) \right\},$$

$$\left\{ \frac{1}{\sqrt{3}} \cdot (1, 1, 1), \frac{1}{\sqrt{2}} \cdot (1, 0, -1), \frac{1}{\sqrt{6}} \cdot (1, -2, 1) \right\}.$$

V prostoru \mathbb{C}^3 se standardním skalárním součinem je ortogonální bázi např. báze $\{(2, i, i), (1, -i, -i), (0, 1, -1)\}$; z ní můžeme snadno získat ortonormální bázi

$$\left\{ \frac{1}{\sqrt{6}} \cdot (2, i, i), \frac{1}{\sqrt{3}} \cdot (1, -i, -i), \frac{1}{\sqrt{2}} \cdot (0, 1, -1) \right\}.$$

(iii) V prostoru všech polynomů nejvýše třetího stupně (s reálnými koeficienty) se skalárním součinem definovaným rovností

$$(p|q) = \int_{-1}^1 p(x)q(x) dx$$

je $\{1, x, x^2 - \frac{1}{3}, x^3 - \frac{3}{5}x\}$ ortogonální báze (viz 26.3(iii)).

(iv) V prostoru $T^{n \times n}$ čtvercových matic řádu n se skalárním součinem

$$(A|B) = \text{tr}(A \cdot \overline{B}^T)$$

tvorí ortonormální bázi n^2 matic, které mají pouze na jediném místě jedničku a na ostatních místech nuly. Tato báze odpovídá kanonické bázi prostoru T^{n^2} se standardním skalárním součinem. Viz 26.3(iv).

(v) V prostoru \mathbb{R}^3 se skalárním součinem definovaným rovností

$$(x|y) = x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_2 + x_3y_3$$

(viz 26.3(v)) je ortonormální bázi např. báze $\{(1, 0, 0), (0, 0, 1), (1, -1, 0)\}$.

26.12. Pythagorova věta. *Jsou-li x, y navzájem ortogonální vektory unitárního prostoru, potom je*

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

Důkaz. Zřejmě je

$$\|x + y\|^2 = (x + y|x + y) = (x|x) + (x|y) + (y|x) + (y|y) = \|x\|^2 + \|y\|^2,$$

neboť vektory x, y jsou navzájem ortogonální. \square

26.13. Věta. *Ortogonalní podmnožina unitárního prostoru, která neobsahuje nulový vektor, je lineárně nezávislá.*

Důkaz. Nechť M je ortogonální podmnožina unitárního prostoru V , která neobsahuje nulový vektor. Jestliže

$$a_1v_1 + a_2v_2 + \dots + a_nv_n = 0,$$

kde v_1, \dots, v_n jsou navzájem různé vektory množiny M a $a_1, \dots, a_n \in T$, potom pro každé $j = 1, \dots, n$ je

$$0 = \left(\sum_{k=1}^n a_k v_k \mid v_j \right) = \sum_{k=1}^n a_k \cdot (v_k \mid v_j) = a_j \cdot \|v_j\|^2.$$

Protože množina M neobsahuje nulový vektor, je $\|v_j\|^2 \neq 0$ a tedy $a_j = 0$. Proto je množina M lineárně nezávislá. \square

Zatímco ortogonální množina může obsahovat nulový vektor, množina ortonormální ho obsahovat nemůže (viz definice 26.10). Každá ortonormální množina je tedy podle předešlého lineárně nezávislá. Poznamenejme ještě, že z každé ortogonální podmnožiny neobsahující nulový vektor můžeme normováním vektorů vytvořit množinu ortonormální (viz příklad 26.11(ii)).

ze které je možno při daných vektorech w_1, \dots, w_m vypočítat všechny vektory $x \in W^\perp$. Podprostor W^\perp je tedy tvořen všemi řešeními výše uvedené homogenní soustavy lineárních rovnic a je tedy

$$\dim W^\perp = n - \dim W ,$$

tj. podprostor W^\perp je direktním doplňkem podprostoru W v prostoru T^n . Tato skutečnost platí obecněji, v případě, že podprostor W je konečně dimenzionálním podprostorem jakéhokoli unitárního prostoru (viz dále 26.21).

V následující větě se poprvé v této kapitole objevuje předpoklad konečné dimenze.

26.17. Věta. *Každý unitární prostor konečné dimenze má ortonormální bázi.*

Důkaz. Na začátku této kapitoly (viz poznámka za 26.2) jsme si uvědomili, že skalární součin na reálném, resp. komplexním vektorovém prostoru V je symetrická pozitivně definitní bilineární forma, resp. hermitovská pozitivně definitní seskvilineární forma. V části věnované formám jsme dokázali, že k takovéto formě f existuje báze N prostoru V , která je vůči ní normální (viz 25.3). Vzhledem k tomu, že forma f je — jako skalární součin — pozitivně definitní, je matice formy f vzhledem k bázi N jednotková. Protože v matici formy f vzhledem k bázi N stojí na místě ij hodnota formy f v i -tém a j -tém vektoru báze N , tj. skalární součin těchto dvou vektorů, je báze N ortonormální bázi unitárního prostoru V . \square

Důkaz věty 26.17 dává zcela konkrétní návod, jak najít ortonormální bázi unitárního prostoru konečné dimenze (viz následující příklad). Později poznáme další způsob nalezení ortonormální báze (viz 26.27).

26.18. Příklad.

(i) Dokážeme, že rovnost

$$(x|y) = 2x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2 ,$$

kde $x = (x_1, x_2)$, $y = (y_1, y_2)$, definuje na vektorovém prostoru \mathbb{R}^2 skalární součin, a najdeme ortonormální bázi tohoto unitárního prostoru.

Matici dané bilineární formy převedeme symetrickými úpravami na matici diagonální; současně budeme sledovat prováděné řádkové úpravy:

$$\begin{aligned} \left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) &\rightsquigarrow \left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 0 & -1 & 1 & -2 \end{array} \right) &\rightsquigarrow \left(\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 0 & 2 & 1 & -2 \end{array} \right) &\rightsquigarrow \\ &\rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 1 & \frac{1}{\sqrt{2}} & \frac{-2}{\sqrt{2}} \end{array} \right) \end{aligned}$$

První řádek jsme přičetli k (-2) -násobku druhého, první sloupec k (-2) -násobku druhého, potom jsme oba řádky a oba sloupce vynásobili číslem $\frac{1}{\sqrt{2}}$. Levá část výsledné matice je jednotková matice a proto skutečně jde o skalární součin. V rádcích pravé části výsledné matice je nalezená ortonormální báze:

$$\left\{ \left(\frac{1}{\sqrt{2}}, 0 \right), \left(\frac{1}{\sqrt{2}}, \frac{-2}{\sqrt{2}} \right) \right\}$$

Jinou úpravou můžeme dojít k jiné ortonormální bázi. Např. odečtením druhého řádku od prvního a odečtením druhého sloupce od prvního, tj.

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & 1 & -1 \\ 1 & 1 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{array} \right),$$

dostáváme ortonormální bázi $\{(1, -1), (0, 1)\}$.

(ii) Dokážeme, že rovnost

$$(x|y) = x_1\bar{y}_1 - ix_1\bar{y}_2 + (1+i)x_1\bar{y}_3 + ix_2\bar{y}_1 + 3x_2\bar{y}_2 + (1-i)x_3\bar{y}_1 + 4x_3\bar{y}_3,$$

kde $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$, definuje na vektorovém prostoru \mathbb{C}^3 skalární součin, a najdeme ortonormální bázi tohoto unitárního prostoru.

Matici dané seskvilineární formy převedeme hermitovskými úpravami na matici diagonální; současně budeme sledovat prováděné řádkové úpravy:

$$\begin{aligned} & \left(\begin{array}{ccc|ccc} 1 & -i & 1+i & 1 & 0 & 0 \\ i & 3 & 0 & 0 & 1 & 0 \\ 1-i & 0 & 4 & 0 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & -i & 1+i & 1 & 0 & 0 \\ 0 & 2 & 1-i & -i & 1 & 0 \\ 0 & 1+i & 2 & -1+i & 0 & 1 \end{array} \right) \rightsquigarrow \\ & \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 1-i & -i & 1 & 0 \\ 0 & 1+i & 2 & -1+i & 0 & 1 \end{array} \right) \rightsquigarrow \\ & \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 1-i & -i & 1 & 0 \\ 0 & 0 & 2 & -3+3i & -1-i & 2 \end{array} \right) \rightsquigarrow \\ & \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -i & 1 & 0 \\ 0 & 0 & 4 & -3+3i & -1-i & 2 \end{array} \right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & \frac{-i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 & \frac{-3+3i}{2} & \frac{-1-i}{2} & 1 \end{array} \right) \end{aligned}$$

Ke druhému řádku jsme přičetli $(-i)$ -násobek a ke třetímu řádku $(-1+i)$ -násobek prvního řádku. Potom jsme ke druhému sloupci přičetli i -násobek a ke třetímu $(-1-i)$ -násobek prvního sloupce. K dvojnásobku třetího řádku jsme přičetli $(-1-i)$ -násobek druhého řádku a k dvojnásobku třetího sloupce $(-1+i)$ -násobek

druhého sloupce. Druhý řádek a druhý sloupec jsme vynásobili $\frac{1}{\sqrt{2}}$, třetí řádek a třetí sloupec jsme vynásobili $\frac{1}{2}$. Protože je levá část výsledné matice jednotkovou maticí, jde opravdu o skalární součin. V řádcích pravé části výsledné matice je nalezená ortonormální báze:

$$\left\{ (1, 0, 0), \frac{1}{\sqrt{2}}(-i, 1, 0), \frac{1}{2}(-3 + 3i, -1 - i, 2) \right\}$$

26.19. Lemma. *Nechť $\{w_1, \dots, w_m\}$, kde $m \geq 1$, je ortogonální podmnožina unitárního prostoru V , která neobsahuje nulový vektor. Potom ke každému vektoru $v \in V$ existují jednoznačně určená čísla $c_1, \dots, c_m \in T$ taková, že vektor*

$$v - c_1 w_1 - c_2 w_2 - \dots - c_m w_m$$

je kolmý k podprostoru $[w_1, \dots, w_m]$.

Důkaz. Vektor $v - c_1 w_1 - c_2 w_2 - \dots - c_m w_m$ je kolmý k podprostoru $[w_1, \dots, w_m]$ právě tehdy, když pro každé $j = 1, \dots, m$ je skalární součin

$$(v - c_1 w_1 - c_2 w_2 - \dots - c_m w_m | w_j) = (v | w_j) - c_j \cdot (w_j | w_j)$$

roven nule. To však nastane právě tehdy, když pro každé $j = 1, \dots, m$ je

$$c_j = \frac{(v | w_j)}{\|w_j\|^2}.$$

Čísla c_1, \dots, c_m s výše uvedenou vlastností tedy existují a jsou určena jednoznačně. \square

Povšimněme si, že každé z čísel c_1, \dots, c_m závisí pouze na vektoru v a jediném vektoru z ortogonální množiny $\{w_1, \dots, w_m\}$.

26.20. Definice. Nechť $\{w_1, \dots, w_m\}$, kde $m \geq 1$, je ortogonální podmnožina unitárního prostoru V , která neobsahuje nulový vektor. *Fourierovými koeficienty* vektoru $v \in V$ vůči ortogonální množině $\{w_1, \dots, w_m\}$ budeme rozumět čísla

$$c_j = \frac{(v | w_j)}{\|w_j\|^2}, \quad j = 1, \dots, m.$$

Uvědomme si ještě jednou, že j -tý Fourierův koeficient vektoru v vůči ortogonální množině $\{w_1, \dots, w_m\}$ je Fourierovým koeficientem vektoru v vůči jednorvkové množině $\{w_j\}$. Je-li vektor w_j normovaný, je příslušný Fourierův koeficient roven číslu $(v | w_j)$.

26.21. Věta o ortogonálním rozkladu. *Nechť W je podprostor konečné dimenze unitárního prostoru V . Potom je $V = W \oplus W^\perp$, tj. ke každému vektoru $v \in V$ existují jednoznačně určené vektory $v^p \in W$ a $v^\perp \in W^\perp$, pro které je $v = v^p + v^\perp$.*

Důkaz. Nechť $\{w_1, \dots, w_m\}$ je ortonormální báze podprostoru W (existuje podle věty 26.17) a $v \in V$ libovolně zvolený vektor. Podle lemmatu 26.19 existují koeficienty c_1, \dots, c_m takové, že pro vektor

$$v^p = c_1 w_1 + \dots + c_m w_m$$

je $v - v^p = v^\perp \in W^\perp$. Tedy $V = W + W^\perp$. Rovnost $W \cap W^\perp = O$ byla dokázána v 26.16. Viz též věta 9.2. \square

Rovnost $v = v^p + v^\perp$ někdy nazýváme *ortogonálním rozkladem* vektoru v určeným podprostorem W . V unitárním prostoru V konečné dimenze je tedy (viz poznámka za 26.16)

$$\dim W^\perp = \dim V - \dim W .$$

26.22. Definice. Nechť W je konečně dimenzionální podprostor unitárního prostoru V . *Ortogonální projekcí* vektoru $v \in V$ na podprostor W budeme rozumět jednoznačně určený vektor $v^p \in W$, pro který je $v = v^p + v^\perp$, kde $v^\perp \in W^\perp$.

Ve větě 26.21 je dokázána existence a jednoznačnost ortogonální projekce vektoru $v \in V$ na konečně dimenzionální podprostor W prostoru V . Zvolíme-li v podprostoru W nějakou ortogonální bázi $\{w_1, \dots, w_m\}$, potom ortogonální projekci vektoru v na podprostor W je vektor $v^p = c_1 w_1 + \dots + c_m w_m$, kde c_1, \dots, c_m jsou Fourierovy koeficienty vektoru v vůči ortogonální množině $\{w_1, \dots, w_m\}$. Ortogonální projekci v^p vektoru v tedy navíc umíme určit souřadnicemi vzhledem k libovolné ortogonální bázi podprostoru W . Později najdeme souřadnice ortogonální projekce v^p vektoru v vzhledem k libovolné bázi podprostoru W .

Povšimněme si ještě, že při důkazu Cauchyovy–Schwarzovy nerovnosti 26.6 jsme vlastně užili Fourierův koeficient $a = \frac{(x|y)}{\|y\|^2}$ vektoru x vůči množině $\{y\}$. Místo podmínky pro nezápornost normy $\|x - ay\|$ je možno užít Pythagorovu větu. Podle lemmatu 26.19 jsou totiž vektory ay a $x - ay$ kolmé, takže podle Pythagorovy věty 26.12 je

$$\|x\|^2 = \|ay + x - ay\|^2 = \|ay\|^2 + \|x - ay\|^2 \geq |a|^2 \cdot \|y\|^2$$

a po dosazení za a a jednoduché úpravě dostáváme Cauchyovu–Schwarzovu nerovnost

$$\|x\|^2 \cdot \|y\|^2 \geq |(x|y)|^2 .$$

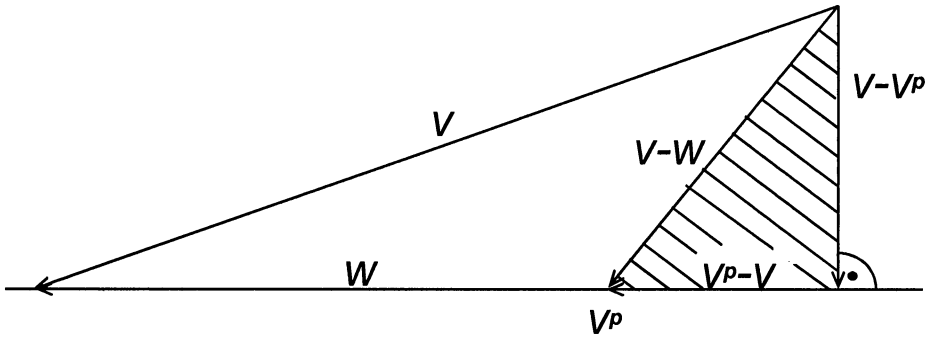
26.23. Věta o aproximaci. *Nechť W je konečně dimenzionální podprostor unitárního prostoru V . Ortogonální projekce v^p vektoru $v \in V$ na podprostor W je nejlepší aproximací tohoto vektoru v podprostoru W , tj. norma vektoru $v - v^p$ je menší než norma vektoru $v - w$ pro každé $w \in W$, $w \neq v^p$:*

$$\forall w \in W \quad w \neq v^p \quad \|v - v^p\| < \|v - w\|$$

Důkaz. Jestliže je $w \in W$ a $w \neq v^p$, pak je $0 \neq v^p - w \in W$ a vektory $v - v^p$ a $v^p - w$ jsou podle věty 26.21 navzájem ortogonální. Podle Pythagorovy věty je

$$\|v - w\|^2 = \|v - v^p\|^2 + \|v^p - w\|^2 > \|v - v^p\|^2 .$$

Situace je znázorněna na obrázku, Pythagorovu větu užíváme pro vyšrafovaný trojúhelník. \square



26.24. Besselova nerovnost. *Jestliže $\{w_1, \dots, w_m\}$ je ortonormální podmnožina unitárního prostoru V a c_1, \dots, c_m Fourierovy koeficienty vektoru $v \in V$ vůči této množině, potom je*

$$\|v\|^2 \geq \sum_{k=1}^m |c_k|^2 .$$

Důkaz. Označme symbolem v^p ortogonální projekci vektoru $v \in V$ na podprostor $[w_1, \dots, w_m]$. Podle Pythagorovy věty je

$$\|v\|^2 = \|v^p\|^2 + \|v - v^p\|^2 \geq \|v^p\|^2 .$$

Podle 26.19 – 26.22 je

$$\|v^p\|^2 = \left(\sum_{j=1}^m c_j w_j \mid \sum_{k=1}^m c_k w_k \right) = \sum_{j,k=1}^m c_j \bar{c}_k (w_j \mid w_k) = \sum_{k=1}^m c_k \bar{c}_k = \sum_{k=1}^m |c_k|^2 .$$

Tím je tvrzení dokázáno. \square

Besselova nerovnost tak umožňuje odhadnout normu vektoru pomocí jeho Fourierových koeficientů vůči libovolné konečné ortonormální podmnožině.

26.25. Trigonometrické polynomy. Uvažujme prostor V reálných funkcí, které jsou spojité na intervalu $\langle 0, 2\pi \rangle$, se skalárním součinem definovaným rovností

$$(f|g) = \int_0^{2\pi} f(x)g(x) dx .$$

Pro každé přirozené číslo n označme symbolem V_n podprostor prostoru V generovaný funkcemi

$$1, \cos x, \sin x, \cos 2x, \sin 2x, \dots, \cos nx, \sin nx ;$$

prvky tohoto prostoru (tj. lineární kombinace uvedených $2n+1$ funkcí) se nazývají *trigonometrické polynomy* nejvýše n -tého stupně. Uvedené funkce tvoří ortogonální bázi prostoru V_n , neboť

$$(\cos kx | \cos mx) = \int_0^{2\pi} \cos kx \cos mx dx = 0, \quad k, m = 0, 1, 2, \dots, k \neq m$$

$$(\sin kx | \sin mx) = \int_0^{2\pi} \sin kx \sin mx dx = 0, \quad k, m = 1, 2, \dots, k \neq m$$

$$(\sin kx | \cos mx) = \int_0^{2\pi} \sin kx \cos mx dx = 0, \quad k = 1, 2, \dots, m = 0, 1, 2, \dots .$$

Podprostor V_n má tedy dimenzi $2n+1$. Dále je

$$\|1\|^2 = \int_0^{2\pi} dx = 2\pi ,$$

$$\|\cos kx\|^2 = \int_0^{2\pi} \cos^2 kx dx = \pi, \quad k = 1, 2, \dots ,$$

$$\|\sin kx\|^2 = \int_0^{2\pi} \sin^2 kx dx = \pi, \quad k = 1, 2, \dots .$$

Množina funkcí

$$\frac{1}{\sqrt{2\pi}}, \frac{1}{\sqrt{\pi}} \cos x, \frac{1}{\sqrt{\pi}} \sin x, \dots, \frac{1}{\sqrt{\pi}} \cos nx, \frac{1}{\sqrt{\pi}} \sin nx$$

je tedy ortonormální bázi prostoru V_n .

Fourierovy koeficienty $c_0, c_1, c_2, \dots, c_{2n-1}, c_{2n}$ vůči množině

$$\{1, \cos x, \sin x, \cos 2x, \sin 2x, \dots, \cos nx, \sin nx\}$$

jsou

$$c_0 = \frac{1}{2\pi} \int_0^{2\pi} f(x) dx ,$$

$$c_1 = \frac{1}{\pi} \int_0^{2\pi} f(x) \cos x \, dx, \quad c_2 = \frac{1}{\pi} \int_0^{2\pi} f(x) \sin x \, dx,$$

$$c_{2n-1} = \frac{1}{\pi} \int_0^{2\pi} f(x) \cos nx \, dx, \quad c_{2n} = \frac{1}{\pi} \int_0^{2\pi} f(x) \sin nx \, dx.$$

Trigonometrický polynom

$$p(x) = c_0 + c_1 \cos x + c_2 \sin x + \dots + c_{2n-1} \cos nx + c_{2n} \sin nx$$

je podle věty 26.23 nejlepší aproximací funkce f v prostoru trigonometrických polynomů n -tého stupně.

26.26. Věta. *Každou ortonormální podmnožinu unitárního prostoru konečné dimenze je možno rozšířit na ortonormální bázi celého prostoru.*

Důkaz. Necht $\{w_1, \dots, w_k\}$ je ortonormální podmnožina unitárního prostoru V dimenze n ; pišme $W = [w_1, \dots, w_k]$. Jestliže je $k < n$, pak nutně existuje vektor $v \in V \setminus W$; označme v^p jeho projekci na podprostor W . Vektor $v^\perp = v - v^p \in W^\perp$ je nenulový, neboť $v \notin W$; symbolem w_{k+1} označíme vektor vzniklý normováním vektoru v^\perp . Množina $\{w_1, \dots, w_k, w_{k+1}\}$ je tedy ortonormální. Pokud je $k+1 < n$, pokračujeme stejným způsobem. Po $n - k$ krocích dospějeme k ortonormální bázi $\{w_1, \dots, w_n\}$ prostoru V . \square

Z předchozí věty vyplývá, že každý unitární prostor konečné dimenze má ortonormální bázi. Tento fakt jsme však již dokázali ve větě 26.17.

