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 půky semestru a jednu z druhé půlky semestru, na které si připraví odpovědi. Spíše než technické detaily důkazů je třeba znát jejich základní myšlenku.

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 ireducibilních prvků a prvočinitelů komutativního monoidu s krácením. Jednoznačnost ireducibilního rozkladu.

1. Rozklad prvků oboru integrity hlavních ideálů na prvočinitele.

1. Eukeidovský obor: příklady, 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. Jednoznačnost kořenového a rozkladového nadtělesa polynomu.

2. Existence algebraického uzávěru.

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

2. Řešitelnost polynomu v radikálech a Galoisova grupa jeho rozkladového nadtělesa.

2. Konečné těleso jako rozkladové nadtěleso tělesa $\mathbb{Z}_p$.

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.

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 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 $\mathbb{Z}[i]$ eukleidovský. Stručně vysvětlete.
Rozhodněte, zda je obor $\mathbb{Z}[\sqrt{5}]$ eukleidovský. Stručně vysvětlete.
Rozhodněte, zda je obor $\mathbb{Z}[x]$ eukleidovský. Stručně vysvětlete.
Rozhodněte, zda je obor $\mathbb{Z}_2[x]$ eukleidovský. Stručně vysvětlete.
Rozhodněte, zda je obor $\mathbb{Q}[x]$ eukleidovský. Stručně vysvětlete.
Rozhodněte, zda je obor $\mathbb{Z}_7[x]$ eukleidovský. Stručně vysvětlete.
Je v eukleidovském oboru každý prvočinitel ireducibilním prvkem?

4. Polynomy a mocninné řady

Definujte násobení v okruhu formálních Laurentových řad.
Které prvky oboru formálních mocninných řad nad oborem jsou invertibilní?
Které prvky oboru formálních mocninných řad nad tělesem jsou invertibilní?
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 $R[x]$ je obor integrity?
Je stupeň oboru polynomů nad tělesem eukleidovskou funkcí? Stručně vysvětlete.

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 multiplikativní grupě tělesa $\mathbf{Z}_{67}$? Stručně zdůvodněte.
Existuje prvek řádu 66 v multiplikativní grupě tělesa $\mathbf{Z}_{67}$? Stručně zdůvodněte.
Existuje prvek řádu 6 v multiplikativní grupě tělesa $\mathbf{Z}_{67}$? Stručně zdůvodněte.
Existuje prvek řádu 11 v multiplikativní grupě tělesa $\mathbf{Z}_{67}$? Stručně zdůvodněte.
Existuje prvek řádu 12 v multiplikativní 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 $\alpha \in U$, uveďte postačující podmínku, za níž $T[\alpha] \neq T(\alpha)$.
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 $\sqrt{5} + \sqrt[11]{13} \in \mathbf{R}$ 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 Galoisova teorie

Definujte pojem rozkladového nadtělesa polynomu.

Vyslovte tvrzení o existenci a jednoznačnosti rozkladového nadtělesa polynomu.

Je pro prvočíslo p každé kořenové nadtěleso polynomu $X^p - 1$ nad $\mathbb{Q}$ Galoisovým rozšířením? Vysvětlete.

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

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

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

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

Definujte Galoisovo rozšíření.

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

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

Najděte aspoň dva různé prvky Galoisovy grupy rozšíření $\mathbb{Z}_5 \subseteq F$, kde F je konečné těleso o 125 prvcích. (Uvažte endomorfismy na tělesech kladné charakteristiky.)

8. Abelova-Ruffiniho věta a Galoisovy grupy

Definujte Galoisovu grupu rozšíření těles.

Existuje nějaká nekonečná Galoisovu grupa Galoisova rozšíření? Stručně vysvětlete.

Je vypadá Galoisova grupa rozšíření $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}]$?

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

Je vypadá Galoisova grupa rozšíření $\mathbb{R} \subseteq \mathbb{C}$?

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

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.
Existuje podtěleso o čtyřech prvcích 32-prvkového tělesa? Stručně zdůvodněte.
Existuje podtěleso o čtyřech prvcích 16-prvkového tělesa? Stručně zdůvodněte.

10. IREDUCIBILNÍ ROZKLADY POLYNOMŮ

Co je bezčtvercový rozklad a je k dispozici pro každý nekonstantní polynom?
Je polynom $x^{10} + 3x^5 + 4$ nad tělesem $\mathbb{Z}_5$ bezčtvercový?
Je polynom $x^5 + 3x^2 + x + 3$ nad tělesem $\mathbb{Z}_5$ bezčtvercový?
Je polynom $x^5 + x^2 + 2x + 1$ nad tělesem $\mathbb{Z}_5$ bezčtvercový?
Najděte ireducibilní rozklad polynomu $x^4 - x$ nad tělesem $\mathbb{Z}_2$.
Popište ireducibilní rozklad polynomu $x^4 - x$ nad čtyřprvkovým tělesem.
Vyslovte Čínskou větu o zbytcích pro polynomy nad konečnými tělesy.
Pro která konečná tělesa je zobrazení $t \to t^5$ izomorfismus?
Pro která konečná tělesa je zobrazení $t \to t^{64}$ identita?