Algebra II — Cvičení — podzim 2005

Cvičení 1 — 19. 9. — Ideály

C11 Určete podgrupu grupy $(\mathbb{C}, +)$ generovanou prvkem i. Určete podokruh, podtěleso a ideál okruhu $(\mathbb{C}, +, \cdot)$ generovaný prvkem i. Totéž pro prvky $\sqrt[3]{2}$ a e.

C12 Popište svaz ideálů okruhu $\mathbb{Z}_2 \times \mathbb{Z}_4$.

C13 Ukažte, že ideál $(x, 2)$ není hlavní ideál okruhu $\mathbb{Z}[x]$.

C14 Určete všechny ideály v okruhu $M_2(\mathbb{R})$ (okruh matic typu 2×2 nad reálnými čísly).

C15 Určete maximální ideály v okruhu $\mathbb{R}[x]$.

C16 Pro okruh R a jeho ideály I, J klademe $I + J = \{i + j \mid i \in I, j \in J\}$. Dokažte, že $\cap$ i $+$ jsou operace na množině všech ideálů okruhu R.

Domácí úloha

D1a Pro okruh R a jeho ideály I, J klademe $I \circ J = \{i \cdot j \mid i \in I, j \in J\}$. Rozhodněte, zda $\circ$ je operace na množině všech ideálů okruhu R.

D1b Dokažte, že v okruhu $\mathbb{Z}_n$ je každý ideál hlavní.

Prémiové příklady

P1 Určete pro která $n \in \mathbb{N}$ je v okruhu $\mathbb{Z}_n[x]$ každý ideál hlavní.

P2 Dokažte, že každý ideál okruhu $\mathbb{Z}[x]$ je konečně generovaný.

Cvičení 2 — 26. 9. — Faktorokruhy

C21 Dokažte, že množina všech polynomů, které mají součet koeficinetů dělitelný 3, tvoří v okruhu $\mathbb{Z}[x]$ ideál. Určete čemu je izomorfní příslušný faktorokruh.

C22 Určete čemu je izomorfní faktorokruh $\mathbb{Q}[x]/(x - 2)$.

C23 Určete čemu je izomorfní faktorokruh $\mathbb{Q}[x, y]/(x, y - 1)$.

C24 Ukažte, že faktorokruh $\mathbb{Q}[x, y]/(x^2, y^2)$ je izomorfní okruhu čtvercových matic:

$$\left\{ \begin{pmatrix} d & 0 & 0 & 0 \\ c & d & 0 & 0 \\ b & 0 & d & 0 \\ a & b & c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Q} \right\}.$$

C25 Označme pro prvočíslo p okruh $M_p = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z},\ p \nmid n \right\}$. Popište všechny ideály tohoto okruhu. Určete, které z nich jsou hlavní, které prvoideály a které maximalní ideály.

Domácí úloha

D2 Pro dané přirozené číslo n a celé číslo k označme $I(k, n) = \{f \in \mathbb{Z}[x] \mid n \mid f(k)\}$. Dokažte, že $I(k, n)$ je ideál okruhu $\mathbb{Z}[x]$. Rozhodněte, pro která n, k je tento ideál hlavní, pro která je maximální, pro která je to prvoideál. Nalezněte generátory tohoto ideálu.

Prémiové příklady

P3 Určete čemu jsou izomorfní faktorokruhy příslušné ideálům z příkladu C25.

Cvičení 3 — 3. 10. — Jednoduchá rozšíření a minimální polynomy

C31 Určete, které prvky patří do tělesa $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. Určete dimenze příslušných rozšíření (nad $\mathbb{Q}$).

C32 Buď $\alpha \in \mathbb{C}$ kořenem (ireducibilního) polynomu $x^3 - x - 2 \in \mathbb{Q}[x]$. Určete stupeň rozšíření tělesa $\mathbb{Q}(\alpha)$ nad tělesem $\mathbb{Q}$ a udejte bázi tohoto rozšíření. Vyjádřete prvky α^{-1}, $(1+\alpha)^3$ v této bázi.

C33 Určete, které prvky patří do tělesa $\mathbb{Q}(\pi)$.

C34 Určete minimální polynomy prvku $\sqrt{2+\sqrt{2}}$ nad $\mathbb{Q}$ a nad $\mathbb{Q}(\sqrt{2})$.

