4. Algebrou za kulatější obory a hranatější rozšíření

Okruhová a tělesová rozšíření

1. Popište prvky uvedených oborů a porovnejte je pomocí inkluze:
   (a) $\mathbb{Z}[\sqrt{6}]$, $\mathbb{Z}[\sqrt{24}]$, $\mathbb{Z}[\sqrt{2},\sqrt{3}]$. (b) $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{24}]$, $\mathbb{Q}[\sqrt{2},\sqrt{3}]$.
   [(a) $\mathbb{Z}[\sqrt{24}] \subseteq \mathbb{Z}[\sqrt{6}] \subseteq \mathbb{Z}[\sqrt{2},\sqrt{3}]$. (b) $\mathbb{Q}[\sqrt{6}] = \mathbb{Q}[\sqrt{24}] \subseteq \mathbb{Q}[\sqrt{2},\sqrt{3}]$]

2. Jsou obory $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ a $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ totožné? A jsou totožné obory $\mathbb{Z}[\sqrt{2},\sqrt{3}]$ a $\mathbb{Z}[\sqrt{2}+\sqrt{3}]$? [Ano, položme $a = \sqrt{2}+\sqrt{3}$, pak $\sqrt{2} = \frac{a^2-5}{2} \cdot a - 2a$, podobně pro $\sqrt{3}$.
   Ne; stačí ukázat, že $\sqrt{2} \notin \mathbb{Z}[\sqrt{2}+\sqrt{3}]$. Rozmyslíme si, že pro $\alpha = \sqrt{2}+\sqrt{3}$ máme $\mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 + d\alpha^3 \mid a,b,c,d \in \mathbb{Z}\}$, zatímco $\sqrt{2} = \frac{1}{2}\alpha^3 - \frac{9}{2}\alpha \notin \mathbb{Z}[\alpha]$.]

3. Popište prvky oborů $\mathbb{Q}[\sqrt[3]{s}]$ a $\mathbb{Q}(\sqrt[3]{s})$ pro $s \in \mathbb{Z} \setminus \{0\}$. Jsou totožné?
   [$\mathbb{Q}[\sqrt[3]{s}] = \mathbb{Q}(\sqrt[3]{s}) = \{a + b\sqrt[3]{s} + c\sqrt[3]{s} \mid a,b,c \in \mathbb{Q}\}$, každý polynom $p \in \mathbb{Q}$ umíme vydělit se zbytkem polynomem $x^3 - s$ tak, že $p = q(x^3-s) + r$, kde $\deg(r) < 3$, proto $p(\sqrt[3]{s}) = r(\sqrt[3]{s})$, pokud je $\sqrt[3]{s} \in \mathbb{Q}$ jsou oba obory rovny $\mathbb{Q}$, jinak si všimněme, že $x^3 - s$ je ireducibilní a díky Eukleidově algoritmu umíme pro každý nenulový polynom r stupně < 3 najít $a,b \in \mathbb{Q}[x]$, pro něž $ar + b(x^3 - s) = 1$, tedy $a(\sqrt[3]{})r(\sqrt[3]{}) = 1$ a našli jsme inverz $a(\sqrt[3]{}) \in \mathbb{Q}[\sqrt[3]{s}]$ k prvku $r(\sqrt[3]{s})$.]

Kvadratická rozšíření celých čísel

4. Vydělte v oboru $\mathbb{Z}[i]$ se zbytkem číslo α číslem β, je-li:
   (a) $\alpha = 5+7i$, $\beta = 3-i$ (b) $\alpha = 3+2i$, $\beta = 1+i$
   [(a) 3 možné výsledky: $\alpha = (1+3i)\cdot\beta + (-1-i) = (1+2i)\cdot\beta + (2i) = 3i\cdot\beta + (2-2i)$
   (b) 4 možné výsledky: $3+2i = 2\cdot\beta + 1 = 3\cdot\beta + (-i) = (2-i)\cdot\beta + i = (3-i)\cdot\beta - 1$]

