Algebra — cvičení 5, řešení

3. (a) Nalezněte v $\mathbb{Z}[i]$ NSD čísel $3+i, 4+2i$. Rozložíme na ireducibilní prvky:

- $3+i = (1+i)(2-i)$;
- $4+2i = (1+i)(1-i)(2+i)$.

Řešením je proto $1+i$ (prvky $2-i$ a $2+i$ nejsou asociované).

3. (b) Nalezněte v $\mathbb{Z}[i]$ NSD čísel $3+6i, 12-3i$. Po vydělení třemi dostaneme prvky $1+2i$ a $4-i$, jejichž normy, konkrétně 5 a 17, jsou nesoudělné; musí proto být i $1+2i$ a $4-i$ nesoudělné. Největší společný dělitel zadaných čísel je proto 3.

4. Najděte $a \in \mathbb{N}$ tak, aby ideál $a\mathbb{Z}$ byl roven: a) $28\mathbb{Z} + 63\mathbb{Z}$; b) $15\mathbb{Z} + 18\mathbb{Z} + 40\mathbb{Z}$; c) $(-28)\mathbb{Z} \cap (-63)\mathbb{Z}$. K řešení si vystačíme se dvěma fakty z přednášky: 1) $\mathbb{Z}$ je obor hlavních ideálů; 2) pro hlavní ideály nad jakýmkoliv komutativním okruhem R platí $aR \subseteq bR \iff b \mid a$. V případě (a) takto dostáváme, že $28\mathbb{Z} \subseteq a\mathbb{Z}$ a $63\mathbb{Z} \subseteq a\mathbb{Z}$, což znamená, že a musí být společným dělitelem čísel 28 a 63. Na druhou stranu, když je b společným dělitelem 28 a 63, pak musí $b\mathbb{Z} \supseteq 28\mathbb{Z} + 63\mathbb{Z} = a\mathbb{Z}$. Hledané a proto musí být největším společným dělitelem čísel 28 a 63, tj. $a = 7$.

Podobně v případu (b) dostaneme, že $a = \mathrm{NSD}(15, 18, 40) = 1$. V případu (c) lze využít analogickou úvahu, tentokrát ovšem s obrácenými inkluzemi. Hledané a je proto (kladným) nejmenším společným násobkem čísel -28 a -63, to jest $a = 252$.

5. Nechť $R = \mathbb{Z}[i]$. Najděte $a \in R$ takové, že $aR = (5+3i)R \cap (13+18i)R$. Připomeňme, že $\mathbb{Z}[i]$ je Eukleidův obor, a tedy obor hlavních ideálů. Jako v posledním případu výše hledáme nejmenší společný násobek v $\mathbb{Z}[i]$ prvků $5+3i$ a $13+18i$. Minulý týden jsme on-line spočítali, že ireducibilní rozklady daných čísel jsou:

- $5+3i = (1+i)(4-i)$;
- $13+18i = (4-i)(2+5i)$.

Jejich nejmenším společným násobkem je proto $(13+18i)(1+i) = -5+31i = a$.

6. V $\mathbb{Z}[i\sqrt{3}]$ jsou $(-2)2 = (i\sqrt{3}+1)(i\sqrt{3}-1)$ dva různé ireducibilní rozklady prvku -4. Všechny čtyři prvky mají totiž normu 4, a jelikož v $\mathbb{Z}[i\sqrt{3}]$ neexistují prvky normy 2 (není možno, aby $2 = a^2 + 3b^2$, kde $a, b \in \mathbb{Z}$), jedná se o ireducibilní prvky. Zároveň $2 \nmid (i\sqrt{3}+1)$, jelikož $\frac{i\sqrt{3}+1}{2} \notin \mathbb{Z}[i\sqrt{3}]$, a tedy 2 ani -2 nejsou asociované s $i\sqrt{3}+1$.

Na druhou stranu v $\mathbb{Z}[\sqrt{2}]$ je $\sqrt{2}\sqrt{2} = (-4+3\sqrt{2})(4+3\sqrt{2})$ jeden a tentýž ireducibilní rozklad prvku 2. Předně všechny čtyři prvky mají normu 2, a proto jsou skutečně ireducibilní. Dále $\pm 4 + 3\sqrt{2} = \sqrt{2}(3 \pm 2\sqrt{2})$, kde poslední činitel je invertibilní v $\mathbb{Z}[\sqrt{2}]$. Všechny čtyři prvky jsou proto asociované.

7. Nechť $S = \mathbb{Z}[x]$. Uvažujme ideály $I = 2S + xS$ a $J = 3S + xS$. Ukažte, že množina $\{ab; a \in I, b \in J\}$ netvoří ideál v okruhu S. Dokažte také, že I, J nejsou hlavní ideály.

