

Zkoušený nejprve v písemném testu stručně zodpoví 10 otázek na znění definic a vět, znalost základních příkladů a aplikace teorie a elementární početní úlohy a poté dostane dvě teoretické otázky, jednu z první půlky semestru a jednu z druhé půlky semestru, na které si připraví odpovědi.

Níže jsou uvedeny nejprve teoretické otázky a dále seznam otázek, z nichž bude sestaven úvodní test. Nutnou podmínkou absolvování zkoušky je aspoň padesátiprocentní úspěšnost v testu:

Otázka 1:

1. Booleovy algebry, Booleovy okruhy. Popis kongruencí a podalgeber na Booleových algebrách pomocí Booleových okruhů.

1. Vztah ireducibilní prvky a prvočinitelů komutativního monoidu s krácením. Jednoznačnost ireducibilního rozkladu.

1. Rozklad prvků oboru integrity hlavních ideálů na prvočinitele.

1. Eukleidovský obor integrity: jeho ideály, hledání největších společných dělitelů a vztah k UFD oborům.

1. Struktura konečné multiplikativní grupy tělesa.

1. Konstrukce kořenového a rozkladového nadtělesa polynomu.

1. Minimální polynom algebraického prvku: existence a jeho vztah ke kořenovým nadtělesům.

1. Vztah stupně minimálního polynom algebraického prvku a jednoduchého rozšíření.

Otázka 2:

2. Existence algebraického uzávěru.

2. Galoisovy grupy Galoisových rozšíření a vztah Galoisových grup pak $Gal(V/U)$, $Gal(V/T)$ a $Gal(U/T)$ pro Galoisova rozšíření $T \subseteq U \subseteq V$.

2. Konečné těleso jako rozkladové nadtěleso.

2. Existence ireducibilního polynomu stupně n nad konečným komutativním tělesem.

2. Nástin algoritmu bezčtvercového rozkladu polynomu nad konečným tělesem.

2. Nástin algoritmu ireducibilní rozklad bezčtvercového polynomu nad konečným tělesem.

2. Algebry jako homomorfní obrazy absolutně volné algebry.

2. Variety algeber a jejich popis pomocí uzávěrových vlastností.

Otázky testu:

1. BOOLEOVY OKRUHY

Definujte Booleův okruh.

Kdy je Booleův okruh oborem integrity?

Uveďte příklad Booleova okruhu.

Popište konstrukci Booleova okruhu na Booleově algebře.
 Popište konstrukci Booleovy algebry na Booleově okruhu.
 Jak souvisí kongruence a podalgebry Booleovy algebry a Booleova okruhu?
 Kolik kongruencí existuje na Booleově algebře o 2^n prvků?
 Kolik kongruencí existuje na Booleově okruhu o 2^n prvků?

2. DĚLITELNOST

Zaveďte relace dělení a asociovanosti na komutativním monoidu s krácením.
 Zaveďte relace dělení a asociovanosti na oboru integrity.
 Popište relaci dělení a asociovanosti na oboru integrity pomocí ideálů.
 Kdy tvoří relace dělení na komutativním monoidu s krácením uspořádání?
 Definujte v komutativním monoidu s krácením největší společný dělitel.
 Definujte v komutativním monoidu s krácením ireducibilní prvek.
 Definujte v komutativním monoidu s krácením prvočinitel.
 Je v oboru integrity každý prvočinitel ireducibilním prvkem? Pokud ne, uveďte příklad.
 Je v oboru integrity každý ireducibilní prvek prvočinitelem? Pokud ne, uveďte příklad.
 Vyslovte tvrzení o jednoznačnosti ireducibilního rozkladu v komutativním monoidu s krácením.
 Vyslovte tvrzení o existenci a jednoznačnosti ireducibilního rozkladu v oborech integrity hlavních ideálů.