5. Pokud umíme dělit se zbytkem, můžeme provádět Eukleidův algoritmus (jednoznačnost dělení nebyla nikde potřeba). Nalezněte tedy v $\mathbb{Z}[i]$ NSD čísel
   (a) $3+i, 4+2i$ [$1+i$] (b) $3+6i, 12-3i$ [3]

6. Dělte se zbytkem v oboru $\mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[\sqrt{2}i]$ dvojici $(1+4\sqrt{2}i) : (3+\sqrt{2}i)$.
   [$(1+4\sqrt{2}i) = (3+\sqrt{2}i)\cdot(1+\sqrt{2}i)$]

7. Najděte v oboru $\mathbb{Z}[\sqrt{3}]$ nekonečně mnoho invertibilních prvků. [Všimneme si, že $a = 2+\sqrt{3}$ je invertibilní, jelikož má normu 1. Pak prvky $a^k, k \in \mathbb{N}$ jsou také invertibilní a $a^k \neq a^j$, pro $k \neq j$.]

8. Spočtěte $\mathrm{NSD}(6-3\sqrt{3}, 3+\sqrt{3})$ v oboru $\mathbb{Z}[\sqrt{3}]$. [$\sqrt{3}$]

Ireducibilní rozklady

9. Spočítejte v oboru $\mathbb{Z}[i]$ ireducibilní rozklady prvků
   (a) 3 (b) 5 (c) 6 (d) 7 (e) $10-6i$ (f) $9+3i$.
   [(a) $3 = 3$ (b) $5 = (2+i)(2-i)$, $6 = 3(1+i)(1-i)$ (c) $7 = 7$, $10-6i = -(1+i)^3(4+i)$ (d) $9+3i = 3(1+i)(2-i)$]

10. Spočítejte v oboru $\mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[i\sqrt{2}]$ ireducibilní rozklady prvků

    (a) 2 (b) $3 - i\sqrt{2}$ (c) $5 - i\sqrt{2}$

    [(a) $2 = -(i\sqrt{2})^2$ (b) $3 - i\sqrt{2} = 3 - i\sqrt{2}$ (c) $5 - i\sqrt{2} = -(1 + i\sqrt{2})^3$]

11. Spočítejte v uvedených oborech ireducibilní rozklady polynomů $x^3 - 2$, resp. $x^4 - x^2 - 2$:

	$\mathbb{C}[x]$	$\mathbb{R}[x]$	$\mathbb{Q}[x]$	$\mathbb{Z}_3[x]$	$\mathbb{Z}_5[x]$
$x^3 - 2$	$\prod_{i=0}^{2}(x - \omega^i \sqrt[3]{2})$	$(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$	ireducibilní	$(x+1)^3$	$(x+2)(x^2+3x+4)$
$x^4 - x^2 - 2$	$(x+i)(x-i)(x+\sqrt{2})(x-\sqrt{2})$	$(x^2+1)(x+\sqrt{2})(x-\sqrt{2})$	$(x^2+1)(x^2-2)$	$(x^2+1)^2$	$(x^2+3)(x+2)(x+3)$

    kde $\omega = e^{2\pi i/3}$.

12. Nalezněte všechny ireducibilní polynomy nad $\mathbb{Z}_2$ stupně nejvýše 4.

    $[x,\ x+1,\ x^2+x+1,\ x^3+x+1,\ x^3+x^2+1,\ x^4+x+1,\ x^4+x^3+1,\ x^4+x^3+x^2+x+1]$

13. Dokažte, že všechny ireducibilní polynomy v $\mathbb{R}[x]$ mají stupeň ≤ 2.

    [Stačí využít faktu, že reálné polynomy lichého stupně mají reálný kořen. Polynomy sudého stupně sice reálný kořen mít nemusí, ale pokud mají komplexní kořen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ pak mají za kořen i $\bar{\alpha}$. Součin $(x-\alpha)(x-\bar{\alpha}) \mid f$ v $\mathbb{C}[x]$ a zároveň $(x-\alpha)(x-\bar{\alpha}) \in \mathbb{R}[x]$.]

