

## **Požadavky k SZZ – program Matematika**

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 jisté 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**

Ústní část státní závěrečné zkoušky magisterského programu Matematikase skládá ze společných požadavků pro celý program a z požadavků užšího zaměření. Toto zaměření si posluchač určí volbou tří z tématických okruhů 1 – 12 uvedených níže. Z těchto tří okruhů bude posluchači vybrána jedna otázka, rovněž z tématických okruhů A, B, C obdrží posluchač jednu otázku.

### **Vymezení rozsahu otázek k ústní zkoušce**

### **Okruhy otázek společných pro celý program**

**A. Parciální diferenciální rovnice**

PDR 1. řádu, metoda charakteristik, příklady lineárních a nelineárních rovnic a jejich užití, Fourierova metoda, srovnání řešení PDR a ODR, analytická řešení, věta Cauchyova-Kowalevské. 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. Sobolevovy prostory, variační formulace řešení, zobecněná formulace okrajových úloh, teorie stop, slabá řešení eliptických, parabolických a hyperbolických PDR, regularita řešení, variační metody, metoda konečných prvků.

**B. Homologická algebra, moduly, teorie reprezentací**

Základní pojmy teorie kategorií, součiny, součty, jádra a kojádra v kategorii modulů, volné a projektivní moduly, tenzorový součin, ploché moduly, injektivní moduly, injektivní obal, noetherovské okruhy. Řetězcové komplexy, exaktnost, homologie. Projektivní a injektivní rezolventy. Derivované funktory. Vztah Ext a rozšíření modulů. Projektivní a injektivní dimenze. Lineární reprezentace grup, grupové okruhy a moduly nad nimi. Ireducibilní reprezentace, rozložitelnost na přímé součty ireducibilních reprezentací. Charaktery grup, ortogonalita. Aplikace v teorii konečných grup.

**C. Analýza na varietách, Lieovy grupy a základy geometrických struktur**

Vektorová pole a vnější formy na  $\{\mathbb{R}^n\}$ , podvarietách  $\{\mathbb{R}^n\}$  a varietách, obecná Stokesova věta a její důsledky ve vektorovém počtu, geometrická teorie PDR 1. řádu (diferenciální ideály, Frobeniova věta). 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. Základní koncepty riemannovské a symplektické geometrie, aplikace v optimálním řízení a analytické mechanice, další příklady rovnic matematické fyziky.

**Okruhy otázek užšího zaměření****1. Konvexní analýza a matematické programování**

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

## 2. 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. Typy singulárních bodů dvojrozměrných systémů, klasifikace singulárních bodů lineárních a perturbovaných lineárních systémů, struktura limitní množiny v  $\mathbb{R}^2$ , Dulacovo kritérium, Poincarého-Bendixsonova věta, charakteristické směry.

## 3. Funkcionální analýza

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

## 4. Fourierova analýza

Ekvivalentní tvary Fourierových řad, Dirichletovo jádro a bodová konvergence, Fejérové jádro a konvergence v průměru, konvergence v normě,  $L^1$  a  $L^2$  prostory, konvoluce a korelace, Parsevalovy identity, vícerozměrné Fourierovy řady. Existence a vlastnosti Fourierovy transformace, příklady, Fourierova věta, Plancherelova věta, konvoluce, korelace, Parsevalovy identity, inverzní Fourierova transformace, Schwartzův prostor, zobecnění Fourierovy transformace – distribuce.

## 5. Komplexní analýza

Základní koncepty komplexní analýzy v jedné a více proměnných, porovnání rozdílů těchto konceptů, Hartogův jev. Integrální reprezentace holomorfních funkcí, Bergmanovo jádro. Základy CR geometrie.

## 6. Diferenciální geometrie

Základní koncepty geometrických struktur, bandly reперů, jety, geometrická pole jako řezy asociovaných bandlů, hlavní a asociované konexe. Symetrie diferenciálních operátorů a geometrický přístup k nelineárním PDR.

## 7. Algebraická topologie

Pojem homotopie a homotopické ekvivalence, kofibrace, fibrace. CW-komplexy, simplicialní homologie, singulární homologie a kohomologie, výpočet homologií CW-komplexů, součiny v kohomologiích. Poincarého dualita, homotopické grupy, van Kampenova věta, Whiteheadova věta. Věta o výřezu pro homotopické grupy, Freudenthalova věta, Hurewiczova věta.

## 8. Algebraická geometrie

Rezultanty, Groebnerovy báze. Afinity variety. Hilbertova věta o nulách. Polynomiální funkce, vztah afinity variety a algeber. Projektivní variety. Regulární zobrazení, dominantní

zobrazení, biracionální ekvivalence, vztah kvaziprojektivních variet a rozšíření. Dimenze variety. Tečný prostor. Bezoutova věta.

### **9. Galoisova teorie a její aplikace**

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

### **10. Teorie kategorií**

Kategorie, funktory, přirozené transformace. Yonedovo lemma. Limity a kolimity. Adjungované funktory, Freydova věta. Kartézsky uzavřené kategorie. Monoidální kategorie.

### **11. Teorie her**

Hra  $n$  hráčů v normální formě, rovnovážné situace, maticová a bimaticová hra, úloha o dohodě, opakované hry, hra v rozšířené formě. Hra ve tvaru charakteristické funkce, jádro, von Neumannovo-Morgensternovo řešení, Shapleyho vektor. Teorie sociálního výběru.

### **12. Teorie kódování a kryptografie**

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 a cyklické kódy. Kryptografie a její cíle, základní kryptoanalytické útoky, kryptografické elementy, kryptografické protokoly, symetrické blokové a proudové šifry (operační módy, DES, AES). Asymetrický šifrovací systém, příklady algoritmů, základy použití. Jednocestné funkce. Problematika eliptických křivek.