3. OBORY HLAVNÍCH IDEÁLŮ

Co je obor integrity hlavních ideálů?
 Definujte obor UFD.
 Uveďte příklad oboru integrity, který není oborem integrity hlavních ideálů.
 Uveďte příklad oboru integrity, který není eukleidovský.
 Definujte eukleidovský obor integrity.
 Uveďte nějakou eukleidovskou funkci na podokruhu $\mathbf{Z}[i]$ okruhu komplexních čísel.
 Uveďte nějakou eukleidovskou funkci na oboru polynomů $\mathbf{R}[x]$ s reálnými koeficienty.
 Rozhodněte, zda je obor $\mathbf{Z}[i]$ eukleidovský. Stručně vysvětlete.
 Rozhodněte, zda je obor $\mathbf{Z}[\sqrt{5}]$ eukleidovský. Stručně vysvětlete.
 Rozhodněte, zda je obor $\mathbf{Z}[x]$ eukleidovský. Stručně vysvětlete.
 Rozhodněte, zda je obor $\mathbf{Z}_2[x]$ eukleidovský. Stručně vysvětlete.
 Rozhodněte, zda je obor $\mathbf{Q}[x]$ eukleidovský. Stručně vysvětlete.
 Rozhodněte, zda je obor $\mathbf{Z}_7[x]$ eukleidovský. Stručně vysvětlete.
 Je v eukleidovském oboru každý prvočinitel ireducibilním prvkem?

4. POLYNOMY

Definujte násobení v monoidovém okruhu.
 Definujte sčítání v monoidovém okruhu.
 Definujte stupeň polynomu.
 Uveďte příklad polynomů, pro něž $\deg p \cdot q < \deg p + \deg q$.
 Pro které okruhy R platí, že $\deg(p + q) \leq \max(\deg p, \deg q) \forall p, q \in R[x]$?
 Pro které okruhy R je $R[x]$ obor integrity?
 Vyslovte větu o dělení se zbytkem v oborech polynomů.
 Vyslovte větu o dělení se zbytkem v oborech polynomů nad tělesem.

Lze polynom $X^{17} + X^4 + 2$ vydělit se zbytkem polynomem $2X^2 + 1$ v oboru $\mathbf{Z}[x]$?
 Lze polynom $X^{17} + X^4 + 2$ vydělit se zbytkem polynomem $2X^2 + 1$ v oboru $\mathbf{Q}[x]$?
 Lze polynom $X^{17} + X^4 + 2$ vydělit se zbytkem polynomem $2X^2 + 1$ v oboru $\mathbf{Z}_3[x]$?
 Definujte dosazovací homomorfismus na komutativním okruhu polynomů.
 Definujte kořen a vícenásobný kořen polynomu.
 Co znamená, že se polynom rozkládá na kořenové činitele?
 Jak souvisí stupeň polynomu nad oborem a počet jeho kořenů?
 Definujte derivaci polynomu.
 Popište vícenásobný kořen polynomu pomocí derivace.
 Má polynom $X^{12} - x$ vícenásobný kořen v oboru $\mathbf{Z}_3[x]$? Stručně zdůvodněte.
 Má polynom $X^{12} - 1$ vícenásobný kořen v oboru $\mathbf{Z}_3[x]$? Stručně zdůvodněte.
 Má polynom $X^{11} - 1$ vícenásobný kořen v oboru $\mathbf{Z}_3[x]$? Stručně zdůvodněte.
 Má polynom $X^{22} - x$ vícenásobný kořen v oboru $\mathbf{Z}_{11}[x]$? Stručně zdůvodněte.
 Má polynom $X^{22} - 1$ vícenásobný kořen v oboru $\mathbf{Z}_{11}[x]$? Stručně zdůvodněte.
 Má polynom $X^{22} - x$ vícenásobný kořen v oboru $\mathbf{Z}_{11}[x]$? Stručně zdůvodněte.
 Má polynom $X^{22} - 1$ vícenásobný kořen v oboru $\mathbf{C}[x]$? Stručně zdůvodněte.

