Magisterský program MATEMATIKA, verze z 30. 11. 2017

Požadavky k SZZ
Státní závěrečná zkouška sestává z obhajoby diplomové práce a z ústní zkoušky.

Charakteristika závěrečné práce a její obhajoba
Zpracováním diplomové práce student prokazuje orientaci v problematice dané tématem práce a schopnost odborné práce pod vedením vedoucího. U obhajoby diplomové práce se hodnotí porozumění tématu a úroveň prezentace.

Charakteristika ústní zkoušky
Účelem zkoušky je prověřit, že absolvent je schopen vést debatu na odborné úrovni. Cílem ústní zkoušky není opakovat zkoušky z jednotlivých předmětů a zkoušet detailní znalost teorie a důkazů. Smyslem je prokázat všeobecný přehled o základních pojmech a výsledcích z jednotlivých oborů a širších souvislostech mezi nimi a o jejich možných aplikacích.

Technická realizace
U ústní zkoušky student obdrží **dvě (nebo tři?)** otázky, jednu z okruhů otázek společných pro celý program a **jednu (dvě?)** ze znalostí vybraného povinně volitelného bloku. Následující okruhy vymezují pokládané otázky pouze rámcově.

A. **Okruhy otázek společných pro celý program**

1. Parciální diferenciální rovnice I. PDR 1. řádu, metoda charakteristik, příklady lineárních a nelineárních rovnic a jejich užití, Fourierova metoda, srovnání chování řešení PDR a ODR, analytická řešení, věta Cauchyova-Kovalevské.

2. Parciální diferenciální rovnice II. Řešení významných rovnic matematické fyziky (Laplaceova a Poissonova rovnice, rovnice vedení tepla, vlnová rovnice), harmonické funkce, principy maxima, semigrupy a Brownův pohyb, diskretizace a standardní numerické metody řešení.

3. Parciální diferenciální rovnice III. Sobolevovy prostory, variační formulace řešení, zobecněná formulace počátečních-okrajových úloh, teorie stop, slabá řešení eliptických, parabolických a hyperbolických PDR, regularita řešení, variační metody, metoda konečných prvků.

4. Okruhy a moduly. Moduly, homomorfismy. Součiny, přímé součty, jádra, kojádra. Volné a projektivní moduly. Tensorový součin. Ploché moduly. Injektivní moduly, injektivní obal. Noetherovské okruhy.

5. Homologické algebra. Základní pojmy teorie kategorií. Řetězcové komplexy, exaktnost, homologie. Projektivní a injektivní rezolventy. Derivované funktory. Vztah Ext a rozšíření modulů. Projektivní a injektivní dimenze.

6. Reprezentace grup. Lineární reprezentace grup, grupové okruhy a grupové algebry a moduly nad nimi. Ireducibilní reprezentace, rozložitelnost na přímé součty ireducibilních reprezentací,
Schurovo lemma, Maschkeho věta. Charaktery grup, ortogonalita. Aplikace v teorii konečných grup, indukované reprezentace, Frobeniova věta o reciprocitě.

7. Vektorový diferenciální a integrální počet. Vektorová pole a vnější formy na R^n a podvarietách R^n, obecná Stokesova věta a její důsledky ve vektorovém počtu, geometrická teorie PDR 1. řádu (diferenciální ideály, Frobeniova věta).

8. Lieovy grupy a algebry. Lieovy grupy a podgrupy, vztah k Lieovým algebrám (exponenciální zobrazení, adjungovaná reprezentace, nakrytí grup), diferenciální počet pro funkce s hodnotami v Lieově grupě. Základní koncepty reprezentace Lieových grup, homogenní prostory.

9. Aplikace geometrických struktur. Základní koncepty riemannovské a symplektické geometrie, aplikace v optimálním řízení a analytické mechanice, další příklady rovnic matematické fyziky.

Okruhy otázek bloku 1

1. Konvexní analýza. Konvexní množiny, konvexní obaly, teorie oddělitelnosti, konvexní funkce, kritéria konvexnosti pro diferencovatelné funkce, subgradient a subdiferenciál, Fenchelova transformace, řešení systémů lineárních a konvexních nerovností.