Metoda konstrukce ortonormální báze popsaná ve větě 26.26 dovoluje rozšířit libovolnou ortonormální podmnožinu na ortonormální bázi. Navíc má tato metoda jasný geometrický smysl (konstrukce vektoru $v^\perp = v - v^p$).

V následujícím odstavci budeme výše uvedený postup mírně modifikovat; popíšeme tzv. *Gramův-Schmidtův ortogonalizační proces*, který slouží k získání ortogonální (resp. ortonormální) báze unitárního prostoru konečné dimenze. Při popisu ortogonálních projekcí se zde objevují Fourierovy koeficienty.

26.27. Gramův-Schmidtův ortogonalizační proces. *Necht $\{w_1, \dots, w_n\}$ je báze unitárního prostoru V . Jestliže*

$$v_1 = w_1,$$

$$v_2 = w_2 - \frac{(w_2|v_1)}{\|v_1\|^2} \cdot v_1,$$

$$v_3 = w_3 - \frac{(w_3|v_1)}{\|v_1\|^2} \cdot v_1 - \frac{(w_3|v_2)}{\|v_2\|^2} \cdot v_2,$$

.....

$$v_n = w_n - \frac{(w_n|v_1)}{\|v_1\|^2} \cdot v_1 - \frac{(w_n|v_2)}{\|v_2\|^2} \cdot v_2 - \dots - \frac{(w_n|v_{n-1})}{\|v_{n-1}\|^2} \cdot v_{n-1},$$

potom $\{v_1, \dots, v_n\}$ je ortogonální báze prostoru V .

Důkaz. Pro každé $j = 2, \dots, n$ je $v_j = w_j - w_j^p$, kde w_j^p je ortogonální projekce vektoru w_j na podprostor $[v_1, \dots, v_{j-1}]$. Proto tvoří vektory v_1, \dots, v_n ortogonální množinu. Vzhledem k tomu, že každý z vektorů w_1, \dots, w_n je možno vyjádřit jako lineární kombinaci vektorů v_1, \dots, v_n (viz výše uvedené rovnosti), je $\{v_1, \dots, v_n\}$ množinou generátorů a tedy i bází prostoru V . \square

26.28. Legendreovy polynomy. Uvažujme unitární prostor V všech polynomů stupně nejvýše n na intervalu $\langle -1, 1 \rangle$ se skalárním součinem

$$(p|q) = \int_{-1}^1 p(x)q(x) dx .$$

Provedeme-li Gramův–Schmidtův ortogonalizační proces na bázi $\{1, x, x^2, \dots, x^n\}$, dostaneme polynomy

$$1, \quad x, \quad x^2 - \frac{1}{3}, \quad x^3 - \frac{3}{5}x, \quad \dots .$$

Až na koeficienty jde o polynomy

$$\frac{1}{2^k \cdot k!} \cdot [(x^2 - 1)^k]^{(k)}, \quad k = 0, 1, \dots, n ,$$

kteří se nazývají *Legendreovy*. Po normování dostaneme tzv. *normované Legendreovy polynomy*

$$p_0(x) = \frac{1}{\sqrt{2}}, \quad p_1(x) = \sqrt{\frac{3}{2}} \cdot x, \quad p_2(x) = \frac{3}{2} \cdot \sqrt{\frac{5}{2}} \cdot \left(x^2 - \frac{1}{3}\right), \quad \dots ,$$

kteří tvoří ortonormální bázi prostoru V . Pro každý polynom q stupně nejvýše n je tedy

$$q = c_0 p_0 + c_1 p_1 + \dots + c_n p_n ,$$

kde pro každé $j = 0, 1, \dots, n$ je podle 26.19

$$c_j = \int_{-1}^1 q(x)p_j(x) dx .$$

Jestliže V je unitární prostor, který má ortonormální bázi, potom se skalární součin a norma vektorů snadno vyjádří pomocí souřadnic těchto vektorů vzhledem k uvažované ortonormální bázi. Souřadnice vektorů vzhledem k této bázi se opět snadno vyjádří pomocí skalárního součinu.

26.29. Věta. *Nechť V je unitární prostor a $\{v_\alpha; \alpha \in \Lambda\}$ jeho ortonormální báze. Potom platí:*

- (i) *Pro každý vektor $x \in V$ je $x = \sum_{\alpha \in \Lambda} (x|v_\alpha) \cdot v_\alpha$.*
- (ii) *Pro každé dva vektory $x, y \in V$ je $(x|y) = \sum_{\alpha \in \Lambda} (x|v_\alpha) \cdot \overline{(y|v_\alpha)}$.*
- (iii) *Pro každý vektor $x \in V$ je $\|x\|^2 = \sum_{\alpha \in \Lambda} |(x|v_\alpha)|^2$.*

Důkaz. Pišme

$$x = \sum_{\alpha \in \Lambda} x_\alpha v_\alpha, \quad y = \sum_{\alpha \in \Lambda} y_\alpha v_\alpha;$$

připomeňme, že v těchto součtech jsou skoro všechna čísla x_α rovna nule a rovněž skoro všechna čísla y_α rovna nule. Pro každé pevně zvolené $\alpha \in \Lambda$ je

$$(x|v_\alpha) = \left(\sum_{\beta \in \Lambda} x_\beta v_\beta | v_\alpha \right) = \sum_{\beta \in \Lambda} x_\beta (v_\beta | v_\alpha) = x_\alpha,$$

takže tvrzení (i) platí. Dále je

$$\begin{aligned} (x|y) &= \left(\sum_{\beta \in \Lambda} x_\beta v_\beta | \sum_{\alpha \in \Lambda} y_\alpha v_\alpha \right) = \sum_{\beta \in \Lambda} \sum_{\alpha \in \Lambda} x_\beta \overline{y_\alpha} (v_\beta | v_\alpha) = \\ &= \sum_{\alpha \in \Lambda} x_\alpha \overline{y_\alpha} = \sum_{\alpha \in \Lambda} (x|v_\alpha) \cdot \overline{(y|v_\alpha)}. \end{aligned}$$

Nakonec je podle tvrzení (ii)

$$\|x\|^2 = (x|x) = \sum_{\alpha \in \Lambda} (x|v_\alpha) \cdot \overline{(x|v_\alpha)} = \sum_{\alpha \in \Lambda} |(x|v_\alpha)|^2. \quad \square$$

Uvědomme si, že α -tá souřadnice vektoru x vzhledem k ortonormální bázi je příslušným Fourierovým koeficientem; proto se rovnosti uvedené v tvrzení (i) někdy říká *Fourierův rozvoj* vektoru x vzhledem k ortonormální bázi $\{v_\alpha; \alpha \in \Lambda\}$.

Tvrzení (ii) říká, že skalární součin vektorů x, y se pomocí jejich souřadnic vzhledem k ortonormální bázi vypočte stejným způsobem, jako se počítá skalární součin v příkladu 26.3(ii). Rovnostem uvedeným v tvrzeních (ii) a (iii) se někdy říká *Parsevalova rovnost*.

Srovnajte tvrzení 26.24 a 26.29(iii) i jejich důkazy; ve větě 26.24 máme pouze ortonormální podmnožinu (nikoli bázi) unitárního prostoru.

26.30. Poznámka. Nechť V je vektorový prostor nad tělesem T . Skalární součin na prostoru V můžeme zavést také takto. Zvolíme nějakou bázi N prostoru V a definujeme skalární součin vektorů $x, y \in V$ rovností

$$(x|y) = \sum_{\alpha \in \Lambda} x_\alpha \overline{y_\alpha},$$

kde x_α , resp. y_α je α -tá souřadnice vektoru x , resp. y vzhledem k bázi N , tj.

$$\langle x \rangle_N = (x_\alpha)_{\alpha \in \Lambda}, \quad \langle y \rangle_N = (y_\alpha)_{\alpha \in \Lambda}$$

(vlastnosti skalárního součinu uvedené v definici 26.1 se snadno ověří).

Báze N je nyní ortonormální bázi takto definovaného unitárního prostoru V ; strukturu unitárního prostoru jsme na vektorovém prostoru V získali vlastně tak, že jsme bázi N prohlásili za ortonormální — skalární součin je potom definován Parsevalovou rovností (srovnej s 26.29).

Definujeme-li takto skalární součin, dostaneme unitární prostor, který má ortonormální bázi. Jestliže je naopak V unitární prostor, který má ortonormální bázi, pak z věty 26.29 vyplývá, že skalární součin může být definován výše uvedeným způsobem, tj. prohlášením nějaké báze za bázi ortonormální.

Jestliže je však V unitární prostor, který ortonormální bázi nemá — a takové unitární prostory existují, potom skalární součin v tomto prostoru nelze definovat výše uvedeným způsobem. Takovéto prostory mají nutně nekonečnou dimenzi (viz 26.17). Vidíme tedy, že unitárních prostorů ve smyslu definice 26.1 je „více“ než unitárních prostorů, jejichž skalární součin je definován způsobem uvedeným na začátku této poznámky. Definice 26.1 dává „navíc“ právě ty unitární prostory, které nemají ortonormální bázi.

Nechť V je reálný unitární prostor. Pro každé dva vektory $x, y \in V$ je podle Cauchyovy–Schwarzovy nerovnosti

$$-||x|| \cdot ||y|| \leq (x|y) \leq ||x|| \cdot ||y|| ;$$

v komplexním prostoru nelze tuto úpravu provést, neboť $(x|y)$ nemusí být reálné číslo. Jsou-li vektory x, y nenulové, je tedy

$$-1 \leq \frac{(x|y)}{||x|| \cdot ||y||} \leq 1 .$$

Toto zjištění dává možnost zavést v reálném unitárním prostoru úhly a jejich velikosti.

26.31. Definice. Nechť x, y jsou nenulové vektory reálného unitárního prostoru. Velikost úhlu φ , který svírají vektory x, y , definujeme pomocí vztahů

$$\cos \varphi = \frac{(x|y)}{||x|| \cdot ||y||}, \quad 0 \leq \varphi \leq \pi .$$

26.32. Kosinová věta. *Nechť x, y jsou nenulové vektory reálného unitárního prostoru. Jestliže vektory x, y svírají úhel φ , potom je*

$$\|x - y\|^2 = \|x\|^2 + \|y\|^2 - 2 \cdot \|x\| \cdot \|y\| \cdot \cos \varphi .$$

Důkaz. Podle definice normy vektoru je

$$\|x - y\|^2 = (x - y | x - y) = (x|x) + (y|y) - 2(x|y) = \|x\|^2 + \|y\|^2 - 2(x|y) .$$

Podle definice úhlu je

$$2 \cdot (x|y) = 2 \cdot \|x\| \cdot \|y\| \cdot \cos \varphi .$$

Odtud plyne rovnost uvedená ve větě. \square

26.33. Příklady. Uvažujme unitární prostor \mathbb{R}^4 se standardním skalárním součinem a jeho podprostor

$$W = [(1, 2, 1, 2), (1, 0, 0, 1)] .$$

Ortogonalním doplňkem podprostoru W v prostoru \mathbb{R}^4 je podprostor všech řešení homogenní soustavy lineárních rovnic s maticí

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix} ,$$

tedy

$$W^\perp = [(2, 1, 0, -2), (0, 1, -2, 0)] .$$

Chceme-li najít ortonormální bázi prostoru \mathbb{R}^4 , jejíž první část je bází podprostoru W a druhá část bází podprostoru W^\perp , můžeme použít Gramův–Schmidtův ortogonalizační proces 26.27, ve kterém figurují Fourierovy koeficienty. Vyjdeme např. z báze

$$\{(1, 0, 0, 1), (1, 2, 1, 2), (1, 0, 0, 0), (0, 1, 0, 0)\} ,$$

jejíž první dva vektory tvoří bázi podprostoru W . Nyní je podle 26.27

$$v_1 = (1, 0, 0, 1) ,$$

$$v_2 = (1, 2, 1, 2) - \frac{3}{2}(1, 0, 0, 1) = \left(-\frac{1}{2}, 2, 1, \frac{1}{2}\right) .$$

Pro zjednodušení dalšího výpočtu vezmeme za vektor v_2 dvojnásobek vypočítaného vektoru; kolmost vektorů k vektoru v_1 zůstane zachována:

$$v_2 = (-1, 4, 2, 1)$$

Dále je

$$v_3 = (1, 0, 0, 0) - \frac{1}{2}(1, 0, 0, 1) - \frac{-1}{22}(-1, 4, 2, 1) .$$

Pro zjednodušení dalšího výpočtu vezmeme 22-násobek tohoto vektoru a pak ho ještě zkrátíme na polovinu:

$$v_3 = (5, 2, 1, -5)$$

Dále je

$$v_4 = (0, 1, 0, 0) - \frac{0}{2}(1, 0, 0, 1) - \frac{4}{22}(-1, 4, 2, 1) - \frac{2}{55}(5, 2, 1, -5) .$$

Nejprve vypočteme 55-násobek tohoto vektoru, pak ho vynásobíme jedenácti a položíme

$$v_4 = (0, 1, -2, 0) .$$

Vypočtené vektory nyní normujeme a tak získáme ortonormální báze podprostorů W a W^\perp :

$$W = \left[\frac{1}{\sqrt{2}}(1, 0, 0, 1), \frac{1}{\sqrt{22}}(-1, 4, 2, 1) \right] ,$$
$$W^\perp = \left[\frac{1}{\sqrt{55}}(5, 2, 1, -5), \frac{1}{\sqrt{5}}(0, 1, -2, 0) \right] .$$

27. UNITÁRNÍ ZOBRAZENÍ

27.1. Definice. Necht U a V jsou unitární prostory nad týmž tělesem T . Zobrazení f prostoru U do prostoru V se nazývá *unitární*, jestliže pro každé dva vektory $x, y \in U$ je

$$(f(x)|f(y)) = (x|y) .$$

Unitární zobrazení je tedy definováno jako zobrazení, které *zachovává skalární součin*.

Necht f je zobrazení unitárního prostoru U do unitárního prostoru V ; jestliže pro každý vektor $x \in U$ je $\|f(x)\| = \|x\|$, pak říkáme, že zobrazení f *zachovává normu*.

27.2. Věta. Necht U a V jsou unitární prostory nad tělesem T a f zobrazení prostoru U do prostoru V . Následující tvrzení jsou ekvivalentní:

- (i) f je unitární,
- (ii) f je monomorfismus zachovávající normu,
- (iii) f je homomorfismus zachovávající normu.

Důkaz. (i) \implies (ii) Necht f je unitární zobrazení. Užitím definice normy, vlastností skalárního součinu a definice unitárního zobrazení dostáváme, že pro libovolně zvolené vektory $x, y \in U$ platí:

$$\begin{aligned} \|f(x+y) - f(x) - f(y)\|^2 &= (f(x+y) - f(x) - f(y) | f(x+y) - f(x) - f(y)) = \\ &= (f(x+y) | f(x+y)) - (f(x+y) | f(x)) - (f(x+y) | f(y)) - (f(x) | f(x+y)) + \\ &+ (f(x) | f(x)) + (f(x) | f(y)) - (f(y) | f(x+y)) + (f(y) | f(x)) + (f(y) | f(y)) = \\ &= (x+y|x+y) - (x+y|x) - (x+y|y) - (x|x+y) + (x|x) + (x|y) - \\ &\quad - (y|x+y) + (y|x) + (y|y) = 0 \end{aligned}$$

Norma vektoru $f(x+y) - f(x) - f(y)$ je rovna nule, proto je

$$f(x+y) = f(x) + f(y) .$$

Podobně je pro vektor $x \in U$ a číslo $a \in T$:

$$\begin{aligned} \|f(ax) - a \cdot f(x)\|^2 &= (f(ax) - a \cdot f(x) | f(ax) - a \cdot f(x)) = \\ &= (f(ax) | f(ax)) - \bar{a} \cdot (f(ax) | f(x)) - a \cdot (f(x) | f(ax)) + a\bar{a} \cdot (f(x) | f(x)) = \\ &= (ax|ax) - \bar{a} \cdot (ax|x) - a \cdot (x|ax) + a\bar{a} \cdot (x|x) = 0 . \end{aligned}$$

Norma vektoru $f(x) - a \cdot f(x)$ je rovna nule, proto je

$$f(ax) = a \cdot f(x) .$$

Pro každé $x \in U$ je

$$\|f(x)\| = \sqrt{(f(x)|f(x))} = \sqrt{(x|x)} = \|x\| .$$

Jestliže je $f(x) = o$, je podle předchozího $\|x\| = 0$ a proto $x = o$. Unitární zobrazení je tedy monomorfismus zachovávající normu.

Implikace $(ii) \implies (iii)$ je triviální.

$(iii) \implies (i)$ Nechť f je homomorfismus zachovávající normu. Pro každé dva vektory $x, y \in U$ a číslo $a \in T$ je proto $\|f(x + ay)\| = \|x + ay\|$. Tedy

$$(f(x + ay)|f(x + ay)) = (x + ay|x + ay) .$$

Protože je f homomorfismus, je

$$(f(x) + a \cdot f(y)|f(x) + a \cdot f(y)) = (x + ay|x + ay)$$

a odtud

$$\begin{aligned} (f(x)|f(x)) + \bar{a} \cdot (f(x)|f(y)) + a \cdot (f(y)|f(x)) + a\bar{a} \cdot (f(y)|f(y)) &= \\ = (x|x) + \bar{a} \cdot (x|y) + a \cdot (y|x) + a\bar{a} \cdot (y|y) . \end{aligned}$$

Tedy

$$\begin{aligned} \|f(x)\|^2 + \bar{a} \cdot (f(x)|f(y)) + a \cdot (f(y)|f(x)) + a\bar{a} \cdot \|f(y)\|^2 &= \\ = \|x\|^2 + \bar{a} \cdot (x|y) + a \cdot (y|x) + a\bar{a} \cdot \|y\|^2 . \end{aligned}$$

Protože f zachovává normu, je

$$\bar{a} \cdot (f(x)|f(y)) + a \cdot (f(y)|f(x)) = \bar{a} \cdot (x|y) + a \cdot (y|x) .$$

Pro $a = 1$ dostáváme rovnost

$$(f(x)|f(y)) + (f(y)|f(x)) = (x|y) + (y|x) .$$

Jestliže $T = \mathbb{R}$, je tedy $(f(x)|f(y)) = (x|y)$. Jestliže $T = \mathbb{C}$, položíme ještě $a = i$ a po zkrácení dostáváme rovnost

$$(f(x)|f(y)) - (f(y)|f(x)) = (x|y) - (y|x) .$$

Z obou rovností (pro $a = 1$ a pro $a = i$) dostáváme rovnost $(f(x)|f(y)) = (x|y)$. Homomorfismus zachovávající normu je tedy unitární zobrazení. \square

Z předchozí věty plyne, že místo o unitárním zobrazení můžeme hovořit o *unitárním monomorfismu* či o *unitárním vnoření*.

27.3. Definice. *Izometrií* budeme rozumět každý unitární izomorfismus. Dva unitární prostory se nazývají *izometrické*, existuje-li izometrie jednoho na druhý.

V následující větě shrneme několik jednoduchých tvrzení, jejichž důkazy jsou zjevné.

27.4. Věta.

- (i) *Složení dvou unitárních zobrazení je unitární zobrazení.*
- (ii) *Složení dvou izometrií je izometrie.*
- (iii) *Inverzní izomorfismus k izometrii je izometrie.*
- (iv) *Množina všech izometrií unitárního prostoru (tj. unitárních automorfismů tohoto prostoru) tvoří grupu.*
- (v) *Obrazem ortonormální (ortonormální) báze (resp. podmnožiny) unitárního prostoru při unitárním zobrazení f je ortogonální (ortonormální) báze (resp. podmnožina) unitárního prostoru $\text{Im } f$.*
- (vi) *Převádí-li zobrazení f ortonormální bázi jednoho unitárního prostoru injektivně na ortonormální podmnožinu druhého unitárního prostoru, pak je f unitární zobrazení.*

Důkaz. Tvrzení (i) – (v) jsou zřejmá. Tvrzení (vi) se dokáže s pomocí Parsevalovy rovnosti 26.29(ii). Nechť f je zobrazení prostoru U do prostoru V , které injektivně převádí ortonormální bázi prostoru U na ortonormální bázi prostoru $\text{Im } f$. Vzhledem k Parsevalově rovnosti je skalární součin vektorů $x, y \in U$ roven skalárnímu součinu vektorů $f(x)$ a $f(y)$, tj. f je unitární zobrazení. \square

27.5. Věta. *Dva konečně generované unitární prostory nad tělesem T jsou izometrické právě tehdy, když mají stejnou dimenzi.*

Důkaz. Jestliže jsou dva unitární prostory izometrické, jsou jako vektorové prostory izomorfní a mají proto stejnou dimenzi (i bez předpokladu konečných dimenzí).

Jestliže mají dva unitární prostory stejnou konečnou dimenzi, zvolíme v každém nějakou ortonormální bázi (viz věta 26.17) a libovolně vzájemně jednoznačné zobrazení těchto bází rozšíříme na izomorfismus těchto prostorů, který je zřejmě izometrií (viz 27.4(vi)). \square

Dva unitární prostory stejné nekonečné dimenze nemusí být izometrické. Uvažujme unitární prostor V , který nemá ortonormální bázi. Zvolme nějakou bázi tohoto prostoru a definujme pomocí této báze nový skalární součin způsobem uvedeným v poznámce 26.30; zvolená báze je potom ortonormální bází vzhledem k tomuto novému skalárnímu součinu. Uvažované dva unitární prostory definované na témže vektorovém prostoru nejsou izometrické, neboť jeden ortonormální bázi má a druhý nemá.

27.6. Definice. Matice A nad tělesem T se nazývá *unitární*, jestliže $A^T \cdot \bar{A} = E$. Jestliže $T = \mathbb{R}$, pak hovoříme o *ortogonální* (nebo též *ortonormální*) matici.