C35 Určete minimální polynomy prvků

$$\alpha = \sqrt[3]{4} + \sqrt[3]{2} - 1, \quad \beta = \sqrt{\sqrt{2+\sqrt{2}}+\sqrt{2}}, \quad \gamma = \sqrt{2}+\sqrt{3}, \quad \delta = \sqrt{7+4\sqrt{3}}+\sqrt{7-4\sqrt{3}}.$$

Domácí úloha

D3a Určete všechny inkluze mezi následujícími podtělesy tělesa $\mathbb{C}$: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2},\sqrt{6})$, $\mathbb{Q}(\sqrt{3},\sqrt{6})$, $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{6})$. Určete stupně rozšíření těchto těles nad $\mathbb{Q}$. Jsou tělesa $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt{3})$ izomorfní?

D3b Určete minimální polynom prvku $\sqrt{7+4\sqrt{3}}$ nad $\mathbb{Q}$.

Prémiové příklady

P4 Určete minimální polynom prvku $\sqrt[3]{16+8\sqrt{5}}$.

P1–varianta Dokažte, že je v okruhu $\mathbb{Z}_n[x]$ každý ideál hlavní právě tehdy, když n není dělitelné druhou mocninou prvočísla. Postupně dokažte, že:

- Pokud existuje prvočíslo p takové, že $p^2 \mid n$, pak ideál (x,p) není hlavní ideál v $\mathbb{Z}_n[x]$.
- Pokud n je prvočíslo, pak $\mathbb{Z}_n[x]$ je okruhem hlavních ideálů.
- Pokud n je součinem různých prvočísel $p_1, p_2, \ldots, p_k$, pak okruh $\mathbb{Z}_n[x]$ je izomorfní součinu okruhů $\mathbb{Z}_{p_1}[x]$, $\mathbb{Z}_{p_2}[x]$, $\ldots$,$\mathbb{Z}_{p_k}[x]$.
- Každý ideál I v konečném součinu okruhů je součinem příslušných ideálů v jednotlivých komponentách součinu. Pokud jsou navíc tyto ideály hlavní, je hlavní i původní ideál I.

Cvičení 4 — 10. 10. — Konečná rozšíření a rozkladové těleso

C41 Ukažte, že tělesa $\mathbb{Q}(\sqrt{2})$ a $\mathbb{Q}(\sqrt{3})$ nejsou izomorfní.

C42 Je-li $\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ izomorfismus, pak $\varphi(\alpha)$ má stejný minimální polynom jako α. Dokažte.

C43 Dokažte, že $\mathbb{Q}(\sqrt{2},\sqrt{3})$ je jednoduché rozšíření $\mathbb{Q}$.

C44 Určete všechny automorfismy (izomorfismy na sebe) tělesa $\mathbb{Q}(\sqrt{2})$.

C45 Určete stupeň rozšíření rozkladového tělesa polynomu $x^4 - 2$ nad $\mathbb{Q}$.

C46 Určete stupeň rozšíření rozkladového tělesa polynomu $x^n - 1$ nad $\mathbb{Q}$, pro $n = 3, 4, 5, 6$.

C47 Určete stupeň rozšíření rozkladového tělesa polynomu $x^n - 1$ nad $\mathbb{Q}$, pro n prvočíslo.

C48 Dokažte, že pro polynom stupně n nad $\mathbb{Q}$, je stupeň rozkladového tělesa tohoto polynomu menší nebo roven $n!$.

C49 Uvažujme ireducibilní polynom $f = x^3 + x + 1$ nad $\mathbb{Z}_2$. Popište těleso $\mathbb{Z}_2[x]/(f)$. Určete všechny jeho podtělesa.

Domácí úloha

D4a Určete všechny automorfismy tělesa $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

D4b Určete stupeň rozšíření rozkladového tělesa polynomu $x^3 - 5$ nad $\mathbb{Q}$.

D4c Uvažujme ireducibilní polynom f stupně 4 nad $\mathbb{Z}_2$. Popište těleso $\mathbb{Z}_2[x]/(f)$. Určete všechny jeho podtělesa.

Prémiové příklady

P5 Popište všechna konečná rozšíření tělesa $\mathbb{C}$.

