Ústní část SZZ oboru MIT: neoficiální rozpis témat

(platné pro studenty, kteří nastoupili 2019/20 a později)

David Stanovský, garant oboru MIT *verze 5.8.2024*

Oficiální zkušební okruhy jsou formulovány v karolince a dostupné na webu fakulty. Tento rozpis berte jako informativní. Snažil jsem se o úplný výčet tradičně zkoušených témat, ale mohl jsem na něco zapomenout a je třeba brát v úvahu, že zkouší komise a na důležitost jednotlivých témat mohou mít různí zkoušející různý názor. Pod konkrétním heslem (např. „Struktura cyklických grup“) se typicky rozumí znalost celé stejnojmenné sekce z příslušného učebního materiálu.

Oficiální popis ústní části: Zkouška má přehledový charakter. Jsou kladeny širší otázky a žádá se, aby posluchač prokázal pochopení základních problémů, byl schopen je ilustrovat na konkrétních situacích a osvědčil určitou míru syntézy a hlubšího pochopení. Student dostane po jedné otázce z tematických okruhů 1., 2. a 3., přičemž u tematického okruhu 3 si student volí jednu z variant 3A nebo 3B.

1. Lineární algebra, geometrie a analýza

Oficiální popis: - Maticový počet, soustavy lineárních rovnic, skalární součin, kvadratické formy - Afinní a projektivní geometrie, grupy transformací - Posloupnosti a řady, diferenciální počet jedné a více proměnných

Neoficiální upřesnění:

1. Maticový počet a soustavy lineárních rovnic *[Lineární algebra 1]*
Základní maticové operace, hodnost matice, regulární matice. Soustavy lineárních rovnic, podmínky řešitelnosti, Gaussova eliminace, výpočet inverzní matice. Determinanty a metody jejich výpočtu, Cramerovo pravidlo. Vlastní čísla matic a diagonalizace.

2. Vektorové prostory a skalární součiny *[Lineární algebra 1,2]*
Pojem vektorového prostoru, lineární nezávislost, lineární obal, báze a dimenze. Steinitzova věta o výměně. Podprostory a jejich dimenze. Skalární součin, ortogonalizační proces, QR rozklad matice, ortogonální matice. Ortogonální projekce a metoda nejmenších čtverců.

3. Lineární zobrazení a bilineární formy *[Lineární algebra 1,2]*
Lineární zobrazení a jejich matice, matice základních geometrických zobrazení. Věta o dimenzi jádra a obrazu. Vlastní čísla lineárních zobrazení a matic, algebraická a geometrická násobnost, charakterizace diagonalizovatelných matic. Charakterizace ortogonálně diagonalizovatelných reálných matic. Bilineární a kvadratické formy a jejich matice, polární báze a zákon setrvačnosti pro kvadratické formy.

4. Afinní a projektivní geometrie *[Geometrie 1]*
Afinní a projektivní prostor, afinní a homogenní souřadnice. Projektivní, afinní a shodná zobrazení. Klasifikace shodností v rovině. Přímé shodnosti v prostoru, rotace a kvaterniony. Dělící poměr a dvojpoměr. Menelaova a Pappova věta. Křivost a znaménková křivost křivky. Kuželosečky v projektivní a afinní reálné rovině.

5. Posloupnosti a řady čísel a funkcí *[Matematická analýza 1,2,3]*
Limity posloupností a součty řad. Kritéria absolutní a neabsolutní konvergence číselných řad.

6. Diferenciální počet *[Matematická analýza 1,2]*
Spojitost a derivace funkcí jedné reálné proměnné. Hlubší věty o spojitých funkcích. Věty o střední hodnotě a jejich důsledky. Vztahy monotonie a znaménka derivace. Konvexita. Taylorův polynom. Taylorovy řady. Parciální derivace a derivace zobrazení z R^n do R^m, gradient, Jacobiho matice, derivace složeného zobrazení.