Nechť $A = (a_{ij})$ je matice typu $n \times m$ nad tělesem T . Rovnost $A^T \cdot \bar{A} = E$ vyjádříme v prvcích:

$$\forall i, j = 1, \dots, m \quad \sum_{k=1}^n a_{ki} \cdot \bar{a}_{kj} = \delta_{ij}$$

Matice A je tedy unitární právě tehdy, když její sloupce tvoří ortonormální množinu v unitárním prostoru T^n se standardním skalárním součinem (viz příklad 26.3(ii)). Podle věty 26.13 jsou sloupce unitární matice A lineárně nezávislé, hodnota matice A je tedy m a nutně $m \leq n$.

27.7. Věta. *Jestliže je A čtvercová unitární matice, potom je $|\det A| = 1$.*

Důkaz. Podle definice 27.6 je $A^T \cdot \bar{A} = E$, tedy $\det(A^T \cdot \bar{A}) = 1$ a podle věty o násobení determinantů je

$$\det A^T \cdot \det \bar{A} = \det A \cdot \overline{\det A} = |\det A|^2 = 1. \quad \square$$

Čtvercová unitární matice je tedy regulární. Determinant ortogonální matice ($T = \mathbb{R}$) je roven buď 1 nebo -1 . Poznamenejme, že existují matice, které nejsou unitární a jejichž determinant má absolutní hodnotu 1.

27.8. Věta. *Nechť A je čtvercová matice nad tělesem T . Následující tvrzení jsou ekvivalentní:*

- (i) A je unitární,
- (ii) $A^{-1} = \bar{A}^T$,
- (iii) A^T je unitární,
- (iv) A^{-1} je unitární.

Důkaz. Rovnost $A^T \cdot \bar{A} = E$ z definice unitární matice je zřejmě ekvivalentní s rovností $\bar{A}^T \cdot A = E$ (stačí provést transponování), která je opět ekvivalentní s rovností $A^{-1} = \bar{A}^T$. Poslední rovnost je ekvivalentní s rovností $A \cdot \bar{A}^T = E$, která vyjadřuje skutečnost, že A^T je unitární. Obdobně dostaneme ekvivalentní rovnost $\bar{A}^{-1} = A^T$, resp. $\overline{A^{-1}}^T = A$, která je (podle již dokázané ekvivalence prvního a druhého tvrzení) ekvivalentní s tím, že A^{-1} je unitární. \square

Čtvercová matice řádu n je tedy unitární právě tehdy, když její řádky tvoří ortonormální množinu v unitárním prostoru T^n (viz příklad 26.3(ii)); její sloupce i řádky jsou tedy ortonormálními bázemi prostoru T^n .

27.9. Věta. *Nechť U a V jsou unitární prostory, které mají konečné dimenze. Potom je homomorfismus f prostoru U do prostoru V unitární právě tehdy, když jeho matice vzhledem k nějakým ortonormálním bázím prostorů U, V je unitární.*

Důkaz. Necht M, N jsou ortonormální báze prostorů U, V , f je homomorfismus prostoru U do prostoru V a A matice homomorfismu f vzhledem k bázím M, N . Necht $\dim U = m$, $\dim V = n$, tedy matice A je typu $n \times m$.

Jestliže je f unitární, je $f(M)$ ortonormální podmnožina v prostoru V a podle Parsevalovy rovnosti 26.29(ii) jsou tedy sloupce matice A ortonormální množinou v prostoru T^n , tj. matice A je unitární. Jestliže je naopak matice A unitární, je $f(M)$ ortonormální bází podprostoru $\text{Im } f$ prostoru V a homomorfismus f je unitární (viz 27.4(vi)). \square

27.10. Věta. *Nechť V je unitární prostor konečné dimenze, M, N jeho dvě báze a A matice přechodu od báze M k bázi N . Potom platí:*

- (i) *Jestliže jsou báze M a N ortonormální, je matice A unitární.*
- (ii) *Jestliže je báze N ortonormální a matice A unitární, je báze M ortonormální.*
- (iii) *Jestliže je báze M ortonormální a matice A unitární, je báze N ortonormální.*

Důkaz. Necht $M = \{v_1, \dots, v_n\}$ a $A = (a_{ij})$.

(i) První tvrzení vyplývá z předchozí věty.

(ii) Jestliže je N ortonormální a A unitární, potom podle Parsevalovy rovnosti 26.29(ii) můžeme skalární součin vektorů $v_i, v_j \in M$, $i, j = 1, \dots, n$, vypočítat pomocí jejich souřadnic vzhledem k ortonormální bázi N ,

$$(v_i | v_j) = \sum_{k=1}^n a_{ki} \bar{a}_{kj} = \delta_{ij} ,$$

tj. M je ortonormální.

(iii) Jestliže je M ortonormální a A unitární, potom je podle věty 27.8 matice A^{-1} unitární; matice A^{-1} je maticí přechodu od N k M a tedy podle (ii) je N ortonormální. \square

27.11. Příklady.

(i) Uvažujme unitární prostory \mathbb{R}^3 a \mathbb{R}^4 se standardními skalárními součiny. Homomorfismus f prostoru \mathbb{R}^3 do prostoru \mathbb{R}^4 , který vektoru (x, y, z) přiřazuje vektor

$$\frac{1}{2}(x + y - z, -x + y - z, x - y - z, x + y + z) ,$$

má vzhledem ke kanonickým bázím prostorů \mathbb{R}^3 a \mathbb{R}^4 matici

$$A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 & -1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix} .$$

Snadno se prověří, že homomorfismus f je unitárním zobrazením, resp. že matice A je ortogonální. Dále je

$$\begin{aligned} \text{Im } f &= [(1, -1, 1, 1), (1, 1, -1, 1), (-1, -1, -1, 1)] = \\ &= [(1, 0, 0, 1), (0, 0, -1, 1), (1, 1, 0, 0)] . \end{aligned}$$

(ii) Endomorfismus f unitárního prostoru \mathbb{R}^3 se standardním skalárním součinem, který vektoru (x, y, z) přiřazuje vektor

$$\left(\frac{1}{\sqrt{3}}x + \frac{1}{\sqrt{6}}y - \frac{1}{\sqrt{2}}z, \frac{1}{\sqrt{3}}x - \frac{2}{\sqrt{6}}y, \frac{1}{\sqrt{3}}x + \frac{1}{\sqrt{6}}y + \frac{1}{\sqrt{2}}z \right) ,$$

má vzhledem ke kanonické bázi prostoru \mathbb{R}^3 matici

$$A = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} & -\frac{2}{\sqrt{6}} & 0 \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{6}} \cdot \begin{pmatrix} \sqrt{2} & 1 & -\sqrt{3} \\ \sqrt{2} & -2 & 0 \\ \sqrt{2} & 1 & \sqrt{3} \end{pmatrix} .$$

Endomorfismus f je izometrií prostoru \mathbb{R}^3 , matice A je ortogonální; maticí izometrie f^{-1} prostoru \mathbb{R}^3 je matice

$$A^{-1} = A^T = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & -\frac{2}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{6}} \cdot \begin{pmatrix} \sqrt{2} & \sqrt{2} & \sqrt{2} \\ 1 & -2 & 1 \\ -\sqrt{3} & 0 & \sqrt{3} \end{pmatrix} .$$

(iii) Báze

$$M = \left\{ \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right), \left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right) \right\} \quad \text{a} \quad N = \left\{ \left(\frac{2}{\sqrt{5}}, \frac{1}{\sqrt{5}} \right), \left(\frac{1}{\sqrt{5}}, -\frac{2}{\sqrt{5}} \right) \right\}$$

jsou ortonormální báze prostoru \mathbb{R}^2 se standardním skalárním součinem. Maticí přechodu od báze M k bázi N je matice

$$A = \begin{pmatrix} \frac{3}{\sqrt{10}} & \frac{1}{\sqrt{10}} \\ -\frac{1}{\sqrt{10}} & \frac{3}{\sqrt{10}} \end{pmatrix} = \frac{1}{\sqrt{10}} \cdot \begin{pmatrix} 3 & 1 \\ -1 & 3 \end{pmatrix}$$

a maticí přechodu od báze N k bázi M je matice

$$A^{-1} = A^T = \begin{pmatrix} \frac{3}{\sqrt{10}} & -\frac{1}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} & \frac{3}{\sqrt{10}} \end{pmatrix} = \frac{1}{\sqrt{10}} \cdot \begin{pmatrix} 3 & -1 \\ 1 & 3 \end{pmatrix} .$$

28. GRAMOVY MATICE A DETERMINANTY

28.1. Definice. Nechť V je reálný nebo komplexní unitární prostor. *Gramovou maticí* vektorů $w_1, \dots, w_m \in V$ nazýváme matici

$$G(w_1, \dots, w_m) = \begin{pmatrix} (w_1|w_1) & \dots & (w_1|w_m) \\ (w_2|w_1) & \dots & (w_2|w_m) \\ \dots & \dots & \dots \\ (w_m|w_1) & \dots & (w_m|w_m) \end{pmatrix}.$$

Determinant této matice se nazývá *Gramův determinant* vektorů w_1, \dots, w_m .

Gramova matice vektorů w_1, \dots, w_m je tedy sestavena ze skalárních součinů těchto vektorů; na místě ij je skalární součin $(w_i|w_j)$.

Jestliže je $M = \{v_1, \dots, v_n\}$ báze prostoru V , potom je $G(v_1, \dots, v_n)$ „maticí skalárního součinu“ (tj. maticí příslušné bilineární, resp. seskvilineární formy) vzhledem k bázi M .

28.2. Věta. *Nechť V je unitární prostor a w_1, \dots, w_m jeho vektory. Potom platí:*

- (i) *Gramova matice $G(w_1, \dots, w_m)$ je hermitovská.*
- (ii) *Pro každé číslo $a \in T$ a každé $j = 1, \dots, m$ je*

$$\det G(w_1, \dots, aw_j, \dots, w_m) = |a|^2 \cdot \det G(w_1, \dots, w_m).$$

- (iii) *Pro každou permutaci $P \in S_m$ je*

$$\det G(w_{P(1)}, \dots, w_{P(m)}) = \det G(w_1, \dots, w_m).$$

Důkaz. Z první vlastnosti skalárního součinu (viz 26.1(i)) vyplývá, že Gramova matice je hermitovská.

Vynásobíme-li vektor w_j číslem $a \in T$, vynásobí se j -tý řádek odpovídající Gramovy matice číslem a a j -tý sloupec číslem \bar{a} ; příslušný Gramův determinant se proto vynásobí číslem $a \cdot \bar{a} = |a|^2$.

Provedeme-li permutaci P vektorů w_1, \dots, w_m , provede se v odpovídající Gramově matici permutace P řádků i sloupců a Gramův determinant se tedy nezmění. \square

V odstavcích 26. paragrafu (viz 26.19 – 26.22) jsme určili souřadnice ortogonální projekce v^p vektoru v na podprostor $W = [w_1, \dots, w_m]$, kde vektory w_1, \dots, w_m tvořily ortogonální bázi podprostoru W (těmito souřadnicemi jsou tzv. Fourierovy koeficienty vektoru v vůči ortogonální množině $\{w_1, \dots, w_m\}$). Nyní najdeme souřadnice vektoru v^p vzhledem k libovolné bázi podprostoru W ; budeme dokonce uvažovat i obecnější případ, kdy je podprostor W generován vektory w_1, \dots, w_m , které nemusí být lineárně nezávislé.

28.4. Věta.

- (i) *Gramův determinant lineárně závislých vektorů je roven nule.*
(ii) *Gramův determinant lineárně nezávislých vektorů je kladný.*

Důkaz. (i) Vztah mezi lineární nezávislostí vektorů a regularitou jejich Gramovy matice byl ukázán v druhé části důkazu předchozího lemmatu.

(ii) Necht' w_1, \dots, w_m jsou lineárně nezávislé vektory unitárního prostoru V . Podprostor $W = [w_1, \dots, w_m]$ je též unitární; skalární součin na prostoru W (tj. zúžení skalárního součinu prostoru V) je pozitivně definitní hermitovská seskvilineární, resp. symetrická bilineární forma — označme ji f . Gramova matice $G(w_1, \dots, w_m)$ je maticí formy f vzhledem k bázi $\{w_1, \dots, w_m\}$. Matice formy f vzhledem k nějaké ortonormální bázi N prostoru W je jednotková. Podle 23.7, resp. 24.7 je tedy

$$E = B^T \cdot G(w_1, \dots, w_m) \cdot \overline{B},$$

kde B je matice přechodu od báze N k bázi $\{w_1, \dots, w_m\}$. Podle věty o násobení determinantů je

$$1 = \det B^T \cdot \det G(w_1, \dots, w_m) \cdot \overline{\det B} = |\det B|^2 \cdot \det G(w_1, \dots, w_m).$$

Gramův determinant lineárně nezávislých vektorů je tedy kladný.

Jiný důkaz. Zvolme v podprostoru $[w_1, \dots, w_m]$ ortonormální bázi N (viz 26.17). Vzhledem k Parsevalově rovnosti 26.29 je

$$G(w_1, \dots, w_m) = A \cdot \overline{A}^T,$$

kde A je matice řádu m , která pro každé $j = 1, \dots, m$ má v j -tém řádku souřadnice vektoru w_j vzhledem k bázi N . Podle věty o násobení determinantů je nyní

$$\det G(w_1, \dots, w_m) = \det A \cdot \det \overline{A}^T = \det A \cdot \overline{\det A} = |\det A|^2.$$

Odtud vyplývají tvrzení (i) a (ii). \square

Tvrzení předchozí věty přejde v případě jednoho vektoru ve čtvrtou vlastnost skalárního součinu (viz 26.1(iv)) a v případě dvou vektorů v Cauchyovu-Schwarzovu nerovnost 26.6:

$$\det G(w_1) = (w_1|w_1) \geq 0;$$

rovnost platí právě tehdy, když je $w_1 = o$.

$$\begin{aligned} \det G(w_1, w_2) &= (w_1|w_1) \cdot (w_2|w_2) - (w_1|w_2) \cdot (w_2|w_1) = \\ &= \|w_1\|^2 \cdot \|w_2\|^2 - |(w_1|w_2)|^2 \geq 0, \end{aligned}$$

neboli

$$|(w_1|w_2)| \leq \|w_1\| \cdot \|w_2\|;$$

rovnost platí právě tehdy, když jsou vektory w_1, w_2 lineárně závislé.

28.5. Věta. *Nechť W je konečně dimenzionální podprostor unitárního prostoru V . Jestliže $v = v^p + v^\perp$ je ortogonální rozklad vektoru $v \in V$ určený podprostorem W , tj. $v^p \in W$, $v^\perp \in W^\perp$, potom*

$$\|v^\perp\|^2 = \frac{\det G(v, w_1, \dots, w_m)}{\det G(w_1, \dots, w_m)},$$

kde $\{w_1, \dots, w_m\}$ je nějaká báze podprostoru W .

Důkaz. Nechť $\{w_1, \dots, w_m\}$ je báze podprostoru W . Podle 28.3 je

$$v^p = \sum_{j=1}^m \frac{\det G_j}{\det G(w_1, \dots, w_m)} \cdot w_j,$$

kde symbol G_j má stejný smysl jako ve větě 28.3. Dále je

$$\begin{aligned} \|v^\perp\|^2 &= (v^\perp|v^\perp) = (v - v^p|v - v^p) = (v - v^p|v) = (v|v) - (v^p|v) = \\ &= (v|v) - \sum_{j=1}^m \frac{\det G_j}{\det G(w_1, \dots, w_m)} \cdot (w_j|v), \end{aligned}$$

takže

$$\|v^\perp\|^2 \cdot \det G(w_1, \dots, w_m) = \|v\|^2 \cdot \det G(w_1, \dots, w_m) - \sum_{j=1}^m \det G_j \cdot (w_j|v). \quad (1)$$

Rozvineme-li determinant matice $G(v, w_1, \dots, w_m)^T$ podle prvního řádku, dostaneme rovnost

$$\begin{aligned} \det G(v, w_1, \dots, w_m) &= \\ &= (v|v) \cdot \det G(w_1, \dots, w_m) + \sum_{j=1}^m (-1)^j \cdot (w_j|v) \cdot (-1)^{j-1} \cdot \det G_j. \quad (2) \end{aligned}$$

Porovnáním rovností (1) a (2) – jejich pravé strany se rovnají – dostáváme rovnost

$$\|v^\perp\|^2 \cdot \det G(w_1, \dots, w_m) = \det G(v, w_1, \dots, w_m),$$

kterou jsme měli dokázat. \square

28.6. Přibližné řešení soustavy lineárních rovnic.

V technické praxi nebo v experimentálních vědách se často setkáváme s případem, kdy nějaká reálná nebo komplexní veličina \mathfrak{V} je lineární kombinací reálných nebo komplexních veličin $\mathfrak{U}_1, \dots, \mathfrak{U}_m$, nebo ji případně chceme lineární kombinací těchto veličin aproximovat. Předpokládejme tedy, že

$$\mathfrak{V} = \sum_{j=1}^m x_j \mathfrak{U}_j,$$

kde x_1, \dots, x_m jsou konstanty, které chceme najít. Veličiny $\mathfrak{U}_1, \dots, \mathfrak{U}_m, \mathfrak{V}$ jsou zjištěny experimentálně v n případech (např. měřeních), přičemž číslo n může být dostatečně velké:

	\mathfrak{U}_1	\mathfrak{U}_2	...	\mathfrak{U}_m	\mathfrak{V}
1	u_{11}	u_{12}	...	u_{1m}	v_1
2	u_{21}	u_{22}	...	u_{2m}	v_2
\vdots	\vdots	\vdots	...	\vdots	\vdots
n	u_{n1}	u_{n2}	...	u_{nm}	v_n

Má tedy platit

$$\begin{aligned} u_{11}x_1 + u_{12}x_2 + \dots + u_{1m}x_m &= v_1, \\ u_{21}x_1 + u_{22}x_2 + \dots + u_{2m}x_m &= v_2, \\ \dots & \\ u_{n1}x_1 + u_{n2}x_2 + \dots + u_{nm}x_m &= v_n. \end{aligned} \tag{3}$$

Pro hledané koeficienty x_1, \dots, x_m tedy máme n lineárních rovnic. Víme, že taková soustava nemusí mít řešení v exaktním slova smyslu.

Připomeňme, že soustava má řešení právě tehdy, když je sloupec pravých stran lineární kombinací sloupců matice této soustavy; koeficienty této lineární kombinace jsou hledaná čísla x_1, \dots, x_m (nemusí být určena jednoznačně).

Protože se snažíme co možná nejpřesněji stanovit čísla x_1, \dots, x_m , usilujeme o to, aby číslo n bylo podstatně větší než číslo m ; provádíme tedy např. větší počet měření, při nichž však dochází k chybám, nepřesnostem a zaokrouhlování. Navíc nemusí být skutečný vztah mezi veličinami $\mathfrak{U}_1, \dots, \mathfrak{U}_m, \mathfrak{V}$ „přesně lineární“. To vše způsobuje, že soustava (3) exaktní řešení většinou nemá.

Hledáme tedy koeficienty x_1, \dots, x_m tak, aby se levé strany soustavy (3) nelišily mnoho od pravých stran. Za míru odchylky se většinou bere součet čtverců absolutních hodnot rozdílů levých a pravých stran, tj. číslo

$$\Delta = \sum_{j=1}^n |v_j - u_{j1}x_1 - u_{j2}x_2 - \dots - u_{jm}x_m|^2.$$

jednoznačně, dá se však vyjádřit více způsoby jako lineární kombinace vektorů u_1, \dots, u_m .

Jestliže má soustava (3) exaktní řešení, pak výše uvedeným způsobem dojdeme právě k němu. Vektor v je totiž vektorem podprostoru $[u_1, \dots, u_m]$, je roven své ortogonální projekci na tento podprostor a nalezená čísla x_1, \dots, x_m , jsou řešením soustavy (3). Číslo Δ je rovno nule; to odpovídá i tomu, že vektory v, u_1, \dots, u_m jsou lineárně závislé a tedy $G(v, u_1, \dots, u_m) = 0$.

28.7. Příklad. Snadno se přesvědčíme, že soustava lineárních rovnic

$$\begin{aligned} 2x_1 + x_2 + x_3 &= 2, \\ x_1 - x_2 - x_3 &= 1, \\ x_1 + x_2 + 3x_3 &= 0, \\ x_2 - x_3 &= 2 \end{aligned}$$

nemá řešení. Najdeme tedy přibližné řešení pomocí Gramovy matice, jak to bylo ukázáno v předchozím. Položme

$$u_1 = (2, 1, 1, 0), \quad u_2 = (1, -1, 1, 1), \quad u_3 = (1, -1, 3, -1), \quad v = (2, 1, 0, 2)$$

a vyřešme soustavu lineárních rovnic s Gramovou maticí $G(u_1, u_2, u_3)$ a sloupcem pravých stran $((v|u_1), (v|u_2), (v|u_3))^T$. Jde o soustavu rovnic

$$\begin{aligned} 6x_1 + 2x_2 + 4x_3 &= 5, \\ 2x_1 + 4x_2 + 4x_3 &= 3, \\ 4x_1 + 4x_2 + 12x_3 &= -1, \end{aligned}$$

která má jediné řešení $x_1 = 1, x_2 = 1, x_3 = -\frac{3}{4}$. Přibližným řešením zadané soustavy rovnic je tedy trojice $(1, 1, -\frac{3}{4})$. Správnost výpočtu můžeme prověřit zkontrolováním kolmosti vektoru $v - x_1 u_1 - x_2 u_2 - x_3 u_3 = \frac{1}{4}(-1, 1, 1, 1)$ na vektory u_1, u_2, u_3 . „Chybu“ Δ můžeme vypočítat podle vzorce

$$\Delta = \frac{\det G(v, u_1, u_2, u_3)}{\det G(u_1, u_2, u_3)} = \frac{36}{144} = \frac{1}{4}$$

nebo přímo podle definice; jde o dvojmoc normy vektoru $\frac{1}{4}(-1, 1, 1, 1)$.