Cvičení 5 — 17. 10. — Konečná tělesa, Grupy automorfismů

C51 Uvažujme šestnáctiprvkové těleso $\mathbb{F}_{16}$. Buď β generátor jeho čtyřprvkového podtělesa.
a) Určete minimální polynom prvku β nad $\mathbb{Z}_2$. Napište jeho rozklad na ireducibilní polynomy nad $\mathbb{Z}_2(\beta)$.
b) Určete všechny ireducibilní polynomy stupně 2 nad $\mathbb{Z}_2(\beta)$.
c) Nechť f je nějaký ireducibilní polynom stupně 2 nad $\mathbb{Z}_2(\beta)$. Nalezněte jeho kořeny v $\mathbb{F}_{16}$. Popište izomorfismus $\mathbb{F}_{16}$ a $\mathbb{Z}_2(\beta)[x]/(f)$.

C52 Uvažujme těleso $\mathbb{F}_{p^n}$ o p^n prvcích a jeho grupu auomorfismů $(Aut(\mathbb{F}_{p^n}), \circ)$. Nechť zobrazení $\iota : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ je definováno vztahem $\iota(x) = x^p$.
a) Dokažte, že ι je automorfismus tělesa $\mathbb{F}_{p^n}$.
b) Ukažte, že ι je prvek řádu n v grupě $(Aut(\mathbb{F}_{p^n}), \circ)$.
c) Ukažte, že $\mathbb{F}_{p^n}$ je jednoduché rozšíření tělesa $\mathbb{F}_p = \mathbb{Z}_p$ a proto existuje právě n automorfismů $\mathbb{F}_{p^n}$. tzn. $(Aut(\mathbb{F}_{p^n}), \circ)$ je n prvková cyklická grupa.

C53 Popište, kolik je homomorfismů z $\mathbb{F}_{p^n}$ do $\mathbb{F}_{q^m}$ a jak vypadají.

C54 Určete grupu automorfismů rozkladového tělesa polynomu $x^5 - 1$ nad $\mathbb{Q}$.

Domácí úloha

D5 Pro některou dvojici f, g různých ireducibilních polynomů stupně 2 nad $\mathbb{Z}_3$ popište všechny homomorfismy z $\mathbb{Z}_3[x]/(f)$ do $\mathbb{Z}_3[x]/(g)$.

Prémiové příklady

P6 Určete grupu automorfismů rozkladového tělesa polynomu $x^4 - 2$ nad $\mathbb{Q}$.

Cvičení 6 — 24. 10. — Symetrické polynomy

C61 Rozložte mnohočlen $f(x, y, z) = (x + y)(x + z)(y + z) + xyz$ pomocí elementárních symetrických polynomů.

C62 Rozložte mnohočlen $f(x, y, z) = x^4 + y^4 + z^4$ pomocí elementárních symetrických polynomů.

C63 Řešte soustavu rovnic:

$$x_1^2 + x_2^2 = \frac{7}{3}$$
$$x_1^3 + x_2^3 = 3$$

C64 Řešte soustavu rovnic:

$$\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1^2 + x_2^2 + x_3^2 &= x_1^3 + x_2^3 + x_3^3 \\ x_1 x_2 x_3 &= 2 \end{aligned}$$

C65 O kubickém polynomu $f(x) = x^3 + x^2 - 1 \in \mathbb{C}[x]$ víme, že má tři různé kořeny x_1, x_2, x_3. Sestavte normovaný kubický polynom, jehož kořeny jsou x_1^3, x_2^3, x_3^3.

Domácí úloha

D6 Buď A množina. Označme následující podmnožiny množiny $\mathcal{P}(A \times A)$:

$S(A)$ množinu všech symetrických relací na množině A,

$T(A)$ množinu všech tranzitivních relací na množině A,

$R(A)$ množinu všech reflexivních relací na množině A,

$E(A)$ množinu všech relací ekvivalence na množině A,

$U(A)$ množinu všech uspořádání na množině A.

Rozhodněte, zda dané množiny uspořádané inkluzí tvoří svaz, resp. úplný svaz. Pokud ano, popište jak vypadají suprema a infima.

Prémiové příklady

P7 Dejte příklad polynomu více proměnných, který není symetrický, ale jeho třetí mocnina je symetrickým polynomem.