2. Matematické programování. Metody nepodmíněné minimalizace (Fibonacciho metoda, metoda zlatého řezu, Newtonova metoda atd.), Langrangeův princip, podmínky optimality, Kuhnovy-Tuckerovy podmínky, konvexní programování, slabá a silná dualita, sedlové body, stínová cena.

3. Obecná teorie ODR. Carathéodoryho třída funkcí, existence a jednoznačnost řešení rovnic s nespojitou pravou stranou, Carathéodoryho věta pro rovnice vyšších řádů, prodloužitelnost řešení, globální řešení, dolní a horní řešení, Wintnerova věta, Kneserova věta, Fukuharovy věty.

4. Kompaktní a samoadjungované operátory. Banachova věta o inverzním operátoru, spektrum operátoru, adjungované a samoadjungované operátory, vlastnosti kompaktních operátorů v Banachových prostorech, Volterrovy a Fredholmovy operátory, Hilbertova-Schmidtova věta.

5. Nelineární funkcionální analýza. Gateauxova a Fréchetova derivace, striktně a uniformně konvexní prostory, konvexní funkce v prostorech nekonečné dimenze, projekce, integrace v Banachových prostorech, věty o pevném bodu a jejich aplikace v teorii diferenciálních rovnic.

6. Fourierovy řady. Ekvivalentní tvary Fourierových řad, Dirichletovo jádro a bodová konvergence, Fejérovo jádro a konvergence v průměru, konvergence v normě, L^1 a L^2 prostory, konvoluce a korelace, Parsevalovy identity, vícerozměrné Fourierovy řady.

7. Fourierova transformace. Existence a vlastnosti Fourierovy transformace, příklady, Fourierova věta, Plancherelova věta, konvoluce, korelace, Parsevalovy identity, inverzní Fourierova transformace, Schwartzův prostor, zobecnění Fourierovy transformace – distribuce.

8. Autonomní rovnice. Typy singulárních bodů dvojrozměrných systémů, klasifikace singulárních bodů lineárních a perturbovaných lineárních systémů, struktura limitní množiny v R^2, Dulacovo kritérium, Poincarého-Bendixsonova věta, charakteristické směry.

Okruhy otázek bloku 2

1. Funkcionální analýza I. Banachovy a Hilbertovy prostory, Rieszova-Fischerova věta, Hahnova-Banachova věta a její aplikace, duální prostor, Banachova-Steinhausova věta, slabá konvergence.

2. Funkcionální analýza II. Lineární operátory, spojitost a ohraničenost; adjungované operátory, samoadjungované operátory v Hilbertově prostoru, kompaktní operátory; definice spektra lineárního operátoru, klasifikace bodů spektra, spektrum kompaktního operátoru; aplikace na integrální operátory.

3. Komplexní analýza. Základní koncepty komplexní analýzy v jedné a více proměnných, porovnání rozdílů, Hartogsův jev; integrální reprezentace holomorfních funkcí, Bergmanovo jádro; základy CR geometrie.

3. Diferenciální geometrie. Základní koncepce geometrických struktur, bandly reperů, jety, geometrická pole jako řezy asociovaných bandlů, hlavní a asociované konexe; symetrie diferenciálních operátorů a geometrický přístup k nelineárním PDR.

4. Algebraická topologie I. CW-komplexy. Simpliciální homologie. Singulární homologie a kohomologie. (Ko)homologie CW-komplexů. Součiny v kohomologiích. Poincarého dualita.

6. Algebraická topologie II. Homotopické grupy. Fibrace a kofibrace. Fundamentální grupa, van Kampenova věta. Hurewitzova věta. Whiteheadova věta. Věta o výřezu, Freudenthalova věta.

7. Algebraická geometrie I. Rezultanty, Groebnerovy báze. Afinní variety. Hilbertova věta o nulách. Polynomiální funkce, vztah afinních variet a algeber.