29. ADJUNGOVANÉ A SAMOAJUNGOVANÉ HOMOMORFISMY

29.1. Definice. Nechť U a V jsou unitární prostory nad týmž tělesem T . Homomorfismy $f : U \rightarrow V$ a $g : V \rightarrow U$ se nazývají *navzájem adjungované*, jestliže pro libovolně zvolené vektory $u \in U$ a $v \in V$ je

$$(f(u) | v) = (u | g(v)) .$$

Endomorfismus prostoru U se nazývá *samoajungovaný*, jestliže pro libovolně zvolené vektory $u_1, u_2 \in U$ je

$$(f(u_1) | u_2) = (u_1 | f(u_2)) .$$

Vzhledem k první vlastnosti skalárního součinu (viz 26.1(i)) jsou rovnosti

$$(f(u) | v) = (u | g(v)) \quad \text{a} \quad (g(v) | u) = (v | f(u))$$

navzájem ekvivalentní, takže vztah vzájemné adjungovanosti je symetrický.

Ke každému homomorfismu $f : U \rightarrow V$ existuje nejvýše jeden homomorfismus $g : V \rightarrow U$, takový, že f a g jsou navzájem adjungované. Pokud by pro každé $u \in U$ a $v \in V$ platilo

$$(f(u) | v) = (u | g_1(v)) = (u | g_2(v)) ,$$

pak by pro každé $u \in U$ a $v \in V$ bylo

$$(u | g_1(v) - g_2(v)) = 0 ;$$

položíme-li např. $u = g_1(v) - g_2(v)$, dostáváme ze čtvrté vlastnosti skalárního součinu rovnost $g_1(v) = g_2(v)$ pro každé $v \in V$.

Jsou-li homomorfismy $f_1 : U \rightarrow V$ a $g_1 : V \rightarrow U$ navzájem adjungované a homomorfismy $f_2 : U \rightarrow V$ a $g_2 : V \rightarrow U$ také navzájem adjungované, jsou homomorfismy $f_1 + f_2$ a $g_1 + g_2$ rovněž navzájem adjungované. Pro libovolně zvolené vektory $u \in U$ a $v \in V$ je totiž

$$(f_1(u) | v) = (u | g_1(v)) , \quad (f_2(u) | v) = (u | g_2(v)) ;$$

sečtením těchto dvou rovností dostaneme rovnost

$$((f_1 + f_2)(u) | v) = (u | (g_1 + g_2)(v)) .$$

Jsou-li homomorfismy $f : U \rightarrow V$ a $g : V \rightarrow U$ navzájem adjungované, pak jsou pro každé číslo $a \in T$ homomorfismy af a $\bar{a}g$ rovněž navzájem adjungované, neboť z rovnosti $(f(u) | v) = (u | g(v))$ ihned vyplývá rovnost

$$((af)(u) | v) = (u | (\bar{a}g)(v)) .$$

Jsou-li homomorfismy $f : U \rightarrow V$ a $g : V \rightarrow U$ navzájem adjungované a homomorfismy $f' : V \rightarrow W$ a $g' : W \rightarrow V$ také navzájem adjungované, pak jsou homomorfismy $f'f$ a gg' rovněž navzájem adjungované. Pro libovolně zvolené vektory $u \in U$ a $w \in W$ je totiž

$$(f'f(u) | w) = (f(u) | g'(w)) = (u | gg'(w)) .$$

29.2. Věta. *Jestliže $f : U \rightarrow V$ a $g : V \rightarrow U$ jsou navzájem adjungované homomorfismy unitárních prostorů U a V , potom endomorfismus gf prostoru U , resp. fg prostoru V je samoadjungovaný.*

Důkaz. Jsou-li homomorfismy $f : U \rightarrow V$ a $g : V \rightarrow U$ navzájem adjungované, potom pro libovolné vektory $u_1, u_2 \in U$ je

$$(gf(u_1) | u_2) = (f(u_1) | f(u_2)) = (u_1 | gf(u_2)) ,$$

takže endomorfismus gf prostoru U je samoadjungovaný. Stejně se ukáže, že je samoadjungovaný i endomorfismus fg prostoru V . \square

29.3. Věta. *Nechť U, V jsou unitární prostory konečných dimenzí a M, N jejich ortonormální báze. Nechť $f : U \rightarrow V, g : V \rightarrow U$ jsou homomorfismy a A, B jejich matice vzhledem k bázím M, N , resp. N, M . Homomorfismy f a g jsou navzájem adjungované právě tehdy, když je $A = \bar{B}^T$.*

Důkaz. Pišme $M = \{u_1, \dots, u_m\}, N = \{v_1, \dots, v_n\}, A = (a_{kj})$ a $B = (b_{jk})$. Z definice matice homomorfismu plyne, že pro každé $j = 1, \dots, m$ a $k = 1, \dots, n$ je

$$(f(u_j) | v_k) = \left(\sum_{s=1}^n a_{sj} v_s | v_k \right) = a_{kj} ,$$

$$(u_j | g(v_k)) = \left(u_j | \sum_{r=1}^m b_{rk} u_r \right) = \bar{b}_{jk} .$$

Jsou-li tedy homomorfismy f a g navzájem adjungované, je $A = \bar{B}^T$.

Předpokládejme naopak, že $A = \bar{B}^T$. Jsou-li $x \in U$ a $y \in V$ libovolné vektory, potom je podle věty 11.2

$$\langle f(x) \rangle_N = (A \cdot \langle x \rangle_M^T)^T = \langle x \rangle_M \cdot A^T ,$$

$$\overline{\langle g(y) \rangle}_M^T = \overline{B \cdot \langle y \rangle}_N^T = \overline{B} \cdot \overline{\langle y \rangle}_N^T ;$$

podle Parsevalovy rovnosti je potom

$$(f(x) | y) = \langle f(x) \rangle_N \cdot \overline{\langle y \rangle}_N^T = \langle x \rangle_M \cdot A^T \cdot \overline{\langle y \rangle}_N^T ,$$

$$(x | g(y)) = \langle x \rangle_M \cdot \overline{\langle g(y) \rangle}_M^T = \langle x \rangle_M \cdot \overline{B} \cdot \overline{\langle y \rangle}_N^T .$$

Protože $A^T = \overline{B}$, jsou homomorfismy f a g navzájem adjungované. \square

29.4. Důsledek. *Navzájem adjungované homomorfismy konečně dimenzionálních unitárních prostorů mají stejnou hodnotu.*

Důkaz. Stačí si uvědomit, že hodnota homomorfismu je rovna hodnotě jeho matice a užít větu 29.3. \square

29.5. Důsledek. *Endomorfismus komplexního (resp. reálného) unitárního prostoru konečné dimenze je samoadjungovaný právě tehdy, když jeho matice vzhledem k nějaké ortonormální bázi je hermitovská (resp. symetrická).*

Důkaz. Důkaz plyne z věty 29.3. \square

Nyní je zřejmé, proč je samoadjungovaný endomorfismus na komplexním, resp. reálném unitárním prostoru nazýván též *hermitovským*, resp. *symetrickým* endomorfismem.

29.6. Důsledek. *Nechť U a V jsou unitární prostory konečných dimenzí. Ke každému homomorfismu $f : U \rightarrow V$ existuje právě jediný homomorfismus $g : V \rightarrow U$, takový, že f a g jsou navzájem adjungované.*

Důkaz. Nechť M a N jsou ortonormální báze unitárních prostorů U a V , nechť $f : U \rightarrow V$ je homomorfismus a A jeho matice vzhledem k bázím M , N . Jestliže $g : V \rightarrow U$ je homomorfismus, jehož maticí vzhledem k bázím N , M je matice \overline{A}^T , potom podle věty 29.3 jsou homomorfismy f a g navzájem adjungované; zřejmě je g jediným takovým endomorfismem (viz např. 11.2). \square

Homomorfismus g z předchozího důsledku nazýváme *adjungovaným homomorfismem* k homomorfismu f ; budeme jej značit f_{ad} . Endomorfismus f prostoru V je tedy samoadjungovaný právě tehdy, když $f_{ad} = f$.

Jestliže jsou $f, g : U \rightarrow V$ a $h : V \rightarrow W$ homomorfismy unitárních prostorů U, V, W konečných dimenzí, potom je podle předešlého (viz poznámky za definicí 29.1)

$$(f_{ad})_{ad} = f , \quad (f + g)_{ad} = f_{ad} + g_{ad} , \quad (af)_{ad} = \bar{a} \cdot f_{ad} , \quad (hf)_{ad} = f_{ad} \cdot h_{ad} .$$

Poznamenejme ještě, že podle věty 29.3 a důsledku 29.5 můžeme snadno konstruovat příklady navzájem adjungovaných homomorfismů a samoadjungovaných endomorfismů.

29.7. Věta. *Nechť U, V jsou unitární prostory konečných dimenzí a f homomorfismus prostoru U do prostoru V . Potom je*

$$\text{Ker } f_{ad} = (\text{Im } f)^\perp, \quad \text{Im } f_{ad} = (\text{Ker } f)^\perp$$

a podprostory $\text{Im } f_{ad}$ a $\text{Im } f$ jsou na sebe izomorfne zobrazeny zúženými homomorfismů f a f_{ad} .

Důkaz. Nechť $v \in \text{Im } f$ a $v' \in \text{Ker } f_{ad}$. Potom existuje vektor $u \in U$, pro který $f(u) = v$ a tedy

$$(v | v') = (f(u) | v') = (u | f_{ad}(v')) = (u | o) = 0.$$

Odtud

$$\text{Ker } f_{ad} \subseteq (\text{Im } f)^\perp$$

a proto

$$d(f_{ad}) \leq \dim V - r(f).$$

Nechť $u \in \text{Im } f_{ad}$ a $u' \in \text{Ker } f$. Potom existuje vektor $v \in V$, pro který $f_{ad}(v) = u$ a tedy

$$(u' | u) = (u' | f_{ad}(v)) = (f(u') | v) = (o | v) = 0.$$

Odtud

$$\text{Im } f_{ad} \subseteq (\text{Ker } f)^\perp$$

a proto

$$r(f_{ad}) \leq \dim U - d(f).$$

Sečtením obou nerovností a užitím věty o hodnotě a defektu dostáváme:

$$\dim V = d(f_{ad}) + r(f_{ad}) \leq \dim V + \dim U - r(f) - d(f) = \dim V.$$

Nastane tedy rovnost ve všech třech vztazích a proto je

$$\text{Ker } f_{ad} = (\text{Im } f)^\perp \quad \text{a} \quad \text{Im } f_{ad} = (\text{Ker } f)^\perp.$$

Homomorfismus f je na prostoru $\text{Im } f_{ad}$ prostý, zobrazuje $\text{Im } f_{ad}$ na $\text{Im } f$. Homomorfismus f_{ad} je prostý na $\text{Im } f$ a zobrazuje $\text{Im } f$ na $\text{Im } f_{ad}$. \square

Nechť U, V jsou unitární prostory konečných dimenzí. Je-li f homomorfismus prostoru U do prostoru V , potom je

$$U = \text{Ker } f \oplus \text{Im } f_{ad}, \quad V = \text{Ker } f_{ad} \oplus \text{Im } f,$$

přičemž $\text{Ker } f$ a $\text{Im } f_{ad}$ jsou navzájem ortogonální doplňky v prostoru U a $\text{Ker } f_{ad}$ a $\text{Im } f$ jsou navzájem ortogonální doplňky v prostoru V .

Je-li f samoadjungovaný endomorfismus prostoru U , potom je

$$U = \text{Ker } f \oplus \text{Im } f ,$$

přičemž $\text{Ker } f$ a $\text{Im } f$ jsou navzájem ortogonální doplňky v prostoru U .

Připomeňme nyní pojem vlastního čísla a vlastního vektoru endomorfismu.

Nechť f je endomorfismus prostoru V nad tělesem T . Jestliže je $f(v) = av$, pro nějaký skalár $a \in T$ a nenulový vektor $v \in V$, pak říkáme, že a je vlastní číslo endomorfismu f a v vlastní vektor endomorfismu f příslušný k vlastnímu číslu a . Jestliže je A matice endomorfismu f vzhledem k bázi M prostoru V , potom je

$$\langle f(v) \rangle_M^T = A \cdot \langle v \rangle_M^T = a \cdot \langle v \rangle_M^T ,$$

tj. skalár a je vlastním číslem matice A a vektor $\langle v \rangle_M$, tj. vektor souřadnic vektoru v vzhledem k bázi M , je příslušným vlastním vektorem matice A .

Z důsledku 29.5 a věty 17.20 vyplývá, že všechna vlastní čísla samoadjungovaného endomorfismu jsou reálná.

29.8. Věta. *Nechť V je (reálný nebo komplexní) unitární prostor konečné dimenze. Ke každému samoadjungovanému endomorfismu f prostoru V existuje ortonormální báze prostoru V složená z vlastních vektorů endomorfismu f .*

Důkaz. Nechť f je samoadjungovaný endomorfismus prostoru V . Tvrzení věty dokážeme indukcí podle dimenze prostoru V .

Předpokládejme, že $\dim V = 1$; nechť $v \in V$ je libovolně zvolený normovaný vektor. Potom je $N = \{v\}$ ortonormální báze a existuje číslo a takové, že $f(v) = av$, tj. a je vlastní číslo endomorfismu f a v příslušný vlastní vektor. Poznamenejme, že číslo a je reálné, neboť endomorfismus f je samoadjungovaný.

Předpokládejme, že $\dim V = n$ a že tvrzení věty platí pro $n - 1$. Nechť $a \in \mathbb{R}$ je nějaké vlastní číslo endomorfismu f a v_1 příslušný normovaný vlastní vektor, tj. $f(v_1) = av_1$ a $\|v_1\| = 1$.

Ukážeme, že pro ortogonální doplněk $[v_1]^\perp$ podprostoru $[v_1]$ v prostoru V je

$$f([v_1]^\perp) \subseteq [v_1]^\perp .$$

Pro libovolný vektor $x \in [v_1]^\perp$ je totiž

$$(f(x) | v_1) = (x | f(v_1)) = (x | av_1) = a \cdot (x | v_1) = 0 ,$$

takže $f(x) \in [v_1]^\perp$. Endomorfismus f prostoru V tedy můžeme zúžit na endomorfismus f' podprostoru $[v_1]^\perp$ dimenze $n - 1$; zřejmě je endomorfismus f' na tomto podprostoru samoadjungovaný. Podle indukčního předpokladu existuje ortonormální báze $\{v_2, \dots, v_n\}$ podprostoru $[v_1]^\perp$ složená z vlastních vektorů endomorfismu f' . Tedy $N = \{v_1, v_2, \dots, v_n\}$ je ortonormální báze prostoru V složená z vlastních vektorů endomorfismu f . \square

Poznamenejme, že matice samoadjungovaného endomorfismu f vzhledem k výše uvedené bázi N je reálná diagonální matice; na diagonále má vlastní čísla endomorfismu f .

29.9. Důsledek. *Ke každé hermitovské (resp. reálné symetrické) matici A existuje taková unitární (resp. ortogonální) matice C , že $C^{-1}AC$ je reálná diagonální matice. Matice C má ve sloupcích normované vlastní vektory matice A .*

Důkaz. Nechť A je hermitovská (reálná symetrická) matice řádu n . Uvažujme unitární prostor \mathbb{C}^n (resp. \mathbb{R}^n) se standardním skalárním součinem, nechť f je endomorfismus tohoto prostoru, jehož maticí vzhledem ke kanonické bázi je matice A . Endomorfismus f je samoadjungovaný (viz 29.5); podle předchozí věty existuje ortonormální báze M prostoru \mathbb{C}^n (resp. \mathbb{R}^n) složená z vlastních vektorů endomorfismu f . Matice D endomorfismu f vzhledem k bázi M je reálná diagonální matice, na její diagonále jsou vlastní čísla endomorfismu f , tj. vlastní čísla matice A ; je tedy

$$D = C^{-1}AC,$$

kde C je matice přechodu od báze M k bázi kanonické, tj. ve sloupcích matice C jsou vektory báze M . Podle věty 27.10 je C unitární (resp. ortogonální) matice. \square

Důkaz předchozího důsledku dává přímý návod, jak k dané hermitovské (resp. reálné symetrické) matici najít nejen její diagonální tvar, ale zejména unitární (resp. ortogonální) matici C , která ji na tento tvar transformuje.

29.10. Příklady.

(i) Reálná symetrická matice

$$A = \begin{pmatrix} -2 & 2 \\ 2 & 1 \end{pmatrix}$$

má vlastní čísla 2, -3 a příslušné normované vlastní vektory

$$\frac{1}{\sqrt{5}}(1, 2) \quad \text{a} \quad \frac{1}{\sqrt{5}}(2, -1).$$

Podle předešlého důsledku se matice A převede na diagonální tvar D pomocí ortogonální matice

$$C = \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & \frac{-1}{\sqrt{5}} \end{pmatrix},$$

tj.

$$C^{-1}AC = \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & \frac{-1}{\sqrt{5}} \end{pmatrix} \cdot \begin{pmatrix} -2 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & \frac{-1}{\sqrt{5}} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix} = D.$$

Na diagonále matice D jsou vlastní čísla matice A , ve sloupcích matice C jsou odpovídající normované vlastní vektory matice A , dále je $C^{-1} = C^T$.

(ii) Hermitovská matice

$$A = \begin{pmatrix} 1 & -i & 0 \\ i & 0 & -1 \\ 0 & -1 & 1 \end{pmatrix}$$

má vlastní čísla 1, -1, 2 a příslušné normované vlastní vektory

$$\frac{1}{\sqrt{2}} (1, 0, i), \quad \frac{1}{\sqrt{6}} (i, 2, 1), \quad \frac{1}{\sqrt{3}} (i, -1, 1).$$

Podle předchozího důsledku se matice A převede na diagonální tvar $D = C^{-1}AC$ pomocí unitární matice

$$C = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{6}} & \frac{i}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{-1}{\sqrt{3}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{pmatrix},$$

tj.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{-i}{\sqrt{2}} \\ \frac{-i}{\sqrt{6}} & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ \frac{-i}{\sqrt{3}} & \frac{-1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \end{pmatrix} \cdot \begin{pmatrix} 1 & -i & 0 \\ i & 0 & -1 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{6}} & \frac{i}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{-1}{\sqrt{3}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Na diagonále matice D jsou vlastní čísla matice A , ve sloupcích matice C jsou odpovídající normované vlastní vektory matice A , dále je $C^{-1} = \overline{C}^T$.

(iii) Reálná symetrická matice

$$A = \begin{pmatrix} 2 & 2 & -2 \\ 2 & 5 & -4 \\ -2 & -4 & 5 \end{pmatrix}$$

má dvojnásobné vlastní číslo 1 a jednoduché vlastní číslo 10; k vlastnímu číslu 1 přísluší např. normované, navzájem ortogonální vlastní vektory

$$\frac{1}{\sqrt{5}}(2, -1, 0), \quad \frac{1}{3\sqrt{5}}(2, 4, 5)$$

a k vlastnímu číslu 10 normovaný vlastní vektor

$$\frac{1}{3}(1, 2, -2).$$

Matice A se tedy převede na diagonální tvar $D = C^{-1}AC$ pomocí ortogonální matice

$$C = \begin{pmatrix} \frac{2}{\sqrt{5}} & \frac{2}{3\sqrt{5}} & \frac{1}{3} \\ \frac{-1}{\sqrt{5}} & \frac{4}{3\sqrt{5}} & \frac{2}{3} \\ 0 & \frac{5}{3\sqrt{5}} & \frac{-2}{3} \end{pmatrix},$$

tj.

$$\begin{pmatrix} \frac{2}{\sqrt{5}} & \frac{-1}{\sqrt{5}} & 0 \\ \frac{2}{3\sqrt{5}} & \frac{4}{3\sqrt{5}} & \frac{5}{3\sqrt{5}} \\ \frac{1}{3} & \frac{2}{3} & \frac{-2}{3} \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 & -2 \\ 2 & 5 & -4 \\ -2 & -4 & 5 \end{pmatrix} \cdot \begin{pmatrix} \frac{2}{\sqrt{5}} & \frac{2}{3\sqrt{5}} & \frac{1}{3} \\ \frac{-1}{\sqrt{5}} & \frac{4}{3\sqrt{5}} & \frac{2}{3} \\ 0 & \frac{5}{3\sqrt{5}} & \frac{-2}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{pmatrix} .$$

Na diagonále matice D jsou vlastní čísla matice A , ve sloupcích matice C jsou odpovídající normované vlastní vektory matice A , dále je $C^{-1} = C^T$.

29.11. Věta. *Nechť U a V jsou unitární prostory téže dimenze. Izomorfismus $f : U \rightarrow V$ je izometrie právě tehdy, když jsou izomorfismy f a f^{-1} navzájem adjungované.*

Důkaz. Předpokládejme, že f je izometrie. Pro libovolné vektory $u \in U$ a $v \in V$ je

$$(f(u)|v) = (f(u)|ff^{-1}(v)) = (u|f^{-1}(v)) ,$$

takže f a f^{-1} jsou navzájem adjungované.