P8 Určete, pro které uspořádané množiny $(B, \leq)$ platí, že množina všech podmnožin, které spolu s uspřádáním jsou svazem, tvoří vzhledem k inkluzi svaz. Své tvrzení dokažte.

Cvičení 7 — 31. 10. — Svazy, úplné svazy, podsvazy

C71 V příkladu D6 určete, které podmnožiny tvoří podsvaz svazu $(\mathcal{P}(A \times A), \subseteq)$. Popište maximální prvky $U(A)$ a rozhodněte, zda $U(A) \cup \{\top\}$, kde $\top$ je nový největší prvek, tvoří úplný svaz.

C72 Určete (až na izomorfismus) všechny pětiprvkové a šestiprvkové svazy.

C73 Určete svaz podsvazů svazu M_5.

C74 Určete příklad podmnožiny některého pětiprvkového svazu, která není podsvazem tohoto svazu, přestože společně s indukovaným uspořádáním tvoří svaz.

C75 Obsahuje-li neprázdný svaz pouze konečné řetězce, pak je to úplný svaz. Dokažte.

C76 Uvažujme uspořádané množiny: $(\mathcal{P}_f(\mathbb{N}), \subseteq)$ (konečné podmnožiny $\mathbb{N}$), $(\mathcal{P}(\mathbb{N}), \subseteq)$, $(\mathbb{N}, |)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$, $(Sub(\mathbb{R}^3), \subseteq))$ (podprostory vektorového prostoru $\mathbb{R}^3$). Rozhodněte, zda dané uspořádané množiny tvoří svaz, resp. úplný svaz. Pokud tvoří svaz, který není úplný, dejte příklad nějakého úplného svazu, do kterého lze daný svaz vnořit.

C77 Dokažte, že v konečném svazu je každý ideál (resp. filtr) hlavní. Dejte příklad svazu a nehlavního ideálu v něm.

C78 Pro libovolný svaz $(S, \leq)$ určete všechny ideály, které jsou zároveň filtry.

Domácí úloha

D7 Dokažte, že idempotence v algebraické definici svazu je důsledkem ostatních axiomů.

Prémiové příklady

P9 Nechť $(S, \leq)$ je svaz. Prvek $a \in S$ se nazývá kompaktní, pokud platí:

$$(\forall X \subset S)(supX \geq a \implies (\exists Y \subset X)(Y \text{ konečná } \wedge supY \geq a)).$$

Dokažte, že konečná suprema kompaktních prvků jsou kompaktní.

Úplný svaz $(S, \leq)$ se nazývá algebraický, pokud každý prvek je supremem kompaktních prvků. Ukažte, že

a) svaz všech nekonečných podmnožin $\mathbb{N}$ s prázdnou množinou, uspořádaný inkluzí $(\mathcal{P}_\infty(\mathbb{N}) \cup \{\emptyset\}, \subseteq)$ není algebraický svaz;

b) svaz všech komplementů konečných podmnožin $\mathbb{N}$ s prázdnou množinou, uspořádaný inkluzí $(\mathcal{P}_{fc}(\mathbb{N}) \cup \{\emptyset\}, \subseteq)$ je algebraický svaz;

c) svaz všech podgrup dané grupy je algebraický.

Cvičení 8 — 7. 11. — Kongruence svazů, modulární svazy

C81 = C75

C82 Relace ekvivalence ρ na svazu L se nazývá *kongruence* jestliže splňuje:

$$(\forall a, b, c, d \in L)(a\rho b, c\rho d \implies (a \wedge c)\rho(b \wedge d) \quad (a \vee c)\rho(b \vee d).$$

Dokažte, že platí

a) ρ je kongruence $\iff (\forall a, b, c \in L)(a\rho b \implies (a \wedge c)\rho(b \wedge c) \quad (a \vee c)\rho(b \vee c)$,

b) ρ je kongruence $(\forall a, b \in L)(a\rho b \implies (a \wedge b)\rho a, (a \vee b)\rho a$,

c) ρ je kongruence $(\forall a, b, c \in L)(a \leq b \leq c, a\rho c \implies b\rho a$.

