FILIP KONOPKA

$2 = (1+i)(1-i) = 1 - i^2$

~~AD(3): IREDUCIBILNÍ PRVEK, KTERÝ NENÍ PRVOČINITEL~~

~~$4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ V OBORU $\mathbb{Z}[i\sqrt{3}]$~~

~~→ DVA RŮZNÉ IREDUCIBILNÍ ROZKLADY PRVKU 4~~

ALGEBRA I (NMAG 201) – TEST, 8. ÚNORA 2016

~~PRVEK $1 - i\sqrt{3}$ =~~ $2 \mid (1+i\sqrt{3})(1-i\sqrt{3})$ ALE $2 \nmid (1+i\sqrt{3})$ ANI $2 \nmid (1-i\sqrt{3})$

Tvrzení a definice pečlivě formulujte včetně všech předpokladů. Odpovědi na otázky zdůvodněte. Pokud používáte nějaké netriviální tvrzení z přednášky, uveďte explicitně odkaz (často budete vyzváni, abyste všechna použitá tvrzení zformulovali). Časový limit je 150 minut.

$\mathbb{Z}[\sqrt{5}]$: $4 = 2 \cdot 2 = (-1+\sqrt{5})(1+\sqrt{5})$ $\quad 2 \mid 4$ ALE $2 \nmid (\sqrt{5} \pm 1)$

(1) Definujte charakteristiku okruhu.

(3 body)

3

NECHŤ R JE OKRUH.
CHARAKTERISTIKOU OKRUHU ROZUMÍME NEJMENŠÍ TAKOVÉ n, ŽE $\underbrace{1+1+1+\cdots}_{n\text{-KRÁT}} = 0$; POKUD EXISTUJE; JINAK JE CHARAKTERISTIKA 0.

(2) Formulujte Čínskou větu o zbytcích.

(3 body)

2

NECHŤ $m_1, m_2, \dots, m_n$ JSOU PODVOU NESOUDĚLNÁ PŘIROZENÁ ČÍSLA; $u_1, \dots, u_n$ LIBOVOLNÁ CELÁ ČÍSLA
$M := m_1 \cdot m_2 \cdot \dots \cdot m_n$; PAK $\exists!\, x \in \{1, \dots, M-1\}$ (0)
TAKOVÉ, ŽE JE SPLNĚNA SOUSTAVA KONGRUENCÍ:

$x \equiv u_1 \pmod{m_1}$
$x \equiv u_2 \pmod{m_2}$
$\vdots$
$x \equiv u_n \pmod{m_n}$

(3) Definujte v obecném oboru integrity pojmy ireducibilního prvku a prvočinitele. Uveďte příklad ireducibilního prvku v nějakém oboru integrity, který není prvočinitelem.

(4 body)

2

Příklad?

NECHŤ R JE OBOR INTEGRITY.
- ŘEKNEME, ŽE $a \in R$ JE IREDUCIBILNÍ PRVEK, POKUD JE NENULOVÝ, NEINVERTIBILNÍ A NEMÁ VLASTNÍ DĚLITELE V R.
- PRVOČINITEL $a \in R$ JE TAKOVÝ PRVEK, PRO KTERÝ PLATÍ: $a \neq 0$ $a \mid b \cdot c \Rightarrow a \mid b \vee a \mid c$

(4) Definujte eukleidovskou normu a uveďte dva příklady.

(4 body)

R - OBOR INTEGRITY

EUKLEIDOVSKÁ NORMA $\nu : R \to \mathbb{N}^{\cup\{0\}}$ JE TAKOVÉ ZOBRAZENÍ, PRO KTERÉ
(1) $\nu(0) = 0$
(2) KDYKOLIV $a \mid b$; $a, b \in R$, $b \neq 0$ PAK $\nu(a) \leq \nu(b)$
KOMPATABILITA S DĚLITELNOSTÍ
(3) ABSTRAKTNÍ DĚLENÍ $b \neq 0$
PRO KAŽDOU DVOJICI PRVKŮ $a, b \in R$ $\exists u, v \in R$ ŽE: $a = u \cdot b + v$, PŘIČEMŽ $\nu(v) < \nu(b)$

1,5

PŘÍKLADY:
$R = \mathbb{Z}$, EUKLEIDOVSKÁ NORMA: $\nu(a) = |a|$, $a \in R$

4b. (5) Najděte v $\mathbb{R}[x]$ polynom co nejmenšího stupně, aby

$$f(-1)=2,\quad f(1)=0,\quad f(2)=2 \quad a \quad f(4)=12.$$

1) POLYNOM STUPNĚ 1

$f = ax + b$

$$\left.\begin{array}{l} 2 = -a+b \\ 0 = a+b \\ 2 = 2a+b \\ 12 = 4a+b \end{array}\right\} \text{NEEXISTUJE}$$

2) POLYNOM STUPNĚ 2 ((*) POKRAČOVÁNÍ)

$f(x) = ax^2 + bx + c$

$$\begin{array}{l} 2 = a - b + c \\ 0 = a + b + c \\ 2 = 4a + 2b + c \\ 12 = 16a + 4b + c \end{array} \qquad \oplus\ 2 = 2a + 2c$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 4 & 2 & 1 & 2 \\ 16 & 4 & 1 & 12 \end{array}\right)$$

(4 body)

4b. ~~10b~~ (6) Platí $3x^2-1 \mid\mid x^2+2$ v oboru a) $\mathbb{Q}[x]$, b) $\mathbb{Z}_5[x]$, c) $\mathbb{Z}_7[x]$?