Předpokládejme naopak, že f a f^{-1} jsou navzájem adjungované. Pro libovolné vektory $u_1, u_2 \in U$ je

$$(f(u_1)|f(u_2)) = (u_1|f^{-1}f(u_2)) = (u_1|u_2) ,$$

takže f je izometrie. \square

Jiný důkaz. Pokud mají prostory U a V konečnou dimenzi, můžeme předchozí tvrzení dokázat takto. Nechť A je matice izomorfismu f vzhledem k ortonormálním bázím M, N prostorů U, V . Izomorfismus f je izometrií, právě když je matice A unitární (viz věta 27.9), tj. právě když je $A^{-1} = \overline{A}^T$ (viz věta 27.8), tj. právě když je $f^{-1} = f_{ad}$ (viz věta 29.3). \square

29.12. Důsledek.

- (i) *Nechť U, V jsou unitární prostory a $f : U \rightarrow V$ monomorfismus; označme symbolem g izomorfismus prostoru U na podprostor $\text{Im } f$ prostoru V , pro který je $g(u) = f(u)$ pro každé $u \in U$. Potom je monomorfismus f unitární právě tehdy, když jsou g a g^{-1} navzájem adjungované.*
- (ii) *Nechť f je samoadjungovaný endomorfismus unitárního prostoru U . Potom je f izometrie právě tehdy, když je $f^2 = 1_U$. \square*

29.13. Příklady.

(i) Uvažujme unitární prostory \mathbb{R}^3 a \mathbb{R}^4 se standardním skalárním součinem a homomorfismus $f : \mathbb{R}^3 \rightarrow \mathbb{R}^4$, který zobrazuje vektor $(x, y, z) \in \mathbb{R}^3$ na vektor

$$(x + y + 2z, y - z, x + y + 3z, 2x + y) \in \mathbb{R}^4 .$$

Vzhledem ke kanonickým bázím má homomorfismus f matici

$$A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -1 \\ 1 & 1 & 3 \\ 2 & 1 & 0 \end{pmatrix}.$$

Zřejmě je

$$\text{Ker } f = 0 \quad \text{a} \quad \text{Im } f = [(1, 0, 1, 2), (1, 1, 1, 1), (2, -1, 3, 0)].$$

Homomorfismus f_{ad} má podle věty 29.3 vzhledem ke kanonickým bázím prostorů \mathbb{R}^4 a \mathbb{R}^3 matici

$$A^T = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 \\ 2 & -1 & 3 & 0 \end{pmatrix},$$

tj. f_{ad} zobrazuje vektor $(t, u, v, w) \in \mathbb{R}^4$ na vektor

$$(t + v + 2w, t + u + v + w, 2t - u + 3v) \in \mathbb{R}^3.$$

Je

$$\text{Im } f_{ad} = \mathbb{R}^3 \quad \text{a} \quad \text{Ker } f_{ad} = [(-7, 1, 5, 1)];$$

uvědomme si, že je skutečně

$$\text{Ker } f_{ad} = (\text{Im } f)^\perp \quad \text{a} \quad \text{Im } f_{ad} = (\text{Ker } f)^\perp.$$

Homomorfismus f zobrazuje izomorfně prostor \mathbb{R}^3 na prostor $\text{Im } f$, zúžení homomorfismu f_{ad} zobrazuje izomorfně prostor $\text{Im } f$ na prostor \mathbb{R}^3 ; tyto izomorfismy však nejsou navzájem inverzní, neboť např. f zobrazuje vektor $(1, 0, 0)$ na vektor $(1, 0, 1, 2)$ a tento vektor se při f_{ad} zobrazí na vektor $(6, 4, 5)$. Homomorfismus f tedy není unitární (viz 29.11, resp. 21.12), jak je ostatně ihned vidět už z matice A .

Endomorfismy $f_{ad}f$ a ff_{ad} jsou samoadjungované, jejich matice (vzhledem k příslušné kanonické bázi) jsou

$$\begin{pmatrix} 6 & 4 & 5 \\ 4 & 4 & 4 \\ 5 & 4 & 14 \end{pmatrix} \quad \begin{pmatrix} 6 & -1 & 8 & 3 \\ -1 & 2 & -2 & 1 \\ 8 & -2 & 11 & 3 \\ 3 & 1 & 3 & 5 \end{pmatrix}.$$

(ii) Uvažujme unitární prostor \mathbb{R}^4 se standardním skalárním součinem a endomorfismus f tohoto prostoru, který zobrazuje vektor (x, y, z, t) na vektor

$$\left(\frac{1}{2}x + \frac{1}{2}y + \frac{1}{2}z - \frac{1}{2}t, \frac{1}{2}x + \frac{1}{2}y - \frac{1}{2}z + \frac{1}{2}t, \frac{1}{2}x - \frac{1}{2}y + \frac{1}{2}z + \frac{1}{2}t, \frac{1}{2}x - \frac{1}{2}y - \frac{1}{2}z - \frac{1}{2}t \right).$$

Vzhledem ke kanonické bázi má endomorfismus f matici

$$A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Matice A je ortogonální, endomorfismus f je izometrií prostoru \mathbb{R}^4 , $f^{-1} = f_{ad}$, $A^{-1} = A^T$.

(iii) Uvažujme unitární prostory \mathbb{R}^3 a \mathbb{R}^4 se standardním skalárním součinem a homomorfismus $f : \mathbb{R}^3 \rightarrow \mathbb{R}^4$, který zobrazuje vektor $(x, y, z) \in \mathbb{R}^3$ na vektor

$$\left(\frac{1}{3}x - \frac{2}{3}z, -\frac{2}{3}x + \frac{1}{3}z, \frac{2}{3}x + \frac{2}{3}z, y \right) \in \mathbb{R}^4.$$

Vzhledem ke kanonickým bázím má homomorfismus f matici

$$A = \begin{pmatrix} \frac{1}{3} & 0 & -\frac{2}{3} \\ -\frac{2}{3} & 0 & \frac{1}{3} \\ \frac{2}{3} & 0 & \frac{2}{3} \\ 0 & 1 & 0 \end{pmatrix}.$$

Matice A je ortogonální, f je unitární,

$$\text{Im } f = [(1, -2, 2, 0), (0, 0, 0, 1), (-2, 1, 2, 0)].$$

Homomorfismus f_{ad} má podle věty 29.3 vzhledem ke kanonickým bázím prostorů \mathbb{R}^4 a \mathbb{R}^3 matici

$$A^T = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & \frac{2}{3} & 0 \\ 0 & 0 & 0 & 1 \\ -\frac{2}{3} & \frac{1}{3} & \frac{2}{3} & 0 \end{pmatrix},$$

tj. f_{ad} zobrazuje vektor $(t, u, v, w) \in \mathbb{R}^4$ na vektor

$$\left(\frac{1}{3}t - \frac{2}{3}u + \frac{2}{3}v, w, -\frac{2}{3}t + \frac{1}{3}u + \frac{2}{3}v \right) \in \mathbb{R}^3.$$

Dále je $\text{Ker } f_{ad} = (\text{Im } f)^\perp = [(2, 2, 1, 0)]$.

Homomorfismus f zobrazuje izomorfně prostor \mathbb{R}^3 na prostor $\text{Im } f$, zúžení homomorfismu f_{ad} zobrazuje izomorfně prostor $\text{Im } f$ na prostor \mathbb{R}^3 ; tyto dva homomorfismy jsou navzájem inverzní. Je $f_{ad}f = 1_{\mathbb{R}^3}$ a $A^T A = E$. Složení ff_{ad} však nemůže být identitou na prostoru \mathbb{R}^4 , zúžením tohoto homomorfismu však dostaneme identitu na podprostoru $\text{Im } f$. Dále je

$$AA^T = \begin{pmatrix} \frac{5}{9} & -\frac{4}{9} & -\frac{2}{9} & 0 \\ -\frac{4}{9} & \frac{5}{9} & -\frac{2}{9} & 0 \\ -\frac{2}{9} & -\frac{2}{9} & \frac{8}{9} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(iv) Uvažujme unitární prostor \mathbb{R}^3 se standardním skalárním součinem a endomorfismus f tohoto prostoru, který zobrazuje vektor (x, y, z) na vektor

$$(x + 2y + z, 2x + 4y + 2z, x + 2y) .$$

Vzhledem ke kanonické bázi má endomorfismus f matici

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 0 \end{pmatrix} .$$

Matice A je symetrická, endomorfismus f je samoadjungovaný, není unitární. Podprostory

$$\text{Ker } f = [(2, -1, 0)] , \quad \text{Im } f = [(0, 0, 1), (1, 2, 0)]$$

jsou navzájem ortogonálními doplňky v prostoru \mathbb{R}^3 .

30. FORMY NA UNITÁRNÍCH PROSTORECH

Nechť f je seskvilineární (bilineární) forma na komplexním (reálném) unitárním prostoru V konečné dimenze, nechť M, N jsou báze prostoru V . Jestliže A je matice formy f vzhledem k bázi M , potom je $B = C^T \overline{A} C$ matice formy f vzhledem k bázi N , kde C je matice přechodu od báze N k bázi M (viz 23.7, resp. 24.7). Jestliže jsou báze M, N ortonormální, potom je matice C unitární (viz 27.10), tj. $C^T = \overline{C}^{-1}$ (viz 27.8), $B = \overline{C}^{-1} \overline{A} C$ a matice A a B jsou podobné. Z tohoto důvodu můžeme vyslovit následující definici.

30.1. Definice. Nechť f je seskvilineární (bilineární) forma na komplexním (reálném) unitárním prostoru V konečné dimenze a nechť A je matice formy f vzhledem k nějaké ortonormální bázi prostoru V . *Charakteristickým polynomem, minimálním polynomem, vlastními čísly a spektrem* formy f budeme rozumět po řadě charakteristický polynom, minimální polynom, vlastní čísla a spektrum matice A .

Vlastní čísla hermitovské seskvilineární (symetrické bilineární) formy jsou tedy podle 17.20 reálná čísla.

30.2. Věta. *Nechť V je komplexní (reálný) unitární prostor konečné dimenze. Potom ke každé hermitovské seskvilineární (symetrické bilineární) formě f na prostoru V existuje ortonormální báze prostoru V , která je vůči f polární.*

Důkaz. Nechť M je ortonormální báze prostoru V a A matice formy f vzhledem k bázi M . Protože je f hermitovská, je také A hermitovská. Nechť g je endomorfismus prostoru V , jehož maticí vzhledem k bázi M je matice \overline{A} . Homomorfismus g je samoadjungovaný, neboť \overline{A} je hermitovská (viz 29.5); proto existuje podle věty 29.8 ortonormální báze N prostoru V složená z vlastních vektorů endomorfismu g ; nechť D je matice endomorfismu g vzhledem k bázi N .

Matice D je reálná diagonální matice,

$$D = C^{-1} \overline{A} C,$$

kde C je matice přechodu od báze N k bázi M . Protože je C maticí přechodu od jedné ortonormální báze ke druhé ortonormální bázi, je podle 27.10 unitární, tj. $\overline{C}^{-1} = C^T$ (viz 27.8), takže je

$$D = \overline{D} = C^T \overline{A} C.$$

Protože je matice D maticí formy f vzhledem k bázi N (viz 23.7, resp. 24.7), je báze N polární vůči formě f . \square

Maticová modifikace předchozího důkazu. Nechť M je ortonormální báze prostoru V a A matice formy f vzhledem k bázi M . Protože je f hermitovská, je také A hermitovská. Podle důsledku 29.9 existuje unitární matice B taková, že $D = B^{-1} A B$ je reálná diagonální matice. Protože je $B^{-1} = \overline{B}^T$ (viz 27.8), je

$$D = \overline{B}^T A B = C^T \overline{A} C,$$

kde $C = \overline{B}$ je rovněž unitární matice. Matice C je maticí přechodu od nějaké ortonormální báze N k ortonormální bázi M (viz 27.10). Reálná diagonální matice D je maticí formy f vzhledem k bázi N (viz 23.7, resp. 24.7), tj. N je ortonormální báze, která je polární vůči formě f . \square

Endomorfismus g z předchozího důkazu budeme nazývat *samoadjungovaným endomorfismem* přidruženým k hermitovské seskvilineární (symetrické bilineární) formě f . Označíme-li $\lambda_1, \dots, \lambda_n$ prvky stojící na diagonále matice D a položíme-li

$$\langle x \rangle_N = (x_1, x_2, \dots, x_n), \quad \langle y \rangle_N = (y_1, y_2, \dots, y_n),$$

potom rovnost

$$f(x, y) = \lambda_1 x_1 \overline{y_1} + \lambda_2 x_2 \overline{y_2} + \dots + \lambda_n x_n \overline{y_n}$$

je analytické vyjádření formy f vzhledem k bázi N . Přitom jsou $\lambda_1, \lambda_2, \dots, \lambda_n$ vlastní čísla formy f (resp. matice A , resp. matice \overline{A} , resp. endomorfismu g) a báze $N = \{v_1, v_2, \dots, v_n\}$ je složena z vlastních vektorů samoadjungovaného endomorfismu g přidruženého k formě f . Podle definice analytického vyjádření je každé λ_i hodnotou formy f v i -tém vektoru báze N , tj.

$$f(v_i, v_i) = \lambda_i;$$

forma f nabývá svých vlastních čísel ve vlastních vektorech přidruženého endomorfismu.

Vzhledem k tomu, že skalární součin je hermitovská seskvilineární (symetrická bilineární) forma, hovoří věta 30.2 o existenci báze prostoru V , která je polární vůči dvěma formám (skalární součin, forma f), vůči prvním z nich je dokonce normální.

30.3. Extrémální vlastnosti. *Nechť V je komplexní (reálný) unitární prostor konečné dimenze a f hermitovská seskvilineární (symetrická bilineární) forma na prostoru V . Potom pro každý normovaný vektor $x \in V$ je*

$$\lambda_{min} \leq f(x, x) \leq \lambda_{max},$$

kde λ_{min} je nejmenší a λ_{max} největší vlastní číslo formy f .

Důkaz. Jestliže je $N = \{v_1, \dots, v_n\}$ ortonormální báze prostoru V , která je vůči formě f polární, potom je pro každý vektor $x \in V$, $\langle x \rangle_N = (x_1, \dots, x_n)$,

$$f(x, x) = \lambda_1 |x_1|^2 + \lambda_2 |x_2|^2 + \dots + \lambda_n |x_n|^2,$$

kde $\lambda_1, \lambda_2, \dots, \lambda_n$ jsou vlastní čísla formy f . Jestliže je vektor x normovaný, pak je $\|x\|^2 = \sum_{i=1}^n |x_i|^2 = 1$ (viz 26.29) a

$$f(x, x) = \sum_{i=1}^n \lambda_i |x_i|^2 \geq \lambda_{min} \sum_{i=1}^n |x_i|^2 = \lambda_{min},$$

$$f(x, x) = \sum_{i=1}^n \lambda_i |x_i|^2 \leq \lambda_{max} \sum_{i=1}^n |x_i|^2 = \lambda_{max}. \quad \square$$

Množině všech normovaných (jednotkových) vektorů prostoru V někdy říkáme *jednotková sféra*. Forma f tedy na jednotkové sféře nabývá maxima a minima a tyto hodnoty jsou rovny největšímu a nejmenšímu vlastnímu číslu formy f .

Poznamenejme, že pro každé číslo α , pro které je $|\alpha| = 1$, a každý normovaný vektor x je

$$f(\alpha x, \alpha x) = |\alpha|^2 \cdot f(x, x) = f(x, x), \quad \|\alpha x\| = |\alpha|^2 \|x\| = 1,$$

v reálném případě

$$f(-x, -x) = f(x, x),$$

tj. forma f nabývá maxima a minima na jednotkové sféře „vícekrát“. Je-li V reálný unitární prostor, pak forma f nabývá na jednotkové sféře maxima, resp. minima alespoň dvakrát; právě dvakrát v tom případě, kdy jsou příslušné podprostory vlastních vektorů jednodimenzionální.

Tvrzení věty 30.3 můžeme modifikovat takto: pro libovolný nenulový vektor $x \in V$ je

$$\lambda_{min} \leq \frac{f(x, x)}{\|x\|^2} \leq \lambda_{max},$$

resp. v analytickém vyjádření vzhledem k nějaké bázi N

$$\lambda_{min} \leq \frac{\langle x \rangle_N \cdot A \cdot \overline{\langle x \rangle}_N^T}{\|x\|^2} \leq \lambda_{max}.$$

Odtud už je jen krůček k maticovému vyjádření:

30.4. Věta. *Nechť $A = (a_{ij})$ je hermitovská, resp. reálná symetrická matice řádu n a λ_{min} a λ_{max} její nejmenší a největší vlastní číslo. Potom pro každý vektor $x = (x_1, \dots, x_n)$ je*

$$\lambda_{min} \leq \frac{\sum_{i,j=1}^n a_{ij} x_i \bar{x}_j}{\sum_{i=1}^n |x_i|^2} \leq \lambda_{max}. \quad \square$$

Výše uvedenou definici 30.1 a věty 30.2 a 30.3 můžeme přirozeným způsobem přeformulovat pro kvadratické formy podobným způsobem, jako byly v paragrafech 23, 24 a 25 z výsledků dokázaných pro bilineární, resp. seskvilineární formy získány výsledky o kvadratických formách (prvního, resp. druhého druhu). Využijeme toho v následujících příkladech.

30.5. Příklady.

(i) Hermitovská seskvilineární forma f na unitárním prostoru \mathbb{C}^2 se standardním skalárním součinem má vzhledem ke kanonické bázi analytické vyjádření

$$f(x, y) = ix_1 \bar{y}_2 - ix_2 \bar{y}_1.$$

Maticí formy f vzhledem ke kanonické bázi je hermitovská matice

$$A = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix},$$

kteřá má charakteristický (a minimální) polynom $\lambda^2 - 1$ a vlastní čísla 1 a -1 . Samoadjungovaný endomorfismus g prostoru \mathbb{C}^2 , který je přidružený k formě f , má vzhledem ke kanonické bázi matici

$$\bar{A} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

tj. zobrazuje vektor (x_1, x_2) na vektor $(-ix_2, ix_1)$. Normovanými vlastními vektory endomorfismu g příslušnými k vlastním číslům $1, -1$ jsou vektory

$$v_1 = \frac{1}{\sqrt{2}}(-i, 1) \quad \text{a} \quad v_2 = \frac{1}{\sqrt{2}}(i, 1).$$

Báze $N = \{v_1, v_2\}$ je ortonormální bázi prostoru \mathbb{C}^2 , která je polární vůči formě f . Forma f i přidružený endomorfismus g mají vzhledem k bázi N matici

$$D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

tj. analytické vyjádření formy f vzhledem k bázi N má tvar

$$f(x, y) = \xi_1 \bar{\eta}_1 - \xi_2 \bar{\eta}_2,$$

kde

$$\langle x \rangle_N = (\xi_1, \xi_2), \quad \langle y \rangle_N = (\eta_1, \eta_2);$$

forma f je indefinitní. Matice A se transformuje na matici D pomocí vztahu

$$D = C^T A \bar{C},$$

kde unitární matice C je maticí přechodu od báze N ke kanonické bázi, tj.

$$C = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & i \\ 1 & 1 \end{pmatrix};$$

je tedy

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & i \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}.$$

Vlastních čísel $1, -1$ nabývá forma f ve vlastních vektorech přidruženého endomorfismu g , tj. $f(v_1, v_1) = 1, f(v_2, v_2) = -1$. Poznamenejme, že forma f nabývá hodnot 1 a -1 i ve vektorech $\alpha v_1, \alpha v_2$, kde $|\alpha| = 1$.

Pro každý normovaný vektor $x \in \mathbb{C}^2$ je

$$-1 \leq f(x, x) \leq 1 ,$$

tj.

$$-1 \leq ix_1\bar{x}_2 - ix_2\bar{x}_1 \leq 1 ,$$

resp. pro každý nenulový vektor $y \in \mathbb{C}^2$ je

$$-1 \leq \frac{f(y, y)}{\|y\|^2} \leq 1 ,$$

tj.

$$-1 \leq \frac{iy_1\bar{y}_2 - iy_2\bar{y}_1}{|y_1|^2 + |y_2|^2} \leq 1 .$$

Kvadratická forma q určená formou f je hermitovská, má vzhledem ke kanonické bázi matici A . Vzhledem k ortonormální bázi N má analytické vyjádření

$$q(x) = |\xi_1|^2 - |\xi_2|^2$$

a pro každý normovaný vektor $x \in \mathbb{C}^2$ je

$$-1 \leq q(x) \leq 1 .$$

(ii) Reálná symetrická forma f na reálném unitárním prostoru \mathbb{R}^3 se standardním skalárním součinem má vzhledem ke kanonické bázi analytické vyjádření

$$f(x, y) = x_1y_1 - x_1y_2 - x_2y_1 + 2x_2y_2 - x_2y_3 - x_3y_2 + x_3y_3 .$$

Maticí formy f vzhledem ke kanonické bázi je symetrická matice

$$A = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix} ;$$

charakteristický polynom matice A , resp. formy f je polynom $\lambda^3 - 4\lambda^2 + 3\lambda$; vlastními čísly matice A , resp. formy f jsou čísla $0, 1, 3$. Samoadjungovaný endomorfismus g prostoru \mathbb{R}^3 přidružený k formě f má vzhledem ke kanonické bázi matici A , tj. zobrazuje vektor (x_1, x_2, x_3) na vektor

$$(x_1 - x_2, -x_1 + 2x_2 - x_3, -x_2 + x_3) .$$

Normovanými vlastními vektory endomorfismu g příslušnými k vlastním číslům 0, 1, 3 jsou vektory

$$v_1 = \frac{1}{\sqrt{3}}(1, 1, 1), \quad v_2 = \frac{1}{\sqrt{2}}(1, 0, -1), \quad v_3 = \frac{1}{\sqrt{6}}(1, -2, 1).$$

Podle věty 29.8 je $N = \{v_1, v_2, v_3\}$ ortonormální bází prostoru \mathbb{R}^3 a podle důkazu věty 30.2 je tato báze polární vůči formě f . Forma f i přidružený endomorfismus g mají vzhledem k bázi N matici

$$D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

tj. analytické vyjádření formy f vzhledem k bázi N má tvar

$$f(x, y) = \xi_2 \eta_2 + 3\xi_3 \eta_3,$$

kde

$$\langle x \rangle_N = (\xi_1, \xi_2, \xi_3), \quad \langle y \rangle_N = (\eta_1, \eta_2, \eta_3);$$

forma f je pozitivně semidefinitní. Matice A se transformuje na matici D pomocí vztahu

$$D = C^T A C,$$

kde ortogonální matice C je maticí přechodu od báze N ke kanonické bázi, tj.

$$C = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & \frac{-2}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \end{pmatrix}.$$

Vlastních čísel 0, 1, 3 nabývá forma f v normovaných vlastních vektorech přidruženého endomorfismu g , tj.

$$f(v_1, v_1) = f(-v_1, -v_1) = 0, \quad f(v_2, v_2) = f(-v_2, -v_2) = 1,$$

$$f(v_3, v_3) = f(-v_3, -v_3) = 3.$$

Pro každý normovaný vektor $x \in \mathbb{R}^3$ je

$$0 \leq f(x, x) \leq 3,$$

tj.

$$0 \leq x_1^2 - 2x_1x_2 + 2x_2^2 - 2x_2x_3 + x_3^2 \leq 3,$$

resp. pro každý nenulový vektor $y \in \mathbb{R}^3$ je

$$0 \leq \frac{f(y, y)}{\|y\|^2} \leq 3 ,$$

tj.

$$0 \leq \frac{y_1^2 - 2y_1y_2 + 2y_2^2 - 2y_2y_3 + y_3^2}{y_1^2 + y_2^2 + y_3^2} \leq 3 .$$

(iii) Kvadratická forma q na prostoru \mathbb{R}^2 se standardním skalárním součinem má vzhledem ke kanonické bázi analytické vyjádření

$$q(x) = 2x_1^2 - 2x_1x_2 + 2x_2^2 .$$

Maticí formy q vzhledem ke kanonické bázi prostoru \mathbb{R}^2 je symetrická matice

$$A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} ;$$

charakteristickým a minimálním polynomem matice A , resp. formy q je polynom $\lambda^2 - 4\lambda + 3$, vlastními čísly matice A , resp. formy q jsou čísla 1, 3. Samoadjungovaný endomorfismus g prostoru \mathbb{R}^2 přidružený k formě q má vzhledem ke kanonické bázi maticí A , tj. zobrazuje vektor (x_1, x_2) na vektor $(2x_1 - x_2, -x_1 + 2x_2)$. Normovanými vlastními vektory endomorfismu g příslušnými k vlastním číslům 1 a 3 jsou vektory

$$v_1 = \frac{1}{\sqrt{2}}(1, 1) , \quad v_2 = \frac{1}{\sqrt{2}}(1, -1) .$$

Kvadratická forma q i přidružený endomorfismus g mají vzhledem k ortonormální bázi $N = \{v_1, v_2\}$ maticí

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} ,$$

tj. analytické vyjádření formy q vzhledem k N má tvar

$$q(x) = \xi_1^2 + 3\xi_2^2 ,$$

kde $\langle x \rangle_N = (\xi_1, \xi_2)$; forma q je pozitivně definitní. Dále je

$$D = C^T A C ,$$

kde ortogonální matice

$$C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

je maticí přechodu od báze N ke kanonické bázi prostoru \mathbb{R}^2 . Pro každý normovaný vektor $x \in \mathbb{R}^2$ je

$$1 \leq q(x) \leq 3,$$

forma q nabývá na jednotkové sféře maxima (hodnoty 3) ve vektorech $\pm \frac{1}{\sqrt{2}}(1, -1)$ a minima (hodnoty 1) ve vektorech $\pm \frac{1}{\sqrt{2}}(1, 1)$.