5. KOŘENOVÁ A ROZKLADOVÁ NADTĚLESA

Uveďte definici kořenového a rozkladového nadtělesa polynomu.
 Definujte stupeň rozšíření těles.
 Vyslovte tvrzení o existenci kořenového nadtělesa polynomu.
 Vyslovte tvrzení o existenci a jednoznačnosti rozkladového nadtělesa polynomu.
 Je stupeň kořenového nadtělesa polynomu jednoznačně určen polynomem? Stručně vysvětlete.
 Je stupeň kořenového nadtělesa ireducibilního polynomu jednoznačně určen polynomem? Stručně vysvětlete.
 Je stupeň rozkladového nadtělesa polynomu jednoznačně určen polynomem? Stručně vysvětlete.
 Určete stupeň rozšíření kořenového nadtělesa polynomu $x^2 + 1$ nad tělesem \mathbf{Q} . Stručně zdůvodněte.
 Určete stupeň rozšíření kořenového nadtělesa polynomu $x^2 + 1$ nad tělesem \mathbf{R} . Stručně zdůvodněte.
 Určete stupeň rozšíření kořenového nadtělesa polynomu $x^2 + 1$ nad tělesem \mathbf{Z}_3 . Stručně zdůvodněte.
 Existuje prvek řádu 5 v multiplikační grupě tělesa \mathbf{Z}_{67} ? Stručně zdůvodněte.
 Existuje prvek řádu 66 v multiplikační grupě tělesa \mathbf{Z}_{67} ? Stručně zdůvodněte.
 Existuje prvek řádu 6 v multiplikační grupě tělesa \mathbf{Z}_{67} ? Stručně zdůvodněte.
 Existuje prvek řádu 11 v multiplikační grupě tělesa \mathbf{Z}_{67} ? Stručně zdůvodněte.
 Existuje prvek řádu 12 v multiplikační grupě tělesa \mathbf{Z}_{67} ? Stručně zdůvodněte.

6. MINIMÁLNÍ POLYNOMY A ALGEBRAICKÉ PRVKY

Definujte algebraický prvek a algebraické rozšíření těles.
 Co je minimální polynom algebraického prvku nad tělesem?
 Je-li $T \subseteq U$ rozšíření těles a $\alpha \in U$, popište kdy $T[\alpha] \neq T(\alpha)$.
 Je-li $T \subseteq U$ rozšíření těles a $\alpha \in U$, popište kdy $T[\alpha] = T(\alpha)$.
 Je-li $T \subseteq U$ rozšíření těles a $\alpha \in U$, popište kdy je $[T(\alpha) : T]$ konečné.
 Jak souvisí stupeň minimálního polynomu algebraického prvku se stupněm rozšíření?
 Rozhodněte, zda je prvek $\sqrt{5} + \sqrt[4]{13} \in \mathbf{R}$ algebraický nad tělesem \mathbf{Q} . Stručně zdůvodněte.

Rozhodněte, zda je prvek $2^{-\frac{3}{7}} + 3 \in \mathbf{R}$ algebraický nad tělesem \mathbf{Q} . Stručně zdůvodněte.
 Určete stupeň minimálního polynomu prvku $i \in \mathbf{C}$ nad tělesem \mathbf{Q} . Stručně zdůvodněte.
 Určete stupeň minimálního polynomu prvku $i \in \mathbf{C}$ nad tělesem \mathbf{R} . Stručně zdůvodněte.
 Určete stupeň minimálního polynomu prvku $i - \sqrt{15} \in \mathbf{C}$ nad tělesem \mathbf{R} . Stručně zdůvodněte.

Určete stupeň minimálního polynomu prvku $\frac{1}{\sqrt{15}-11} \in \mathbf{R}$ nad tělesem \mathbf{Q} . Stručně zdůvodněte.