8. Algebraická geometrie II. Projektivní variety. Regulární zobrazení, dominantní zobrazení, biracionální ekvivalence, vztah kvaziprojektivních variet a rozšíření. Dimenze variety. Tečný prostor. Bezoutova věta.

Okruhy otázek bloku 3

1. Galoisova teorie. Algebraická, jednoduchá a konečná rozšíření těles. Klasické konstrukce pravítkem a kružítkem. Rozkladová tělesa a normální rozšíření, algebraický uzávěr. Separabilní a neseparabilní rozšíření. Základní věta Galoisovy teorie. Cyklická a radikálová rozšíření. Řešitelné grupy, souvislost s vyjadřováním kořenů polynomů v radikálech.

2. Základy teorie kategorií. Kategorie, funktory, přirozené transformace. Yonedovo lemma. Limity a kolimity.

3. Teorie kategorií. Adjungované funktory, Freydova věta. Kartézsky uzavřené kategorie. Monoidální kategorie.

4. Algebraická topologie I. CW-komplexy. Simpliciální homologie. Singulární homologie a kohomologie. (Ko)homologie CW-komplexů. Součiny v kohomologiích. Poincarého dualita.

5. Algebraická topologie II. Homotopické grupy. Fibrace a kofibrace. Fundamentální grupa, van Kampenova věta. Hurewitzova věta. Whiteheadova věta. Věta o výřezu, Freudenthalova věta.

6. Algebraická geometrie I. Rezultanty, Groebnerovy báze. Afinní variety. Hilbertova věta o nulách. Polynomiální funkce, vztah afinních variet a algeber.

7. Algebraická geometrie II. Projektivní variety. Regulární zobrazení, dominantní zobrazení, biracionální ekvivalence, vztah kvaziprojektivních variet a rozšíření. Dimenze variety. Tečný prostor. Bezoutova věta.

8. Hry v normální a rozšířené formě. Hra n hráčů v normální formě, rovnovážné situace, maticová a bimaticová hra, úloha o dohodě, opakované hry, hra v rozšířené formě.

Okruhy otázek bloku 4

1. Hry v normální a rozšířené formě. Hra n hráčů v normální formě, rovnovážné situace, maticová a bimaticová hra, úloha o dohodě, opakované hry, hra v rozšířené formě.

2. Koaliční hry. Hra ve tvaru charakteristické funkce, jádro, von Neumannovo-Morgensternovo řešení, Shapleyho vektor. Teorie sociálního výběru.

3. Základy teorie kategorií. Kategorie, funktory, přirozené transformace. Yonedovo lemma. Limity a kolimity.

4. Teorie kódování. Entropie, podmíněná entropie, informace a jejich vztahy a vlastnosti. Věta o kódování bez šumu pro zdroje bez paměti. Kompaktní kódování. Šumový kanál, jeho kapacita a Shannonova věta o kódování pro šumové kanály. Samoopravné kódy. Lineární kódy. Cyklické kódy.

5. Základy kryptografie. Kryptografie a její cíle, Kerckhoffsův princip, základní kryptoanalytické útoky, kryptografické elementy, kryptografické protokoly, starověké šifrování, lineární posuvné registry, symetrické blokové a proudové šifry (operační módy, DES, AES). Problematika eliptických křivek.

6. Kryptografie. Asymetrický šifrovací systém, příklady algoritmů, základy použití. Jednocestné funkce. Hashovací funkce v kryptografii, generování klíčů, digitální podpisy (RSA, DH), ukládání hesel. Řízení přístupu - identifikace, autentizace. Možnosti autentizace (hesla, biometriky, čipové karty, certifikáty).

7. Teorie grafů. Orientované a neorientované grafy a jejich reprezentace. Toky v sítích. Hranová a vrcholová souvislost. Eulerovské a hamiltonovské grafy. Párování. Obarvování vrcholů a hran. Rovinné grafy.

8. Matematická logika. Predikátová logika, axiomy a sémantika. Věta o korektnosti, věta o dedukci. Gödelova věta o úplnosti. Věta o kompaktnosti, Löwenheimova-Skolemova věta. Turingův stroj, Gödelova věta o neúplnosti.