• V $\mathbb{Z}_7[x]$ PLATÍ $3x^2-1 \mid\mid x^2+2$; NEBOŤ $3x^2-1$ SE LIŠÍ OD POLYNOMU x^2+2 POUZE PŘENÁSOBENÍM 5 – A TO JE INVERTIBILNÍ PRVEK ; T.J. $5\cdot(3x^2-1) = x^2+2$

(4 body) PRVEK 5 JE INVERTIBILNÍ V $\mathbb{Z}_7$, NEBOŤ $\mathbb{Z}_7$ JE TĚLESO

~~to~~ a) a b)?

2b. (7) Pro která z následujících těles T existuje ireducibilní polynom stupně 3 v $T[x]$: a) $\mathbb{Z}_3$, b) $\mathbb{Q}$, c) $\mathbb{C}$? V každém ze tří případů odpověď zdůvodněte. Kde ireducibilní polynom existuje, uveďte příklad.

• V $\mathbb{C}[x]$ ŽÁDNÝ IREDUCIBILNÍ POLYNOM STUPNĚ 3 NEEXISTUJE, NEBOŤ KOMPLEXNÍ ČÍSLA JSOU ALGEBRAICKY UZAVŘENÉ TĚLESO, PROTO SE KAŽDÝ POLYNOM ROZKLÁDÁ NA SOUČIN POLYNOMŮ STUPNĚ 1 – (VIZ. KOMPLEXNÍ ANALÝZA)

(5 bodů)

(*) POKRAČOVÁNÍ

2b. (8) Kolik prvků řádu 4 obsahují grupy $(\mathbb{Z}_{17}, +, -, 0)$ a $(\mathbb{Z}_{17}^*, \cdot, ^{-1}, 1)$? Které konkrétně prvky to jsou?

ŘÁD PRVKU JE NEJMENŠÍ TAKOVÉ ČÍSLO, KOLIKRÁT MUSÍME PRVEK SLOŽIT SE SEBOU SAMÝM, ABYCHOM DOSTALI JEDNOTKU.

V $(\mathbb{Z}_{17}^*, \cdot, ^{-1}, 1)$: $2\cdot2\cdot2\cdot2 = 16 \neq 1$

$3\cdot3\cdot3\cdot3 = 13 \neq 1$

(5 bodů)

$4\cdot4\cdot4\cdot4 = 1 \Rightarrow$ 4 JE PRVEK ŘÁDU 4 ?

$5\cdot5\cdot5\cdot5 = 8\cdot8 = 4\cdot15 = 60 = 9 \neq 1$

$6\cdot6\cdot6\cdot6 = 4 \neq 1$

$7\cdot7\cdot7\cdot7 = 1 \Rightarrow$ 7 JE PRVEK ŘÁDU 4 ?

$8\cdot8\cdot8\cdot8 = 13\cdot13 = 169 \neq 1$

$9\cdot9\cdot9\cdot9 = 100-3 = 45 \neq 1$

$10\cdot10\cdot10\cdot10 = 15\cdot15 = 70 = 2 \neq 1$

(*) POKRAČOVÁNÍ

(9) Vezměte množinu T všech polynomů nad $\mathbb{Z}_3$ stupně nejvýše 3 spolu s operacemi sčítání a násobení modulo

$$f = x^4 - x - 1$$

(tento polynom je ireducibilní v $\mathbb{Z}_3[x]$, čili T je těleso o 81 prvcích). Najděte v T multiplikativní inverzi prvku $x^2 + 1$.

(7 bodů)

(10) Formulujte kritérium pro určení násobnosti kořenu polynomu $f \in R[x]$ pomocí formálních derivací f pro obecný obor integrity R.

Najděte všechny prvky $a \in \mathbb{Z}_{103}$, pro které má $x^3 + 9x + a$ v $\mathbb{Z}_{103}$ násobný kořen. Svůj výsledek zdůvodněte.

(10 bodů)

(11) Najděte všechna kladná celočíselná řešení soustavy kongruencí

$$x^2 \equiv -1 \pmod{17},$$
$$2^x \equiv -1 \pmod{17}.$$

(10 bodů)

(12) Definujte pojmy levé rozkladové třídy grupy podle podgrupy a transverzálu levého rozkladu grupy podle podgrupy.

Uvažujte permutační grupu $(S_4, \circ, ^{-1}, \mathrm{id})$ a podmnožinu H všech permutací π takových, že $\pi(1) = 1$. Ukažte, že H je podgrupa S_4 a najděte transverzálu levého rozkladu S_4 podle H.

(12 bodů)

(13) Přesně formulujte a dokažte charakterizaci Gaussových oborů pomocí existence NSD a podmínky na řetězce dělitelů.

(14 bodů)

OBOR INTEGRITY R JE GAUSSŮV PRÁVĚ TEHDY, KDYŽ:

4 • PRO KAŽDOU DVOJICI PRVKŮ EXISTUJE NSD
(TJ. $\forall a, b \in R \; \exists \mathrm{NSD}(a,b)$)

• NEEXISTUJE ŽÁDNÁ KLESAJÍCÍ POSLOUPNOST $a_1, a_2, a_3, \dots$; $a_i \in R \; \forall i$ TAKOVÁ, ŽE $a_{i+1} \mid a_i$; PŘIČEMŽ $a_i \nmid a_{i+1}$

K důkazu potřebujeme: 1) Lemma: $\mathrm{NSD}(ca, cb) = c \cdot \mathrm{NSD}(a,b)$

2) Existuje-li v oboru integrity R NSD všech dvojic prvků, pak platí, že každý ireducibilní prvek v R je prvočinitel.