7. ROZKLADOVÁ NADTĚLESA A GALISOVA TEORIE

Definujte pojem rozkladového nadtělesa polynomu.

Definujte algebraický uzávěr tělesa a uveďte nějaký příklad.

Vyslovte tvrzení o existenci a jednoznačnosti rozkladového nadtělesa polynomu.

Jak vypadá rozkladové nadtěleso polynomu $X^2 + 1$ nad tělesem \mathbf{R} ?

Jak vypadá rozkladové nadtěleso polynomu $X^2 + 1$ nad tělesem \mathbf{Q} ?

Jak vypadá rozkladové nadtěleso polynomu $X^3 - 2$ nad tělesem \mathbf{R} ?

Jak vypadá rozkladové nadtěleso polynomu $X^3 - 2$ nad tělesem \mathbf{Q} ?

Definujte Galoisovo rozšíření.

Je rozšíření $\mathbf{Q} \subseteq \mathbf{Q}[\sqrt{5}]$ Galoisovo?

Je rozšíření $\mathbf{Q} \subseteq \mathbf{Q}[\sqrt[3]{5}]$ Galoisovo?

8. ABELOVA-RUFFINIHO VĚTA A GALISOVY GRUPY

Definujte Galoisovu grupu rozšíření těles.

Existuje nějaká nekonečná Galoisova grupa Galoisova rozšíření? Stručně vysvětlete.

Je vpadá Galoisova grupa rozšíření $\mathbf{Q} \subseteq \mathbf{Q}[\sqrt{3}]$?

Je vpadá Galoisova grupa rozšíření $\mathbf{Q} \subseteq \mathbf{Q}[\sqrt[3]{2}]$?

Je vpadá Galoisova grupa rozšíření $\mathbf{R} \subseteq \mathbf{C}$?

Pro $T \subseteq U \subseteq V$ Galoisova rozšíření komutativních těles vyslovte tvrzení o vztahu Galoisových grup pak $Gal(V/U)$, $Gal(V/T)$ a $Gal(U/T)$.

Co znamená, že je polynom řešitelný v radikálech?

Vyslovte tvrzení o vztahu řešitelnosti polynomu v radikálech a řešitelností vhodné grupy.

Vyslovte nějakou verzi Abelovy-Ruffiniho věty o řešitelnosti polynomů.

9. KONEČNÁ TĚLESA

Vyslovte tvrzení o existenci a jednoznačnosti konečných komutativních těles dané velikosti.

Kolik existuje neizomorfních těles o 50 prvcích? Stručně zdůvodněte.

Kolik existuje neizomorfních těles o 49 prvcích? Stručně zdůvodněte.

Kolik existuje neizomorfních těles o 47 prvcích? Stručně zdůvodněte.

Vyslovte tvrzení o existenci ireducibilních polynomů nad konečnými komutativními tělesy.

Existuje ireducibilní polynom stupně 2 nad tělesem o 4 prvcích?

Vyslovte tvrzení o existenci podtěles konečných komutativních těles.

Kolik podtěles obsahuje 64-prvkové těleso? Stručně zdůvodněte. Stručně zdůvodněte.

Existuje podtěleso o čtyřech prvcích 32-prvkového tělesa? Stručně zdůvodněte.

Existuje podtěleso o čtyřech prvcích 16-prvkového tělesa? Stručně zdůvodněte.

Co je bezčtvercový rozklad a je k dispozici pro každý nekonstantní polynom?

10. VOLNÉ ALGEBRY A VARIETY

Zkonstruujte volnou algebrou termů.

Vyslovte tvrzení o tom, jak dostat libovolnou algebru z algebry termů.

Kdy jsou dvě algebry termů izomorfní?

Definujte součin algeber.

Definujte pojem varieta algeber.

Co znamená, že algebra splňuje nějakou identitu?

Vyslovte Birkhoffovu větu charakterizující variety algeber.