Poznamenejme, že symetrickými úpravami matice A , které jsme prováděli dříve, nezískáme některé důležité výsledky, kterých bylo dosaženo v tomto paragrafu výše uvedeným postupem:

$$\left(\begin{array}{cc|cc} 2 & -1 & 1 & 0 \\ -1 & 2 & 0 & 1 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 0 & 6 & 1 & 2 \end{array} \right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 1 & \frac{1}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{array} \right)$$

Odtud vyplývá jen to, že forma q je pozitivně definitní a že báze

$$K = \left\{ \left(\frac{1}{\sqrt{2}}, 0 \right), \left(\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}} \right) \right\}$$

je normální vůči formě f . Nenašli jsme však interval, ve kterém leží hodnoty formy q na jednotkové sféře, ani vektory, ve kterých tato forma nabývá na jednotkové sféře maxima a minima, tj. vlastní čísla formy q a příslušné vlastní vektory přidruženého endomorfismu. Navíc byla forma q původně vyjádřena vzhledem ke kanonické bázi, která je ortonormální, báze K však ortonormální není. Skalární součin tedy nemůžeme počítat standardním způsobem pomocí souřadnic vzhledem k bázi K .

Rovněž hermitovské úpravy hermitovské matice, kterou jsme vyšetřovali např. v příkladu (i), nepostačují ke zjištění výše uvedených skutečností.

31. PSEUDOINVERZNÍ HOMOMORFISMY A MATICE

V desátém paragrafu jsme viděli, že k izomorfismům existují *inverzní izomorfismy* (viz 10.13) a že k epimorfismům, resp. k monomorfismům existují jakési homomorfismy, které bychom mohli nazývat *inverzní zprava*, resp. *inverzní zleva* (viz 10.14 a 10.15). Víme též, že inverzní izomorfismy existují pouze k izomorfismům a že homomorfismy inverzní zprava, resp. zleva existují pouze k epimorfismům, resp. monomorfismům. Pojem inverzního izomorfismu, resp. homomorfismu inverzního zprava (zleva) nyní zobecníme. Nejprve budeme uvažovat obecné vektorové prostory bez skalárního součinu.

31.1. Definice. Necht U, V jsou vektorové prostory nad tělesem T a $f : U \rightarrow V$ homomorfismus. Homomorfismus $g : V \rightarrow U$ se nazývá *pseudoinverzní homomorfismus* k homomorfismu f , jestliže je $fgf = f$.

Povšimněme si, že k nulovému homomorfismu prostoru U do prostoru V je pseudoinverzní každý homomorfismus g prostoru V do prostoru U .

31.2. Věta. Necht U, V jsou vektorové prostory nad tělesem T , $f : U \rightarrow V$ a $g : V \rightarrow U$ homomorfismy. Potom platí:

- (i) Jestliže je f epimorfismus, potom je g pseudoinverzní k f právě tehdy, když je $fg = 1_V$.
- (ii) Jestliže je f monomorfismus, potom je g pseudoinverzní k f právě tehdy, když je $gf = 1_U$.
- (iii) Jestliže je f izomorfismus, potom je g pseudoinverzní k f právě tehdy, když je $g = f^{-1}$.

Důkaz. Podle věty 10.14 je epimorfismem možno krátit zprava. Rovnost $fgf = f$ je tedy ekvivalentní s rovností $fg = 1_V$. Tvrzení (i) je dokázáno, tvrzení (ii) se dokáže obdobně pomocí věty 10.15. Tvrzení (iii) je důsledkem tvrzení (i) a (ii). \square

Pojem pseudoinverzního homomorfismu je tedy přirozeným zobecněním pojmu inverzního izomorfismu i pojmu homomorfismu inverzního zprava či zleva. Z předchozích tvrzení (a z vět 10.13, 10.14 a 10.15) zároveň vyplývá existence pseudoinverzního homomorfismu k izomorfismům, epimorfismům a monomorfismům. Zanedlouho však dokážeme existenci pseudoinverzního homomorfismu v obecném případě (viz 31.7).

31.3. Základní vlastnosti pseudoinverzních homomorfismů. Necht U, V jsou vektorové prostory nad tělesem T , $f : U \rightarrow V$ homomorfismus a $g : V \rightarrow U$ pseudoinverzní homomorfismus k homomorfismu f . Potom platí:

- (i) $r(g) \geq r(f) = r(fg) = r(gf)$;
- (ii) je-li f epimorfismus, je g monomorfismus;
- (iii) je-li f monomorfismus, je g epimorfismus;
- (iv) $\text{Im } f = \{v \in V; fg(v) = v\}$;

- (v) $\text{Ker } f = \{u - gf(u); u \in U\}$;
- (vi) úplný vzor vektoru $v \in \text{Im } f$ je $\{g(v) + u - gf(u); u \in U\}$;
- (vii) $U = \text{Ker } f + \text{Im } g$;
- (viii) $O = \text{Ker } g \cap \text{Im } f$;
- (ix) jestliže je $\varphi \in \text{Aut } U$ a $\psi \in \text{Aut } V$, potom je $\varphi^{-1}g\psi^{-1}$ pseudoinverzní homomorfismus k homomorfismu $\psi f \varphi$;
- (x) všechny pseudoinverzní homomorfismy k homomorfismu f mají tvar $g + \varphi - gf\varphi fg$, kde $\varphi \in \text{Hom}(V, U)$;
- (xi) všechny pseudoinverzní homomorfismy k homomorfismu f mají tvar $g + \varphi(1_V - fg) + (1_U - gf)\psi$, kde $\varphi, \psi \in \text{Hom}(V, U)$.

Důkaz. Zřejmě je

$$r(g) \geq r(fg) \geq r(fgf) = r(f) \geq r(fg) ,$$

$$r(g) \geq r(gf) \geq r(fgf) = r(f) \geq r(gf) ;$$

odtud vyplývá tvrzení (i).

Tvrzení (ii) a (iii) vyplývají z 31.2 a 10.12.

(iv) Jestliže pro vektor $v \in V$ je $v = fg(v)$, potom je zřejmě $v \in \text{Im } f$. Jestliže je $v \in \text{Im } f$, tj. $v = f(u)$ pro nějaký vektor $u \in U$, pak je $v = f(u) = fgf(u) = fg(v)$.

(v) Jestliže je $u \in U$, potom je $f(u - gf(u)) = f(u) - fgf(u) = o$, takže

$$u - gf(u) \in \text{Ker } f .$$

Jestliže je $u \in \text{Ker } f$, je $f(u) = o$ a tedy $u = u - gf(u)$.

(vi) Jestliže je $v \in \text{Im } f$, potom je podle (iv) $v = fg(v)$, tj. vektor $g(v) \in U$ je vzorem vektoru v při homomorfismu f . Úplný vzor vektoru v je tedy

$$g(v) + \text{Ker } f = \{g(v) + u - gf(u); u \in U\} .$$

(vii) Pro každý vektor $u \in U$ je

$$u = (u - gf(u)) + gf(u) \in \text{Ker } f + \text{Im } g .$$

(viii) Jestliže je $v \in \text{Ker } g \cap \text{Im } f$, potom je podle (iv)

$$v = fg(v) = f(o) = o .$$

(ix) Je totiž

$$\psi f \varphi \cdot \varphi^{-1} g \psi^{-1} \cdot \psi f \varphi = \psi f \varphi .$$

(x) Pomocí distributivního zákona zjistíme, že je

$$f(g + \varphi - gf\varphi fg)f = f ,$$

takže $g + \varphi - gf\varphi fg$ je pseudoinverzní homomorfismus k homomorfismu f . Předpokládejme naopak, že g' je nějaký pseudoinverzní homomorfismus k homomorfismu f . Je tedy $fg'f = f$ a $fgf = f$; odtud je $f(g' - g)f = 0$ a $gf(g' - g)fg = 0$. Platí tedy rovnost

$$g' = g + (g' - g) - gf(g' - g)fg .$$

Položíme-li $g' - g = \varphi$, je $g' = g + \varphi - gf\varphi fg$.

(xi) Pomocí distributivního zákona zjistíme, že je

$$f[g + \varphi(1_V - fg) + (1_U - gf)\psi]f = f ,$$

takže $g + \varphi(1_V - fg) + (1_U - gf)\psi$ je pseudoinverzní homomorfismus k homomorfismu f . Předpokládejme naopak, že g' je nějaký pseudoinverzní homomorfismus k homomorfismu f . Podle (x) je

$$g' = g + \varphi - gf\varphi fg, \quad \text{kde } \varphi \in \text{Hom}(V, U) .$$

Je tedy

$$g' = g + \varphi - \varphi fg + \varphi fg - gf\varphi fg = g + \varphi(1_V - fg) + (1_U - gf)\psi ,$$

kde $\psi = \varphi fg$. \square

Jestliže je homomorfismus f epimorfismem nebo monomorfismem, potom se výrazy pro popis všech pseudoinverzních homomorfismů v tvrzeních (x) a (xi) zjednoduší (a splynou), neboť je buď $fg = 1_V$ nebo $gf = 1_U$.

31.4. Definice. Necht U, V jsou vektorové prostory nad tělesem T . Homomorfismy $f : U \rightarrow V$ a $g : V \rightarrow U$ se nazývají *navzájem pseudoinverzní*, jestliže je

$$fgf = f \quad \text{a} \quad gfg = g .$$

31.5. Věta. Necht U, V jsou vektorové prostory nad tělesem T , $f : U \rightarrow V$ homomorfismus a $g : V \rightarrow U$ homomorfismus pseudoinverzní k homomorfismu f . Jestliže je f epimorfismus nebo monomorfismus, potom jsou f a g navzájem pseudoinverzní.

Důkaz. Jestliže je f epimorfismus, je $fg = 1_V$ (viz 31.2) a tedy $gfg = g$. Jestliže je f monomorfismus, je $gf = 1_U$ a tedy opět $gfg = g$. \square

31.6. Věta. *Nechť U, V jsou vektorové prostory nad tělesem T a $f : U \rightarrow V, g : V \rightarrow U$ navzájem pseudoinverzní homomorfismy. Potom platí:*

- (i) $f = 0$ právě tehdy, když $g = 0$,
- (ii) $r(f) = r(g)$,
- (iii) f je monomorfismus, právě když je g epimorfismus,
- (iv) $U = \text{Ker } f \oplus \text{Im } g$,
- (v) $V = \text{Ker } g \oplus \text{Im } f$;
- (vi) Homomorfismus f zobrazuje $\text{Im } g$ izomorfně na $\text{Im } f$, homomorfismus g zobrazuje $\text{Im } f$ izomorfně na $\text{Im } g$ a f a g jsou na těchto podprostorech navzájem inverzní.

Důkaz. Tvrzení (i) plyne ihned z definice 31.4. Tvrzení (ii) plyne z 31.3(i), tvrzení (iii) z 31.3(ii)–(iii), tvrzení (iv) a (v) z 31.3(vii)–(viii) a tvrzení (vi) z 31.3(iv); pro každé $v \in \text{Im } f$ je $fg(v) = v$, pro každé $u \in \text{Im } g$ je $gf(u) = u$. \square

31.7. Věta. *Nechť U, V jsou vektorové prostory nad tělesem T . Ke každému homomorfismu $f : U \rightarrow V$ existuje pseudoinverzní homomorfismus $g : V \rightarrow U$, resp. takový homomorfismus $g : V \rightarrow U$, že homomorfismy f a g jsou navzájem pseudoinverzní.*

Důkaz. Nechť f je homomorfismus prostoru U do prostoru V . Zvolme nějaký direktní doplněk U' podprostoru $\text{Ker } f$ v prostoru U a nějaký direktní doplněk V' podprostoru $\text{Im } f$ v prostoru V (viz 9.5). Je tedy

$$U = \text{Ker } f \oplus U', \quad V = \text{Im } f \oplus V'.$$

Homomorfismus f zobrazuje izomorfně podprostor U' na podprostor $\text{Im } f$ (viz např. věta o hodnotě a defektu). Jestliže je g homomorfismus prostoru V do prostoru U , který zobrazuje $\text{Im } f$ na U' inverzně k f a na V' je definován libovolně, potom je zřejmě $fgf = f$ a g je pseudoinverzní k f . Jestliže g zobrazuje navíc celý podprostor V' na nulový vektor prostoru U , je ještě $gfg = g$. \square

Myšlenka předchozího důkazu je založena na zjištěních zformulovaných v tvrzeních 31.3(iv), (vii), (viii), resp. 31.6(iv), (v), (vi).

Z důkazu je vidět, že pseudoinverzní homomorfismus g k homomorfismu f není obecně určen jednoznačně. Není určen jednoznačně ani v tom případě, kdy mají být f a g navzájem pseudoinverzní. K podprostorům $\text{Ker } f$ a $\text{Im } f$ je totiž možno volit různé direktní doplňky; na této volbě pak závisí definice homomorfismu g .

31.8. Příklad. Homomorfismus f prostoru \mathbb{R}^3 do prostoru \mathbb{R}^4 zobrazuje vektor (x, y, z) na vektor

$$(x + y + 2z, x - 2y + z, 3y + z, 2x - y + 3z).$$

Snadno se vypočte, že $\text{Ker } f = [(5, 1, -3)]$. Jedním z direktních doplňků tohoto podprostoru v prostoru \mathbb{R}^3 je podprostor $[(1, 0, 0), (0, 1, 0)]$. Obrazem tohoto podprostoru je $\text{Im } f$; jelikož

$$\begin{aligned} (1, 0, 0) &\longrightarrow (1, 1, 0, 2), \\ (0, 1, 0) &\longrightarrow (1, -2, 3, -1), \end{aligned}$$

je $\text{Im } f = [(1, 1, 0, 2), (1, -2, 3, -1)]$. Direktním doplňkem podprostoru $\text{Im } f$ v prostoru \mathbb{R}^4 je např. podprostor $[(1, 0, 0, 0), (0, 1, 0, 0)]$. Definujme nyní homomorfismus g prostoru \mathbb{R}^4 do prostoru \mathbb{R}^3 tímto přiřazením:

$$\begin{aligned} (1, 1, 0, 2) &\longrightarrow (1, 0, 0) , \\ (1, -2, 3, -1) &\longrightarrow (0, 1, 0) , \\ (1, 0, 0, 0) &\longrightarrow (0, 0, 0) , \\ (0, 1, 0, 0) &\longrightarrow (0, 0, 0) . \end{aligned}$$

Odtud

$$\begin{aligned} (0, 0, 0, 1) &\longrightarrow \left(\frac{1}{2}, 0, 0\right) , \\ (0, 0, 1, 0) &\longrightarrow \left(\frac{1}{6}, \frac{1}{3}, 0\right) , \end{aligned}$$

takže

$$(a, b, c, d) \longrightarrow \left(\frac{1}{6}c + \frac{1}{2}d, \frac{1}{3}c, 0\right) ;$$

homomorfismus g tedy zobrazí vektor (a, b, c, d) na vektor

$$\frac{1}{6}(c + 3d, 2c, 0) .$$

Prověřením rovností $fgf = f$ a $gfg = g$ se přesvědčíme, že homomorfismy f a g jsou navzájem pseudoinverzní.

Poznamenejme ještě, že pokud bychom vektory báze direktního doplňku podprostoru $\text{Im } f$, tj. vektory $(1, 0, 0, 0), (0, 1, 0, 0)$, zobrazili zcela libovolně, dostali bychom nějaký pseudoinverzní homomorfismus h k homomorfismu f ; homomorfismy f a h by však nemusely být navzájem pseudoinverzní.

Definujme např. homomorfismus h přiřazením

$$\begin{aligned} (1, 1, 0, 2) &\longrightarrow (1, 0, 0) , \\ (1, -2, 3, -1) &\longrightarrow (0, 1, 0) , \\ (1, 0, 0, 0) &\longrightarrow (1, 1, 0) , \\ (0, 1, 0, 0) &\longrightarrow (0, 0, 1) . \end{aligned}$$

Odtud

$$\begin{aligned} (1, 0, 0, 0) &\longrightarrow (1, 1, 0) , \\ (0, 1, 0, 0) &\longrightarrow (0, 0, 1) , \\ (0, 0, 1, 0) &\longrightarrow \left(-\frac{1}{3}, -\frac{1}{6}, \frac{1}{2}\right) , \\ (0, 0, 0, 1) &\longrightarrow \left(0, -\frac{1}{2}, -\frac{1}{2}\right) , \end{aligned}$$

takže homomorfismus h zobrazí vektor (a, b, c, d) na vektor

$$\frac{1}{6}(6a - 2c, 6a - c - 3d, 6b + 3c - 3d) .$$

Prověřením rovnosti $fhf = f$ se přesvědčíme, že homomorfismus h je pseudoinverzní k homomorfismu f . Snadno se také přesvědčíme, že f není pseudoinverzní k h .

Pokud bychom zvolili jiné direktní doplňky podprostorů $\text{Ker } f$ a $\text{Im } f$, dostali bychom jiný homomorfismus g' , takový, že f a g' jsou navzájem pseudoinverzní. Pišme např.

$$\mathbb{R}^3 = \text{Ker } f \oplus [(0, 1, 0), (0, 0, 1)] , \quad \mathbb{R}^4 = \text{Im } f \oplus [(0, 0, 1, 0), (0, 0, 0, 1)]$$

a definujme homomorfismus g' prostoru \mathbb{R}^4 do prostoru \mathbb{R}^3 tímto přiřazením:

$$\begin{aligned} (1, -2, 3, -1) &\longrightarrow (0, 1, 0) , \\ (2, 1, 1, 3) &\longrightarrow (0, 0, 1) , \\ (0, 0, 1, 0) &\longrightarrow (0, 0, 0) , \\ (0, 0, 0, 1) &\longrightarrow (0, 0, 0) . \end{aligned}$$

Odtud

$$\begin{aligned} (1, 0, 0, 0) &\longrightarrow (0, \frac{1}{5}, \frac{2}{5}) , \\ (0, 1, 0, 0) &\longrightarrow (0, -\frac{2}{5}, \frac{1}{5}) , \end{aligned}$$

takže

$$(a, b, c, d) \longrightarrow (0, \frac{1}{5}a - \frac{2}{5}b, \frac{2}{5}a + \frac{1}{5}b) ;$$

homomorfismus g' tedy zobrazí vektor (a, b, c, d) na vektor

$$\frac{1}{5}(0, a - 2b, 2a + b) .$$

Prověřením rovností $fg'f = f$ a $g'fg' = g'$ se přesvědčíme, že homomorfismy f a g' jsou navzájem pseudoinverzní.

31.9. Definice. Necht U, V jsou (reálné nebo komplexní) unitární prostory, homomorfismy $f : U \rightarrow V$ a $g : V \rightarrow U$ necht jsou navzájem pseudoinverzní. Řekneme, že dvojice f, g je *Mooreova–Penroseova*, jestliže je

$$\text{Im } g = (\text{Ker } f)^\perp \quad \text{a} \quad \text{Ker } g = (\text{Im } f)^\perp .$$

Jsou-li homomorfismy f a g navzájem pseudoinverzní, je podle věty 31.6

$$U = \text{Ker } f \oplus \text{Im } g \quad \text{a} \quad V = \text{Ker } g \oplus \text{Im } f .$$

Dvojice f, g je Mooreova–Penroseova právě tehdy, když podprostory $\text{Ker } f$ a $\text{Im } g$ jsou navzájem ortogonálními doplňky v prostoru U a podprostory $\text{Ker } g$ a $\text{Im } f$ jsou navzájem ortogonálními doplňky v prostoru V .