Označme $M = \{ab; a \in I, b \in J\}$. Všimněme si, že $I = \{a \in S;\ a(0) \text{ je sudé}\}$ a $J = \{b \in S;\ b(0) \equiv 0 \pmod 3\}$. Zřejmě tedy $(-2)x, 3x \in M$. Zároveň ale $3x - 2x = x \notin M$. Proč? Buďte totiž $a = \sum_{i=0}^{m} c_i x^i \in I$ a $b = \sum_{j=0}^{n} d_j x^j \in J$ takové, že $ab = x$. Pak $c_0 d_0 = 0$ a zároveň $c_0 d_1 + c_1 d_0 = 1$. To ale není možné: pokud by $c_0 = 0$, pak $c_1 d_0 = 1$ a dostáváme spor s tím, že $3 \mid d_0$; v opačném případě zase $c_0 d_1 = 1$, což je spor s tím, že c_0 je sudé.

Z toho ihned plyne, že ani I, ani J nemůže být hlavní ideál. Pokud by totiž například $I = fS$, pak by $M = \{fsb;\ s \in \mathbb{Z}[x], b \in J\}$ a tato množina by byla uzavřená na sčítání,

jelikož $fs_1b_1 + fs_2b_2 = f(s_1b_1 + s_2b_2)$ pro libovolné $s_1, s_2 \in \mathbb{Z}[x]$ a $b_1, b_2 \in J$. Zvolíme-li tedy $s = 1$ a $b = s_1b_1 + s_2b_2 \in J$, vidíme, že $f(s_1b_1 + s_2b_2) = fsb \in M$.

Dokázat, že I ani J nejsou hlavní ideály, lze i jinak. Uvažujme nyní, že např. $J = gS$. Stejnou úvahou jako v předchozích příkladech dospějeme k tomu, že g musí být společný dělitel prvků 3 a x. Ovšem v oboru S jsou 3 a x nesoudělné, a tedy $g = \pm 1$, což ovšem zřejmě není prvek ideálu J.

8. Již bylo ukázáno v rámci **4. (c)**.

9. Je-li $u = a + b\sqrt{s}$ invertibilní prvek v $\mathbb{Z}[\sqrt{s}]$ a $b \neq 0$, pak je jistě $u \in \mathbb{R} \setminus \{-1, 1\}$. Využitím multiplikativity normy ν, dostáváme, že i u^n je invertibilní pro libovolné $n \in \mathbb{N}$. Pro druhou část úlohy stačí volit $a = 8$, $b = 3$. (To nějak souvisí s tím, že $8/3$ je v jistém smyslu dobrá aproximace čísla $\sqrt{7}$.)

10. Buď $R = \{f \in \mathbb{Q}[x];\, f(0) \in \mathbb{Z}\}$. Pak je R podokruh oboru $\mathbb{Q}[x]$. Dokažte, že pro libovolné $f, g \in R$ existuje $\mathrm{NSD}(f, g)$. Proč není přesto R Gaussovým oborem? Jistě pro libovolné $f \in R$ platí $\mathrm{NSD}(f, 0) = f$. Můžeme proto dále předpokládat, že $f \neq 0 \neq g$.

Nejdříve uvažujme možnost, že *neplatí* $f(0) = 0 = g(0)$. Pak má i každý největší společný dělitel prvků f, g v oboru $\mathbb{Q}[x]$ nenulový absolutní člen. Uvažujme takový $h = \mathrm{NSD}_{\mathbb{Q}[x]}(f, g)$, že $h(0) = \mathrm{NSD}_{\mathbb{Z}}(f(0), g(0))$. Pak je jistě $h \in R$ a také $\frac{f}{h}(0) = f(0)/h(0) \in \mathbb{Z}$ a $\frac{g}{h}(0) = g(0)/h(0) \in \mathbb{Z}$, což znamená, že h je společným dělitelem prvků f, g v oboru R. Je-li $k \in R$ jakýkoliv společný dělitel f, g v R, pro nějž $h \mid k$, pak je jednak $k = \mathrm{NSD}_{\mathbb{Q}[x]}(f, g)$, a tedy $h \parallel k$ v $\mathbb{Q}[x]$, a jednak $h(0) \mid k(0) \mid f(0)$ a $k(0) \mid g(0)$ v $\mathbb{Z}$, a tedy $k(0) = \mathrm{NSD}_{\mathbb{Z}}(f(0), g(0))$. Dostáváme $k = \pm h$, a tedy $h = \mathrm{NSD}_R(f, g)$.

Nyní nechť $f(0) = 0 = g(0)$. Uvažujme největší $n \in \mathbb{N}$ takové, že $x^n \mid f$ a $x^n \mid g$ platí v $\mathbb{Q}[x]$. Pak má alespoň jeden z polynomů f/x^n, g/x^n nenulový absolutní člen. Ovšem nemusí platit, že absolutní členy těchto polynomů jsou celočíselné. Zvolíme proto nenulové $q \in \mathbb{Q}$ tak, aby $f^* := \frac{f}{qx^n}$ a $g^* := \frac{g}{qx^n}$ ležely v R. Z předchozího odstavce dostaneme $h^* = \mathrm{NSD}_R(f^*, g^*)$. Položíme $h = qx^n h^*$. Pak jistě $h(0) = 0$, a tedy $h \in R$. Nyní už není těžké ověřit, že $h = \mathrm{NSD}(f, g)$.