C83 Označme $Con(L)$ množinu všech kongruencí svazu L. Dokažte, že množina $Con(L)$ uspořádaná inkluzí tvoří úplný svaz. Dokažte, že pro libovolnou kongruenci ρ, která je různá od diagonály (identické relace ekvivalence), platí

$$\rho = sup\{\rho_{a,b} \mid a, b \in L, a\rho b\},$$

kde $\rho_{a,b}$ je nejmenší kongruence pro niž jsou v relaci prvky a a b. (Z toho lze odvodit, že $(Con(L), \subseteq)$ je algebraický svaz — nedělalo se.)

C84 Popište svaz kongruencí svazů M_5 a N_5.

C85 Dejte příklad izotonního zobrazeí svazů, které není svazový homomorfismus.

C86 Ve svazu L označujeme $[a, b]$ interval prvků mezi a a b, tj. $[a, b] = \{x \in L \mid a \leq x \leq b\}$. Buďte $a, b \in L$ libovolné prvky modulárního svazu L. Definujme zobrazení $\alpha : [a, a \vee b] \to [a \wedge b, b]$ předpisem $\alpha(x) = x \wedge b$ a podobně zobrazení $\beta : [a \wedge b, b] \to [a, a \vee b]$ předpisem $\beta(x) = x \vee a$. Dokažte, že α a β jsou vzájemně inverzní izomorfismy svazů $[a, a \vee b]$ a $[a \wedge b, b]$.

Domácí úloha

D8 Popište svaz kongruencí svazu, který je součinem dvouprvkového a tříprvkoveho řetězce.

Prémiové příklady

P10 Svaz všech kongruencí svazu je distributivní svaz. Dokažte.

Cvičení 9 — 14. 11. — Distributivní svazy a Boolovy algebry

C91 Ukažte, že svaz podgrup grupy $\mathbb{A}_4$ není modulární.

C92 Určete, pro které množiny A je svaz všech ekvivalencí na množině A distributivní, resp. modulární. Diskutujte tutéž otázku v případě svazu všech symetrických relací a v případě všech tranzitivních relací.

C93 Rozhodněte, zda je svaz všech podprostorů vektorového prostoru $\mathbb{R}^3$ komplementární.

C94 Dokažte, že interval v Boolově algebře je Boolova algebra. Je to Boolova podalgebra?

C95 Označme F množinu všech formulí výrokové logiky nad množinou atomických formulí X (např. $X = \{p, q.r\}$). Na množině F uvažujme relaci $\equiv$ ekvivalence výroků. Dokažte, že $(F/\equiv, \vee, \wedge$ je Boolova algebra. Popište uspořádání množiny $F/\equiv$. Vysvětlete, jak lze chápat ohodnocení formulí. Určete kolik prvků má množina $F/\equiv$.

C96 Dokažte, že konečně generovaný distributivní svaz L je konečný.

Domácí úloha

D9 Rozhodněte, zda svaz podsvazů libovolného svazu je distributivní. (Charakterizujte ty svazy, pro které je svaz jeho podsvazů distributivní. — nepovinné)

Prémiové příklady

P11 Konečný svaz L se nazývá $\vee-$*semimodulární* pokud splňuje

$$(\forall x, y, z)(x \prec y \implies x \vee z = y \vee z \quad \vee \quad x \vee z \prec y \vee z.$$

Analogicky se definuje pojem $\wedge-$semimodulární svazu.

a) Dokažte, že pokud je svaz $\vee-$semimodulární a zároveň $\wedge-$semimodulární, pak je modulární.

b) Ukažte, že svaz všech relací ekvivalencí je $\vee-$semimodulární a není $\wedge-$semimodulární.

c) Dokažte, že každé dva řetězce pokrývajících se prvků se společnýcm nejmenším a největším prvkem jsou v $\vee-$semimodulárním svazu stejně dlouhé, tj. pro $a = a_0 \prec a_1 \prec \cdots \prec a_{n-1} \prec a_n = b$ a $a = b_0 \prec b_1 \prec \cdots \prec b_{m-1} \prec b_m = b$ platí $n = m$. (Diagram semimodulárního svazu, lze tedy kreslit „do pater“.)

P12 Dokažte, že svaz všech podprostorů vektorového prostoru $\mathbb{Q}^3$ je generován následujícími 4 prvky (tj. jednodimenzionálními podprostory) $\langle(1,0,0)\rangle$, $\langle(0,1,0)\rangle$, $\langle(0,0,1)\rangle$, $\langle(1,1,1)\rangle$. (Konečně generovaný modulární svaz tedy nemusí být konečný.)