31.10. Věta. Necht U, V jsou (reálné nebo komplexní) unitární prostory a homomorfismy $f : U \rightarrow V, g : V \rightarrow U$ necht jsou Mooreovou–Penroseovou dvojicí navzájem pseudoinverzních homomorfismů. Potom platí:

- (i) Pro každé $v \in \text{Im } f$ má vektor $g(v)$ nejmenší normu ze všech vektorů vektoru v při homomorfismu f .
- (ii) Pro každé $v \in V$ je $fg(v)$ kolmým průmětem vektoru v na podprostor $\text{Im } f$ a vektor $g(v)$ má nejmenší normu ze všech vektorů vektoru $fg(v)$.

Důkaz.

(i) Libovolný vektor $v \in \text{Im } f$ má tvar $x = g(v) + u - gf(u)$, kde $u \in U$ (viz 31.3(vi)). Protože $g(v) \in \text{Im } g$ a $u - gf(u) \in \text{Ker } f = (\text{Im } g)^\perp$, dostáváme podle Pythagorovy věty

$$\|x\|^2 = \|g(v)\|^2 + \|u - gf(u)\|^2 \geq \|g(v)\|^2 .$$

Je-li $x \neq g(v)$, je $u - gf(u) \neq o$ a tedy $\|x\| > \|g(v)\|$.

(ii) Pro každý vektor $v \in V$ je $v = fg(v) + (v - fg(v))$ ortogonální rozklad vektoru v , neboť $fg(v) \in \text{Im } f$ a $v - fg(v) \in \text{Ker } g = (\text{Im } f)^\perp$. Ostatní je důsledkem tvrzení (i). \square

31.11. Věta. *Nechť U, V jsou (reálné nebo komplexní) unitární prostory a nechť $f : U \rightarrow V, g : V \rightarrow U$ jsou navzájem pseudoinverzní homomorfismy. Dvojice f, g je Mooreova–Penroseova právě tehdy, když jsou homomorfismy fg a gf samoadjungované.*

Důkaz. Předpokládejme nejprve, že f, g je Mooreova–Penroseova dvojice navzájem pseudoinverzních homomorfismů. Proto je

$$U = \text{Ker } f \oplus \text{Im } g, \quad \text{kde} \quad \text{Im } g = (\text{Ker } f)^\perp .$$

Nechť $x, y \in U$; pišme $x = x_1 + x_2, y = y_1 + y_2$, kde $x_1, y_1 \in \text{Ker } f$ a $x_2, y_2 \in \text{Im } g$; nechť dále $v_2, w_2 \in V$ a $g(v_2) = x_2, g(w_2) = y_2$. Nyní je

$$\begin{aligned} (gf(x) | y) &= (gf(x_2) | y_2) = (gf g(v_2) | g(w_2)) = (g(v_2) | gf g(w_2)) = \\ &= (x_2 | gf(y_2)) = (x_1 + x_2 | gf(y_1 + y_2)) = (x | gf(y)) , \end{aligned}$$

tj. endomorfismus gf je samoadjungovaný. Stejným způsobem dokážeme, že je samoadjungovaný i endomorfismus fg ; použijeme k tomu rovnost

$$V = \text{Ker } g \oplus \text{Im } f, \quad \text{kde} \quad \text{Ker } g = (\text{Im } f)^\perp .$$

Předpokládejme naopak, že jsou endomorfismy fg a gf samoadjungované. Protože jsou homomorfismy f a g navzájem pseudoinverzní, je

$$U = \text{Ker } f \oplus \text{Im } g, \quad V = \text{Ker } g \oplus \text{Im } f .$$

Potřebujeme tedy dokázat rovnosti

$$\text{Im } g = (\text{Ker } f)^\perp, \quad \text{Ker } g = (\text{Im } f)^\perp ;$$

k tomu účelu stačí dokázat, že pro každé $x_1 \in \text{Ker } f$ a $x_2 \in \text{Im } g$ je $(x_1 | x_2) = 0$ a pro každé $y_1 \in \text{Ker } g$ a $y_2 \in \text{Im } f$ je $(y_1 | y_2) = 0$. Dokážeme první rovnost. Nechť $z_2 \in V$ a $g(z_2) = x_2$. Potom je

$$\begin{aligned} (x_1 | x_2) &= (x_1 | g(z_2)) = (x_1 | gf g(z_2)) = (x_1 | gf(x_2)) = \\ &= (gf(x_1) | x_2) = (o | x_2) = 0 . \end{aligned}$$

Stejně se dokáže rovnost $(y_1 | y_2) = 0$. \square

31.12. Věta. *Nechť U, V jsou unitární prostory konečných dimenzí. Ke každému homomorfismu $f : U \rightarrow V$ existuje právě jediný homomorfismus $g : V \rightarrow U$, takový, že f, g je Mooreova–Penroseova dvojice navzájem pseudoinverzních homomorfismů.*

Důkaz. Nechť je dán homomorfismus $f : U \rightarrow V$, nechť U' je ortogonální doplněk podprostoru $\text{Ker } f$ v prostoru U a V' ortogonální doplněk podprostoru $\text{Im } f$ v prostoru V . Je tedy

$$U = \text{Ker } f \oplus U', \quad V = \text{Im } f \oplus V'$$

a f zobrazuje izomorfně U' na $\text{Im } f$. Jestliže je g homomorfismus prostoru V do prostoru U , který zobrazuje $\text{Im } f$ na U' inverzně k f a zobrazuje navíc celý podprostor V' na nulový vektor prostoru U , potom je $fgf = f$ a $gfg = g$ (viz důkaz věty 31.7). Navíc je

$$U' = \text{Im } g = (\text{Ker } f)^\perp \quad \text{a} \quad V' = \text{Ker } g = (\text{Im } f)^\perp. \quad \square$$

31.13. Příklad. Endomorfismus f prostoru \mathbb{R}^3 zobrazuje vektor (x, y, z) na vektor

$$(x + y + z, x - y, 2x + z).$$

Snadno se vypočte, že

$$\text{Ker } f = [(1, 1, -2)] \quad \text{a} \quad (\text{Ker } f)^\perp = [(1, -1, 0), (2, 0, 1)].$$

Obrazem tohoto podprostoru je podprostor $\text{Im } f = [(0, 2, 2), (3, 2, 5)]$,

$$\begin{aligned} (1, -1, 0) &\longrightarrow (0, 2, 2), \\ (2, 0, 1) &\longrightarrow (3, 2, 5), \end{aligned}$$

dále je $(\text{Im } f)^\perp = [(1, 1, -1)]$. Mooreův–Penroseův pseudoinverzní endomorfismus g k endomorfismu f je určen přiřazením

$$\begin{aligned} (0, 2, 2) &\longrightarrow (1, -1, 0), \\ (3, 2, 5) &\longrightarrow (2, 0, 1), \\ (1, 1, -1) &\longrightarrow (0, 0, 0). \end{aligned}$$

Odtud

$$\begin{aligned} (1, 0, 0) &\longrightarrow \left(\frac{1}{18}, \frac{7}{18}, \frac{4}{18}\right), \\ (0, 1, 0) &\longrightarrow \left(\frac{4}{18}, -\frac{8}{18}, -\frac{2}{18}\right), \\ (0, 0, 1) &\longrightarrow \left(\frac{5}{18}, -\frac{1}{18}, \frac{2}{18}\right). \end{aligned}$$

Endomorfismus g tedy zobrazuje vektor (a, b, c) na vektor

$$\frac{1}{18}(a + 4b + 5c, 7a - 8b - c, 4a - 2b + 2c).$$

Předchozí výsledky nyní vyjádříme v maticové podobě.

31.14. Definice. Nechť A je matice typu $n \times m$ nad tělesem T . Matice A^- typu $m \times n$ se nazývá *pseudoinverzní matice* k matici A , jestliže $AA^-A = A$. Jestliže platí navíc rovnost $A^-AA^- = A^-$, pak se matice A a A^- nazývají *navzájem pseudoinverzní*.

31.15. Věta. Nechť A je matice typu $n \times m$ a A^- matice typu $m \times n$ nad tělesem T . Potom platí:

- (i) Jestliže je $r(A) = n$ (a tedy $n \leq m$), potom je matice A^- pseudoinverzní k matici A právě tehdy, když je $AA^- = E$.
- (ii) Jestliže je $r(A) = m$ (a tedy $m \leq n$), potom je matice A^- pseudoinverzní k matici A právě tehdy, když je $A^-A = E$.
- (iii) Jestliže je matice A čtvercová regulární, potom je matice A^- pseudoinverzní k matici A právě tehdy, když je $A^- = A^{-1}$.

Důkaz. Matice A je maticí nějakého homomorfismu f prostoru T^m do prostoru T^n a matice A^- maticí nějakého homomorfismu g prostoru T^n do prostoru T^m (vzhledem ke kanonickým bázím). Protože je $r(A) = n$ (resp. $r(A) = m$) právě tehdy, když je f epimorfismus (resp. monomorfismus), vyplývají všechna uvedená tvrzení z odpovídajících tvrzení 31.2(i)–(iii) pro pseudoinverzní homomorfismy. Rovnosti $AA^-A = A$ a $fgf = f$, resp. $AA^- = E$ a $fg = 1_V$, resp. $A^-A = E$ a $gf = 1_U$ jsou totiž ekvivalentní. \square

31.16. Věta. Nechť A je matice typu $n \times m$ nad tělesem T a A^- matice k ní pseudoinverzní. Potom platí:

- (i) $r(A^-) \geq r(A) = r(AA^-) = r(A^-A)$.
- (ii) Všechny pseudoinverzní matice k matici A mají tvar

$$A^- + X - A^-AXAA^-,$$

kde X probíhá všechny matice typu $m \times n$ nad tělesem T .

- (iii) Všechny pseudoinverzní matice k matici A mají tvar

$$A^- + X(E - AA^-) + (E - A^-A)Y,$$

kde matice X a Y probíhají všechny matice typu $m \times n$ nad tělesem T .

Důkaz. Tvrzení (i)–(iii) vzniknou přepisem tvrzení (i), (x) a (xi) z 31.3. \square

Jsou-li tedy matice A a A^- navzájem pseudoinverzní, je $r(A) = r(A^-)$ podle 31.16(i).

31.17. Věta. Ke každé matici A existuje pseudoinverzní matice A^- . Ke každé matici A existuje taková matice A^- , že matice A a A^- jsou navzájem pseudoinverzní.

Důkaz. Nechť je dána matice A typu $n \times m$ nad tělesem T . Matice A je maticí nějakého homomorfismu f prostoru T^m do prostoru T^n vzhledem ke kanonickým

bázím. Podle věty 31.7 existuje homomorfismus g prostoru T^n do prostoru T^m , který je pseudoinverzní k f , resp. takový, že homomorfismy f a g jsou navzájem pseudoinverzní. Matice A^- homomorfismu g vzhledem ke kanonickým bázím je potom pseudoinverzní k matici A , resp. matice A a A^- jsou navzájem pseudoinverzní. \square

Z předcházejícího důkazu (viz též věta 31.7 a následující poznámka) je vidět, že pseudoinverzní matice A^- není určena jednoznačně a to ani v případě, kdy mají být matice A a A^- navzájem pseudoinverzní.

31.18. Příklad. Najdeme nějakou pseudoinverzní matici A^- k reálné matici

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 1 & 1 & 2 & 2 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Matici A budeme chápat jako matici homomorfismu f prostoru \mathbb{R}^4 do prostoru \mathbb{R}^3 utvořenou vzhledem ke kanonickým bázím těchto prostorů. Homomorfismus f tedy funguje takto:

$$\begin{aligned} (1, 0, 0, 0) &\longrightarrow (1, 1, 2) \\ (0, 1, 0, 0) &\longrightarrow (0, 1, 1) \\ (0, 0, 1, 0) &\longrightarrow (2, 2, 4) \\ (0, 0, 0, 1) &\longrightarrow (1, 2, 3) \end{aligned}$$

Obraz prostoru \mathbb{R}^4 při homomorfismu f je generován sloupci matice A ; je tedy

$$\text{Im } f = [(1, 1, 2), (0, 1, 1)],$$

neboť třetí a čtvrtý sloupec matice A jsou lineárními kombinacemi prvních dvou. Jádro $\text{Ker } f$ má tedy dimenzi 2 a podprostor $[(1, 0, 0, 0), (0, 1, 0, 0)]$ je jeho direktním doplňkem (zobrazuje se totiž izomorfně na $\text{Im } f$). Každý pseudoinverzní homomorfismus g k homomorfismu f musí zobrazit vektory $(1, 1, 2)$, $(0, 1, 1)$ na některé jejich vzory při f ; zvolený direktní doplněk podprostoru $\text{Im } f$ v prostoru \mathbb{R}^3 , např. $[(0, 0, 1)]$, můžeme zobrazit libovolně, pokud má být g pouze pseudoinverzní k f . Mají-li být f a g navzájem pseudoinverzní, musíme zobrazit zvolený direktní doplněk na nulový vektor. Definujme tedy homomorfismus g takto:

$$\begin{aligned} (1, 1, 2) &\longrightarrow (1, 0, 0, 0) \\ (0, 1, 1) &\longrightarrow (0, 1, 0, 0) \\ (0, 0, 1) &\longrightarrow (0, 0, 0, 0) \end{aligned}$$

Snadno zjistíme, že je

$$\begin{aligned} (1, 0, 0) &\longrightarrow (1, -1, 0, 0), \\ (0, 1, 0) &\longrightarrow (0, 1, 0, 0). \end{aligned}$$

Maticí homomorfismu g vzhledem ke kanonickým bázím prostorů \mathbb{R}^3 a \mathbb{R}^4 je tedy matice

$$A^{-} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Snadno se ověří, že je opravdu $AA^{-}A = A$ a $A^{-}AA^{-} = A^{-}$, tj. matice A a A^{-} jsou navzájem pseudoinverzní.

Poznamenejme, že $r(A) = r(A^{-}) = 2$; není tedy ani $A^{-}A = E$, ani $AA^{-} = E$ (viz 31.15).

Položme ještě např.

$$X = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Podle 31.16(ii) je matice

$$B = A^{-} + X - A^{-}AXAA^{-} = \begin{pmatrix} -3 & 0 & 1 \\ -2 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

rovněž pseudoinverzní maticí k matici A . Provéřte, že je skutečně $ABA = A$; není však $BAB = B$, tj. matice A a B nejsou navzájem pseudoinverzní.

V určitých situacích můžeme při řešení soustav lineárních rovnic využít i pseudoinverzních matic. Nejdůležitější fakta shrneme v následující větě; později se k této problematice vrátíme.

31.19. Věta. *Nechť A je matice typu $n \times m$ nad tělesem T a nechť y je n -tice prvků tělesa T . Jestliže je A^{-} pseudoinverzní matice k matici A , potom platí:*

- (i) *Soustava $Ax = y$ je řešitelná právě tehdy, když je $AA^{-}y^T = y^T$.*
- (ii) *Jestliže je soustava $Ax = y$ řešitelná, potom je možno množinu všech jejích řešení vyjádřit v tvaru*

$$A^{-}y^T + u^T - A^{-}Au^T,$$

kde vektor u probíhá prostor T^m .

- (iii) *Jestliže je nehomogenní soustava $Ax = y$ řešitelná, potom je možno množinu všech jejích řešení vyjádřit v tvaru By^T , kde B probíhá všechny matice, které jsou k matici A pseudoinverzní.*

Důkaz. Nechť f je homomorfismus prostoru T^m do prostoru T^n , jehož maticí vzhledem ke kanonickým bázím je matice A , a nechť g je homomorfismus prostoru

T^n do prostoru T^m , jehož maticí vzhledem ke kanonickým bázím je matice A^- . Homomorfismus f přiřazuje vektoru $x \in T^m$ vektor $Ax^T \in T^n$, homomorfismus g přiřazuje vektoru $z \in T^n$ vektor $A^-z^T \in T^m$. Protože je $AA^-A = A$, je $fgf = f$, tj. homomorfismus g je pseudoinverzní k homomorfismu f .

(i) Soustava $Ax = y$ je řešitelná právě tehdy, když je $y \in \text{Im } f$. Podle 31.3(iv) to nastane právě tehdy, když je $fg(y) = y$, neboli $AA^-y^T = y^T$.

(ii) Množina všech řešení (řešitelné) soustavy $Ax = y$ je rovna úplnému vzoru vektoru y při homomorfismu f . Podle 31.3(vi) jde o množinu

$$\{g(y) + u - gf(u); u \in T^m\},$$

tj. o množinu všech vektorů, které jdou vyjádřit v tvaru

$$A^-y^T + u^T - A^-Au^T,$$

kde u probíhá prostor T^m .

(iii) Předpokládejme, že nehomogenní soustava $Ax = y$ je řešitelná a B je matice, která je k matici A pseudoinverzní; je tedy $ABA = A$. Připomeňme, že podle (i) je $AA^-y^T = y^T$ a tedy

$$A(By^T) = ABAA^-y^T = AA^-y^T = y^T,$$

takže By^T je řešením soustavy $Ax = y$.

Jestliže je naopak x řešením soustavy $Ax = y$, potom podle předchozího existuje takový vektor $u \in U$, pro který

$$x = g(y) + u - gf(u).$$

Nechť $h : V \rightarrow U$ je nějaký homomorfismus, který zobrazuje vektor y na vektor u , a X jeho matice vzhledem ke kanonickým bázím prostorů T^n a T^m . Je tedy

$$x = g(y) + h(y) - gfh(y),$$

v maticovém tvaru

$$x^T = (A^- + X - A^-AX) \cdot y^T = (A^- + X - A^-AXAA^-) \cdot y^T = By^T,$$

kde podle 31.16(ii) je B nějaká pseudoinverzní matice k matici A . \square

Na závěr tohoto paragrafu budeme uvažovat pouze reálné nebo komplexní matice.

31.20. Definice. Nechť A je komplexní (reálná) matice typu $n \times m$. Matice A^+ typu $m \times n$ se nazývá *Mooreova–Penroseova pseudoinverzní matice* k matici A , jestliže

$$AA^+A = A, \quad A^+AA^+ = A^+$$

a jestliže matice AA^+ , A^+A jsou hermitovské (symetrické).

Uvědomme si, že matice A a A^+ jsou navzájem pseudoinverzní, že jejich vztah je symetrický, tj. o maticích A a A^+ můžeme hovořit jako o Mooreově–Penroseově dvojici navzájem pseudoinverzních matic.

31.21. Věta. *Ke každé matici existuje právě jediná Mooreova–Penroseova pseudoinverzní matice.*

Důkaz. Nechť A je komplexní matice typu $n \times m$. Matice A je maticí nějakého homomorfismu f prostoru \mathbb{C}^m do prostoru \mathbb{C}^n (vzhledem ke kanonickým bázím). Podle věty 31.12 existuje právě jediný homomorfismus g prostoru \mathbb{C}^n do prostoru \mathbb{C}^m , takový, že f a g tvoří Mooreovu–Penroseovu dvojici navzájem pseudoinverzních homomorfismů. Pro matici A^+ homomorfismu g vzhledem ke kanonickým bázím prostorů \mathbb{C}^m a \mathbb{C}^n potom platí vztahy

$$AA^+A = A, \quad A^+AA^+ = A^+;$$

protože jsou podle věty 31.11 endomorfismy fg a gf samoadjungované, jsou podle věty 29.5 matice AA^+ , A^+A hermitovské. Stejně se provede důkaz pro reálnou matici. \square

31.22. Příklady.

(i) Najdeme Mooreovu–Penroseovu matici A^+ k matici

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Matice A je maticí homomorfismu $f: \mathbb{R}^4 \rightarrow \mathbb{R}^2$ (vzhledem ke kanonickým bázím těchto prostorů), který vektor (x, y, z, t) zobrazuje na vektor $(x + y + t, x + y + z)$. Podprostor $\text{Im } f$ je generován sloupci matice A , tj. $\text{Im } f = \mathbb{R}^2$, ortogonální doplněk $(\text{Im } f)^\perp$ je nulový. Podprostor $\text{Ker } f$ je řešením homogenní soustavy lineárních rovnic s maticí A , ortogonální doplněk $(\text{Ker } f)^\perp$ je tedy generován řádky matice A . Homomorfismus f tedy zobrazuje generátory podprostoru $(\text{Ker } f)^\perp$ takto:

$$\begin{aligned} (1, 1, 0, 1) &\longrightarrow (3, 2), \\ (1, 1, 1, 0) &\longrightarrow (2, 3). \end{aligned}$$

Homomorfismus g , který je pseudoinverzní k f , tedy musí být definován přiřazeními

$$\begin{aligned} (3, 2) &\longrightarrow (1, 1, 0, 1), \\ (2, 3) &\longrightarrow (1, 1, 1, 0). \end{aligned}$$

Odtud

$$\begin{aligned} (1, 0) &\longrightarrow \left(\frac{1}{5}, \frac{1}{5}, -\frac{2}{5}, \frac{3}{5}\right), \\ (0, 1) &\longrightarrow \left(\frac{1}{5}, \frac{1}{5}, \frac{3}{5}, -\frac{2}{5}\right). \end{aligned}$$

Dvojice homomorfismů f, g je Mooreovou–Penroseovou dvojicí díky volbě ortogonálních doplňků. Mooreovou–Penroseovou maticí k matici A je tedy matice

$$A^+ = \frac{1}{5} \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ -2 & 3 \\ 3 & -2 \end{pmatrix}.$$

Poznamenejme ještě, že $r(A) = 2$ (A je maticí epimorfismu), tj. podle 31.15(i) je $AA^+ = E$.