Nakonec R není Gaussovým oborem, jelikož $x, x/2, x/4, x/8, \ldots$ tvoří v R nekonečnou ostře klesající posloupnost v dělitelnosti. Nenulový a neinvertibilní prvek x proto nemá v R rozklad na ireducibilní prvky. V důsledku existence NSD ale každý prvek z R, který nějaký ireducibilní rozklad má, má tento rozklad jednoznačný (až na pořadí a asociovanost). A samozřejmě ireducibilní prvky jsou totéž, co prvočinitelé. S trochou práce navíc lze ukázat, že R je Bézoutův obor, tj. každý konečně generovaný ideál v R je hlavní. Dokonce je v R možné hledat NSD algoritmem podobným Eukleidovu (nepřekvapivě jsou k dispozici i Bézoutovy koeficienty pro vyjádření NSD). Ideálem v R, který není hlavní, je například $I = \bigcup_{n=0}^{\infty} \frac{x}{2^n} R$.

11. Rozložte polynom $2x^2 + 2x - 1$ nad eukleidovským oborem $\mathbb{Z}[\sqrt{3}]$ na ireducibilní prvky. Není těžké zadaný polynom rozložit v $\mathbb{Q}(\sqrt{3})[x]$ jako $(2x + 1 + \sqrt{3})(x + \frac{1-\sqrt{3}}{2})$. Z Gaussova lemmatu ($\mathbb{Z}[\sqrt{3}]$ je Gaussův) plyne, že jej musí být možné netriviálně rozložit i nad $\mathbb{Z}[\sqrt{3}]$. A skutečně v $\mathbb{Z}[\sqrt{3}]$ je $2 = (\sqrt{3} - 1)(\sqrt{3} + 1)$, v důsledku čehož máme nad $\mathbb{Z}[\sqrt{3}]$ rozklad

$$2x^2 + 2x - 1 = ((\sqrt{3} - 1)x + 1)((\sqrt{3} + 1)x - 1).$$

V rámci tréninku, analogicky k cvičení 6, si můžete vyzkoušet, jak se situace změní, budete-li uvažovat polynom $2x^2 + 2x + 3$ nad oborem $\mathbb{Z}[i\sqrt{5}]$, který není Gaussův.

12. Najděte všechna řešení $u, v \in \mathbb{Z}$ rovnice $u^2 + 2209 = v^3$. Uvažujme, že nějaké řešení $u, v \in \mathbb{Z}$ máme k dispozici. Pak jistě $1 < v$ a v $\mathbb{Z}[i]$ platí $(u+47i)(u-47i) = v^3$. Ukážeme, že čísla $u + 47i$ a $u - 47i$ jsou v $\mathbb{Z}[i]$ nesoudělná. Předpokládejme, že máme jejich nějaký společný dělitel d. Pak d musí dělit i jejich rozdíl, tj. $d \mid 94i = 47(1 + i)^2$, což je rozklad na ireducibilní prvky. Stačí tedy ukázat, že pro $c \in \{1 + i, 47\}$ jest $c \nmid v^3$.

Pokud by $c \mid v^3$, pak také $c \mid v$; vzhledem k tomu, že c je prvočinitel. Následkem toho $c^3 \mid v^3 = (u + 47i)(u - 47i)$, což znamená, že buď $c^2 \mid u + 47i$, nebo $c^2 \mid u - 47i$. Oba případy vedou ke sporu, jelikož $\frac{u \pm 47i}{2i} \notin \mathbb{Z}[i]$ a $\frac{u \pm 47i}{47^2} \notin \mathbb{Z}[i]$. Ukázali jsme, že $u + 47i$ a $u - 47i$ jsou v $\mathbb{Z}[i]$ nesoudělná.

Porovnáním jednoznačných ireducibilních rozkladů levé a pravé strany rovnosti

$$(u + 47i)(u - 47i) = v^3$$

dospějeme k tomu, že $u + 47i = (a + bi)^3$ pro nějaká $a, b \in \mathbb{Z}$. Zaměříme se na koeficienty u i. Dostáváme $47 = 3a^2b - b^3 = b(3a^2 - b^2)$. Rozebereme čtyři možnosti:

- $b = 1$. Pak $3a^2 - 1 = 47$, a tedy $a = \pm 4$. Obdržíme $u = a^3 - 3ab^2 = \pm 4(16 - 3) = \pm 52$ a $v = 17$.
- $b = 47$. Pak $3a^2 - 2209 = 1$, což znamená, že $a^2 = 2210/3$; žádné takové $a \in \mathbb{Z}$ neexistuje.
- $b = -1$. Pak $3a^2 - 1 = -47$, a tedy $a^2 = -46/3$; opět nelze.
- $b = -47$. Pak $3a^2 - 2209 = -1$, což znamená, že $a^2 = 2208/3 = 736$; a takové $a \in \mathbb{Z}$ opět neexistuje.

Zjistili jsme, že jedinými dvěma řešeními zadané diofantické rovnice jsou $u = 52, v = 17$ a $u = -52, v = 17$.