2. Obecná algebra.

Oficiální popis: Základy teorie grup (Lagrangeova věta, cyklické grupy) - Základy komutativní algebry (obory gaussovské, eukleidovské, hlavních ideálů) - Okruhy polynomů, Hilbertova věta o bázi a o nulách

Neoficiální upřesnění:

1. Grupy *[Algebra]*
Pojem grupy, příklady, Lagrangeova věta, struktura cyklických grup a věta o primitivním prvku (multiplikativní grupy konečných těles jsou cyklické), působení grupy na množině.

2. Dělitelnost v oborech integrity *[Algebra]*
Obory integrity a jejich ideály (hlavní, maximální, prvoideály, radikály), lokalizace a podílové těleso. Hierarchie oborů integrity vzhledem k dělitelnosti (gaussovské obory, obory hlavních ideálů, eukleidovské obory), různé charakterizace, implikace mezi těmito pojmy, protipříklady.

3. Obory polynomů *[Algebra, Úvod do komutativní algebry]*
Polynomiální okruhy (jedné i více proměnných): základní vlastnosti z hlediska dělitelnosti, Gaussova věta, čínská věta o zbytcích pro polynomy. Noetherovské okruhy a Hilbertova věta o bázi, základní principy algebraické geometrie (IV-korespondence), Hilbertova věta o nulách. Kořenová a rozkladová nadtělesa (existence a jednoznačnost), klasifikace konečných těles.

3A. Informační bezpečnost

Oficiální popis: - Základy pravděpodobnosti, entropie, Shannonova věta - Základní algoritmy pro práci s polynomy, rychlá Fourierova transformace - Základní kryptografické koncepty, RSA, výměna klíče

Neoficiální upřesnění:

1. Pravděpodobnost a entropie *[Pravděpodobnost, Teorie informace]*
Slabý zákon velkých čísel a Chernoffovy odhady. Definice entropie a její základní vlastnosti. Typické posloupnosti a jejich pravděpodobnost. Komprese dat a délka optimálního kódu. Kapacita kanálu a Shannonova věta o kódování kanálu. ML a MAP dekódování. Viterbiho algoritmus.

2. Počítačová algebra. *[Počítačová algebra]*
Základní operace s polynomy a jejich výpočetní složitost: Modulární reprezentace, rychlá Fourierova transformace a rychlé násobení polynomů. Rychlé dělení polynomů. Efektivní výpočet největšího společného dělitele celočíselných polyomů. Algoritmy na Čínskou větu o zbytcích, interpolace.

3. Kryptologie *[Úvod do kryptografie, Teoretická kryptografie 1,2]*
Symetrická a asymetrická kryptografie, blokové a proudové šifry, operační režimy blokových šifer, hashovací funkce, MAC, digitální podpis a jejich použití. Problém diskrétního logaritmu a algoritmy na něm založené. Kryptosystém RSA. Složitost útoků hrubou silou, meet-in-the-middle útok, diferenční a lineární kryptoanalýza.

3B. Počítačová geometrie

Oficiální popis: Základy geometrického modelování, Beziérovy křivky a plochy - Maticové rozklady

Neoficiální upřesnění:

1. Geometrické modelování *[Geometrické modelování]*
Polynomiální a racionální Bézierovy křivky a jejich vlastnosti, DeCasteljau algoritmus, B-spline funkce, vložení uzlu, Fergusonovy kubiky, Coonsovy pláty.

2. Výpočetní aspekty lineární algebry *[Numerická lineární algebra]*
Schurova věta a Schurův rozklad. Algoritmy pro numerický výpočet LU, QR a SVD rozkladů, jejich řádové výpočetní náklady a numerická stabilita. Využití rozkladů pro řešení soustav lineárních algebraických rovnic a problému nejmenších čtverců. Stacionární iterační metody pro řešení soustav lineárních algebraických rovnic. Iterační metody pro řešení částečného problému vlastních čísel.