(ii) Najdeme Mooreovu–Penroseovu matici A^+ k matici

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Matice A je maticí endomorfismu f prostoru \mathbb{R}^3 (vzhledem ke kanonické bázi prostoru \mathbb{R}^3), který vektor (x, y, z) zobrazuje na vektor $(x + y, z, 0)$. Podprostor $\text{Im } f$ je generován sloupci matice A , tj. $\text{Im } f = [(1, 0, 0), (0, 1, 0)]$ a $(\text{Im } f)^\perp = [(0, 0, 1)]$. Podprostor $\text{Ker } f$ je řešením homogenní soustavy lineárních rovnic s maticí A , ortogonální doplněk $(\text{Ker } f)^\perp$ je tedy generován řádky matice A ,

$$(\text{Ker } f)^\perp = [(1, 1, 0), (0, 0, 1)].$$

Homomorfismus f tedy zobrazuje generátory podprostoru $(\text{Ker } f)^\perp$ takto:

$$\begin{aligned} (1, 1, 0) &\longrightarrow (2, 0, 0), \\ (0, 0, 1) &\longrightarrow (0, 1, 0). \end{aligned}$$

Homomorfismus g , který má s homomorfismem f tvořit Mooreovu–Penroseovu dvojici navzájem pseudoinverzních homomorfismů, tedy musí být definován takto:

$$\begin{aligned} (2, 0, 0) &\longrightarrow (1, 1, 0), \\ (0, 1, 0) &\longrightarrow (0, 0, 1), \\ (0, 0, 1) &\longrightarrow (0, 0, 0). \end{aligned}$$

Odtud již vyplývá, že Mooreovou–Penroseovou maticí k matici A je matice

$$A^+ = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Poznamenejme, že $r(A) = 2$ (A není maticí epimorfismu ani monomorfismu), tj. není ani $A^+A = E$, ani $AA^+ = E$ (viz 31.15).

(iii) Najdeme Mooreovu–Penroseovu pseudoinverzní matici A^+ k matici

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ -1 & 3 \end{pmatrix}.$$

Matice A je maticí homomorfismu $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ (vzhledem ke kanonickým bázím těchto prostorů), který vektor (x, y) zobrazuje na vektor $(x + y, 2x, -x + 3y)$. Podprostor $\text{Im } f$ je generován sloupci matice A , tj.

$$\text{Im } f = [(1, 2, -1), (1, 0, 3)] \quad \text{a} \quad (\text{Im } f)^\perp = [(-3, 2, 1)].$$

Podprostor $\text{Ker } f$ je řešením homogenní soustavy lineárních rovnic s maticí A , ortogonální doplněk $(\text{Ker } f)^\perp$ je tedy generován řádky matice A , $(\text{Ker } f)^\perp = \mathbb{R}^2$. Homomorfismus f tedy zobrazuje generátory podprostoru $(\text{Ker } f)^\perp$ takto:

$$\begin{array}{ll} (1, 0) & \longrightarrow (1, 2, -1), \\ (0, 1) & \longrightarrow (1, 0, 3). \end{array}$$

Homomorfismus g , který má s homomorfismem f tvořit Mooreovu–Penroseovu dvojici navzájem pseudoinverzních homomorfismů, tedy musí být definován přiřazením

$$\begin{array}{ll} (1, 2, -1) & \longrightarrow (1, 0), \\ (1, 0, 3) & \longrightarrow (0, 1), \\ (-3, 2, 1) & \longrightarrow (0, 0). \end{array}$$

Postupným výpočtem dospějeme k přiřazení

$$\begin{array}{ll} (1, 0, 0) & \longrightarrow \left(\frac{3}{14}, \frac{2}{14}\right), \\ (0, 1, 0) & \longrightarrow \left(\frac{5}{14}, \frac{1}{14}\right), \\ (0, 0, 1) & \longrightarrow \left(-\frac{1}{14}, \frac{4}{14}\right). \end{array}$$

Mooreovou–Penroseovou pseudoinverzní maticí k matici A je matice

$$A^+ = \frac{1}{14} \begin{pmatrix} 3 & 5 & -1 \\ 2 & 1 & 4 \end{pmatrix}.$$

Poznamenejme, že $r(A) = 2$ (A je maticí monomorfismu), tj. podle 31.15(ii) je $A^+A = E$.

31.23. Věta. *Nechť A je komplexní (reálná) matice typu $n \times m$ a nechť y je n -tice prvků tělesa T . Jestliže A^+ je Mooreova–Penroseova pseudoinverzní matice k matici A , potom platí:*

- (i) *Jestliže $Ax = y$ je řešitelná soustava, potom je A^+y^T její řešení, které má ze všech řešení této soustavy nejmenší normu.*
- (ii) *Jestliže $Ax = y$ je neřešitelná soustava, potom je A^+y^T její přibližné řešení, které má ze všech přibližných řešení nejmenší normu.*

Důkaz. Obě tvrzení vyplývají z věty 31.10. \square

31.24. Příklady.

(i) Uvažujme soustavu lineárních rovnic

$$\begin{aligned}x_1 + x_2 &= -1, \\2x_1 &= 2, \\-x_1 + 3x_2 &= -7.\end{aligned}$$

Maticí této soustavy lineárních rovnic je matice

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ -1 & 3 \end{pmatrix},$$

soustava je řešitelná, má jediné řešení $(1, -2)$.

Toto řešení můžeme dostat jako součin Mooreovy–Penroseovy matice A^+ , kterou jsme vypočetli v příkladu 31.22(iii), s vektorem pravých stran:

$$\frac{1}{14} \begin{pmatrix} 3 & 5 & -1 \\ 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 2 \\ -7 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$$

(ii) Uvažujme soustavu lineárních rovnic

$$\begin{aligned}x_1 + x_2 &= 1, \\2x_1 &= 0, \\-x_1 + 3x_2 &= 2.\end{aligned}$$

Maticí této soustavy lineárních rovnic je opět matice A z předchozího příkladu. Uvažovaná soustava nemá řešení v exaktním slova smyslu, neboť sloupec pravých stran není lineární kombinací sloupců matice A .

Vynásobíme-li sloupec pravých stran uvažované neřešitelné soustavy Mooreovu–Penroseovu pseudoinverzní matici A^+ , získáme její přibližné řešení:

$$\frac{1}{14} \begin{pmatrix} 3 & 5 & -1 \\ 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} = \frac{1}{14} \begin{pmatrix} 1 \\ 10 \end{pmatrix} .$$

Poznamenejme, že ke stejnému řešení dospějeme i pomocí Gramovy matice (viz 28.6 a 28.7). Získáme rozšířenou matici

$$\left(\begin{array}{cc|c} 6 & -2 & -1 \\ -2 & 10 & 7 \end{array} \right)$$

řešitelné soustavy rovnic a jednoduchou úpravou dospějeme ke stejnému řešení jako pomocí Mooreovy–Penroseovy pseudoinverzní matice.

(iii) Uvažujme soustavu lineárních rovnic

$$\begin{aligned} x_1 + 3x_2 + x_3 - 2x_4 &= 1 , \\ 2x_1 + x_2 - 2x_3 &= 3 . \end{aligned}$$

Maticí této soustavy lineárních rovnic je matice

$$A = \begin{pmatrix} 1 & 3 & 1 & -2 \\ 2 & 1 & -2 & 0 \end{pmatrix} .$$

Snadno se nahlédne, že je uvažovaná soustava rovnic řešitelná a dimenze jejího řešení je 2.

Mooreovou–Penroseovou pseudoinverzní maticí k matici A je matice

$$A^+ = \frac{1}{42} \begin{pmatrix} 1 & 9 \\ 8 & 2 \\ 5 & -11 \\ -6 & 2 \end{pmatrix}$$

a řešením uvažované soustavy, které má nejmenší normu, je vektor

$$\frac{1}{42} \begin{pmatrix} 1 & 9 \\ 8 & 2 \\ 5 & -11 \\ -6 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 2 \\ 1 \\ -2 \\ 0 \end{pmatrix} .$$

Množinou všech řešení uvažované soustavy je lineární množina

$$\frac{1}{3}(2, 1, -2, 0) + [(0, 4, 2, 7), (1, 0, 1, 1)] .$$

Správnost výsledku se snadno prověří; stačí zjistit, že vektor $\frac{1}{3}(2, 1, -2, 0)$ je opravdu řešením uvažované soustavy a že je kolmý na generátory podprostoru všech řešení odpovídající homogenní soustavy.

(iv) Uvažujme soustavu lineárních rovnic

$$\begin{aligned}x_1 + 3x_2 + x_3 - 2x_4 &= 1, \\2x_1 + x_2 - 2x_3 &= 3, \\x_1 - 2x_2 - 3x_3 + 2x_4 &= 1.\end{aligned}$$

Maticí této soustavy lineárních rovnic je matice

$$A = \begin{pmatrix} 1 & 3 & 1 & -2 \\ 2 & 1 & -2 & 0 \\ 1 & -2 & -3 & 2 \end{pmatrix}.$$

Snadno se nahlédne, že je uvažovaná soustava neřešitelná.

Mooreovou–Penroseovou pseudoinverzní maticí k matici A je matice

$$A^+ = \frac{1}{126} \begin{pmatrix} 11 & 19 & 8 \\ 18 & 12 & -6 \\ -1 & -17 & -16 \\ -10 & -2 & 8 \end{pmatrix}$$

a přibližným řešením s nejmenší normou je vektor

$$\frac{1}{126} \begin{pmatrix} 11 & 19 & 8 \\ 18 & 12 & -6 \\ -1 & -17 & -16 \\ -10 & -2 & 8 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix} = \frac{1}{63} \begin{pmatrix} 38 \\ 24 \\ -34 \\ -4 \end{pmatrix}.$$

Množinou všech přibližných řešení uvažované soustavy je lineární množina

$$\frac{1}{63}(38, 24, -34, -4) + [(0, 4, 2, 7), (1, 0, 1, 1)].$$

LITERATURA

TEORIE MNOŽIN

- [BŠ] B. Balcar, P. Štěpánek, *Teorie množin*, Academia, Praha, 1986, 412 stran.
 [BK1] J. Blažek, B. Kussová, *Množiny a přirozená čísla*, SPN, Praha, 1977, 221 stran.
 [BK2] J. Blažek, B. Vojtášková, *Teorie množin*, PF UJEP, Ústí nad Labem, 1994, 149 stran.
 [Fu] E. Fuchs, *Teorie množin pro učitele*, PřF MU, Brno, 1999, 200 stran.

ALGEBRA

- [BK3] J. Blažek, E. Calda, M. Koman, B. Kussová, *Algebra a teoretická aritmetika I*, SPN, Praha, 1983, 278 stran.
 [BK4] J. Blažek, M. Koman, B. Vojtášková, *Algebra a teoretická aritmetika II*, SPN, Praha, 1985, 258 stran.
 [Ko] V. Kořínek, *Základy algebry*, ČSAV, Praha, 1. vyd. 1953, 488 stran; 2. vyd. 1956, 520 stran.
 [P] L. Procházka, *Algebra*, Academia, Praha, 1990, 560 stran.

Slovensky

- [BM] G. Birkhoff, S. Mac Lane, *Prehľad modernej algebry*, Alfa, SNTL, Bratislava, Praha, 1979, 468 stran; z anglického originálu *A Survey of Modern Algebra*, The Macmillan Company, Inc., New York, 3. vyd. 1965 (1. vyd. 1941, 2. vyd. 1953), přeložili Š. Známa a J. Smítal.
 [K] T. Katriňák, M. Gavalec, E. Gedeonová, J. Smítal, *Algebra a teoretická aritmetika 1*, Alfa, SNTL, Bratislava, Praha, 1985, 349 stran.
 [MB] S. Mac Lane, G. Birkhoff, *Algebra*, Alfa, Bratislava, 1. vyd. 1973; 2. vyd. 1974, 662 stran; z anglického originálu *Algebra*, The Macmillan Company, Inc., New York, 2. vyd. 1968, přeložili A. Legěň a J. Smítal.
 [S] Š. Schwarz, *Základy nauky o riešení rovníc*, SAV, Bratislava, 1. vyd. 1967, 439 stran; 2. vyd., 1968, 454 stran; původně vyšlo r. 1958 v nakladatelství ČSAV, Praha, 345 stran.
 [Š] T. Šalát, A. Haviar, T. Hecht, T. Katriňák, *Algebra a teoretická aritmetika 2*, Alfa, SNTL, Bratislava, Praha, 1986, 215 stran.

LINEÁRNÍ ALGEBRA

- [Bi1] L. Bican, *Lineární algebra*, SNTL, Praha, 1979, 331 stran.
 [B] O. Borůvka, *Základy teorie matic*, Academia, Praha, 1971, 177 stran.
 [By] B. Bydžovský, *Úvod do teorie determinantů a matic a jich užití*, JČMF, Praha, 2. vyd. 1947, 238 stran; 1. vyd. vyšlo roku 1930 pod názvem *Základy teorie determinantů a matic a jich užití*, JČMF, Praha, 211 stran.
 [DN] M. Demlová, J. Nagy, *Algebra*, SNTL, Praha, 1. vyd. 1984; 2. vyd. 1985, 187 stran.
 [Ge] I. M. Gelfand, *Lineární algebra*, ČSAV, Praha, 1953, 230 stran; z ruského originálu *Lekcii po linějnoj algebre*, 2. vyd., Gostechizdat, Moskva, Leningrad, 1951 (3. vyd., Nauka, Moskva, 1966, 280 stran; 1. vyd. 1948) přeložil M. Fiedler.
 [HH] V. Havel, J. Holenda, *Lineární algebra*, SNTL, Praha, 1984.
 [Vo] V. Vodička, *Determinanty a matice v theorii i v praxi I, II*, Přírodovědecké nakladatelství, JČMF, Praha, 1950, 96 a 144 stran.

Anglicky

- [An] H. Anton, *Elementary Linear Algebra*, John Wiley & Sons, Inc., New York, 1973, 1977, 1981, 4. vyd. 1984, 403+46 stran.
- [Ax] S. Axler, *Linear Algebra Done Right*, Springer, New York, 1996, 238 stran.
- [BR] T. S. Blyth, E. F. Robertson, *Basic Linear Algebra*, Springer-Verlag, 2. vyd. 1998, 201 stran.
- [C] H. G. Campbell, *Linear Algebra with Applications*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1. vyd. 1971; 2. vyd. 1980, 338+62 stran.
- [Cu] C. W. Curtis, *Linear Algebra. An Introductory Approach*, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1974; 4. vyd. 1984, x+337 stran.
- [Ha] P. R. Halmos, *Finite Dimensional Vector Spaces*, Princeton University Press, Princeton, 1948, existuje řada dalších vydání (např. 1974, 199 stran); ruský překlad: *Konečnoměrnýje vektornyje prostranstva*, Moskva, 1963, 262 stran.
- [L] P. Lancaster, *Theory of Matrices*, Academic Press, New York, London, 1969, 316 stran; ruský překlad: *Těoriija matric*, Nauka, Moskva, 1978.
- [La] S. Lang, *Linear Algebra*, Addison-Wesley Publishing Company-Reading, 1966.
- [Sa] I. Satake, *Linear Algebra*, Marcel Dekker, Inc., New York, 1975, 308 stran.

Francouzsky

- [Di] J. Dieudonné, *Algèbre linéaire et géométrie élémentaire*, Herman, Paris, 1. vyd. 1964; 3. vyd. 1968; ruský překlad: *Linějnaja algebra i elementarnaja geometrija*, Nauka, Moskva, 1972, 335 stran; anglický překlad: *Linear algebra and Geometry*, Herman, Paris, 1969.

Německy

- [Bo] H. Boseck, *Einführung in die Theorie der linearen Vektorräume*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1965, 308 stran.
- [Kl] W. Klingenberg, *Lineare Algebra und Geometrie*, Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1984, 313 stran.
- [Koe] M. Koecher, *Lineare Algebra und analytische Geometrie*, Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1983, 286 stran.

Rusky

- [KM] A. I. Kostrikin, Ju. I. Manin, *Linějnaja algebra i geometrija*, Izd. Moskovskogo universitěta, Moskva, 1980, 319 stran.
- [Ku] A. G. Kuroš, *Kurs vyššej algebry*, Gos. izd. fiz.-mat. lit., Moskva, 7. vyd. 1962, 431 stran; předchozí vydání 1946, 1950, 1952, 1955, 1956, 1958; anglický překlad *Higher algebra*, Mir, Moskva, 1972, 428 stran.
- [Ma] A. I. Mal'cev, *Osnovy linějnoj algebry*, Nauka, Moskva, 4. vyd. 1975, 400 stran; 1., 2. a 3. vydání vyšla v letech 1948, 1956 a 1970.

SBÍRKY ÚLOH

- [T] L. Tesková, *Sbírka příkladů z lineární algebry*, ZČU, Plzeň, 1995, 141 stran.
- [W] J. Weil a kol., *Rozpracovaná řešení úloh z vyšší algebry*, Academia, Praha, 1987, 650 stran; z francouzských originálů *Solutions développées des exercices 1, 2, 3*, Gauthier-Villars, 1972, 1973, 1976, přeložil L. Beran.

Slovensky

- [FS] A. K. Faddejev, J. S. Sominskij, *Zbierka úloh z vyššej algebry*, Alfa, Bratislava, 1968, 324 stran; ruský originál: *Sbornik zadač po vyššej algebre*, Nauka, Moskva, 8. vyd. 1964, 304 stran.
- [Sv] P. Svätokřížny, *Lineárna algebra v úlohách*, Alfa, Bratislava, 1985.

Rusky

- [Pr] I. V. Proskurjakov, *Sbornik zadač po lineární algebre*, Nauka, Moskva, 5. vyd. 1974, 384 stran; 1. vyd. 1955; 2. vyd. 1961; 3. vyd. 1966; anglický překlad: *Problems in Linear Algebra*, Mir, Moskva, 1978.
- [I] Ch. D. Ikramov, *Zadačnik po lineární algebre*, Nauka, Moskva, 1975, 319 stran.

UČEBNÍ TEXTY MFF UK (1975–2000)

- [B1] J. Bečvář, *Sbírka úloh z lineární algebry*, SPN, Praha, 1975, 196 stran.
- [B2] J. Bečvář, *Vektorové prostory I*, SPN, Praha, 1978, 171 stran; dotisk UK 1980, 2. vyd. SPN 1984, 3. vyd. SPN 1989.
- [B3] J. Bečvář, *Vektorové prostory II*, SPN, Praha, 1980, 199 stran; dotisk SPN 1984, 2. vyd. SPN 1989.
- [B4] J. Bečvář, *Vektorové prostory III. Sbírka úloh*, SPN, Praha, 1982, 191 stran.
- [Be] L. Beran, *Vybrané kapitoly z teorie matic*, SPN, Praha, 1980, 328 stran.
- [Bi2] L. Bican, *Lineární algebra v úlohách*, SPN, Praha, 1979, 303 stran.
- [BH] L. Bican, J. Hurt, *Aplikovaná lineární algebra*, SPN, Praha, 1985, 205 stran.
- [G] P. Goralčík, *Úvod do lineární algebry*, SPN, Praha, 1979, 194 stran.

ROZŠÍŘENÍ OBZORŮ

- [FF] D. K. Faddějev, V. N. Faddějeva, *Numerické metody lineární algebry*, SNTL, Praha, 1964, 682 stran; z ruského originálu *Vyčíslitel'nyje metody lineární algebry*, Fizmatgiz, Moskva 1963, přeložil M. Fiedler.
- [F] M. Fiedler, *Speciální matice a jejich použití v numerické matematice*, SNTL, Praha, 1981, 266 stran.
- [MZ] L. Motl, M. Zahradník, *Pěstujeme lineární algebru*, Karolinum, Praha, 1. vyd. 1995, 2. vyd. 1999, 348 stran.
- [Ta] A. E. Taylor, *Úvod do funkcionální analýzy*, Academia, Praha, 1973, 408 stran; z anglického originálu *Introduction to Functional Analysis*, John Wiley & Sons, Inc., New York, 6. vyd. 1967 (1. vyd. 1958, 423 stran), přeložili M. Hušek a A. Kufner.

Slovensky

- [BB] G. Birkhoff, T. O. Barteo, *Aplikovaná algebra*, Alfa, Bratislava, 1981, 389 stran; z anglického originálu *Modern Applied Algebra*, McGraw-Hill Book Company, Inc., New York, 1970, přeložil J. Smítal.
- [NS] A. W. Naylor, G. R. Sell, *Teória lineárnych operátorov v technických a prírodných vedách*, Alfa, Bratislava, 1981, 629 stran; z anglického originálu *Linear Operator Theory in Engineering and Science*, Holt, Rinehart and Winston, Inc., New York, 1971, přeložili J. Dravecký a P. Mederly.

Anglicky

- [DG] E. Deeba, A. Gunawardena, *Interactive Linear Algebra with Maple V*, Springer-Verlag, 1998, 317 stran.
- [MM] M. Marcus, H. Minc, *A Survey of Matrix Theory and Matrix Inequalities*, Allyn & Bacon, Inc., Boston, 1964; ruský překlad: *Obzor po teorii matric i matricnyh neravenstv*, Nauka, Moskva, 1972, 232 stran.
- [M] M. Marcus, *Finite Dimensional Multilinear Algebra I, II*, Marcel Dekker, Inc., New York, 1973, 1975, 292 a 718 stran.

Rusky

- [Ga] F. R. Gantmacher, *Teorija matric*, Nauka, Moskva, 2. vyd. 1966, 576 stran.
- [GL] I. M. Glazman, Ju. I. Ljubič, *Konečnoměrnnyj linejnnyj analiz v zadačach*, Nauka, Moskva, 1969, 475 stran.

Jindřich Bečvář

LINEÁRNÍ ALGEBRA

Vydal
MATFYZPRESS
vydavatelství
Matematicko-fyzikální fakulty
Univerzity Karlovy v Praze
Sokolovská 83, 186 75 Praha 8
jako svou 329. publikaci

Obálku navrhl Petr Kubát

Z předloh připravených v systému *AMSTeX*
vytisklo Repro středisko UK MFF
Sokolovská 83, 186 75 Praha 8

Vydání čtvrté

Praha 2010

ISBN 978-80-7378-135-4
ISBN 80-86732-57-6 (třetí vydání)
ISBN 80-85863-92-8 (druhé vydání)
ISBN 80-85863-61-8 (první vydání)