14. Rozhodněte, zda je pro každé $a \in \mathbb{Q}$ a $f(x) \in \mathbb{Q}[x]$ pravda, že pokud je $f(x)$ ireducibilní v $\mathbb{Q}[x]$, pak je $f(x+a)$ ireducibilní v $\mathbb{Q}[x]$. [Ano.]

A pro odvážné několik zábavných příkladů navíc:

15. Popište všechny ireducibilní prvky v oboru $\mathbb{Z}[i]$ (viz příklad na str. 27 ve skriptech, doplňte důkaz).

16. Najděte ireducibilní rozklad polynomu $f(x) = 2x^2+2x+3$ v oborech $\mathbb{Q}(\sqrt{-5})[x]$ a $\mathbb{Z}[\sqrt{-5}][x]$. [Běžným způsobem najdeme komplexní kořeny polynomu $x_{1,2} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{-5}$ a získáme rozklad $f(x) = 2(x - x_1)(x - x_2) \in \mathbb{Q}(\sqrt{-5})[x]$; v $\mathbb{Z}[\sqrt{-5}][x]$ je tedy nerozložitelný.]

17. Spočítejte v uvedených oborech ireducibilní rozklady polynomů $2x^2 + 2$, resp. $x^3 - 2$:

	$\mathbb{C}[x]$	$\mathbb{R}[x]$	$\mathbb{Z}[x]$	$\mathbb{Z}[i][x]$
$2x^2+2$	$(2x+2i)(x-i)$	$2x^2+2$	$2(x^2+1)$	$2(x+i)(x-i)$
x^3-2	viz př. 11	viz př. 11	ireducibilní	ireducibilní

18. Rozhodněte, zda je polynom $x^4 + x^2 + 1$ ireducibilní v oboru $\mathbb{Z}_5[x]$. [nemá kořen, tedy jediná možnost je rozklad na součin dvou kvadratických; po chvíli boje zjistíme $x^4+x^2+1 = (1+x+x^2)(1+4x+x^2)$.]

19. Najděte všechny ireducibilní polynomy stupně ≤ 3 v $\mathbb{Z}_3[x]$. [Až na přenásobení konstantou ze $\mathbb{Z}_3[x]$ to jsou: $x, x+1, x+2, x^2+1, x^2+x+2, x^2+2x+2, x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+2x^2+1, x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+x+1, x^3+2x^2+2x+2$.]

20. Najděte v $\mathbb{Z}[x]$ ireducibilní polynom, jehož kořenem je číslo $a = e^{\pi i/3}$. [$x^2 - x + 1$; víme, že platí $a^3 = -1$, tedy a je kořenem polynomu x^3+1, který má ale za kořen i číslo -1, tedy hledaným polynomem $(x^3+1) : (x+1)$.]

21. Rozhodněte, pro která $s, t \in \mathbb{Z}$ platí $\sqrt{s} \in \mathbb{Z}[\sqrt{t}]$. Uvažujte s, t taková, že nejsou dělitelná čtvercem prvočísla.

22. Dokažte tvrzení Příkladu ze str. 31 skript, které v principu říká, že

každé prvočíslo p splňující $p \equiv 3 \pmod 4$ je ireducibilním prvkem oboru $\mathbb{Z}[i]$.

(Nápověda: zkuste sporem uvažovat nějaký rozklad, pak se podívejte na normu, využijte faktu, že prvočísla jsou v $\mathbb{Z}$ prvočinitelé, a nakonec si rozmyslete něco o čtvercích mod4.)

23. Buď $\mathbf{R}$ podokruh oboru $\mathbf{S}$ a $u_1, \ldots, u_n \in S$. Dokažte, že

$$\mathbf{R}[u_1, \ldots, u_n] = \{f(u_1, \ldots, u_n) : \ f \in \mathbf{R}[x_1, \ldots, x_n]\}\,.$$

Jsou-li to tělesa, pak

$$\mathbf{R}(u_1, \ldots, u_n) = \left\{ \frac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)} : \ f, g \in \mathbf{R}[x_1, \ldots, x_n],\ g(u_1, \ldots, u_n) \neq 0 \right\}.$$

24. Dokažte, že algoritmus dělení se zbytkem, který jsme dělali pro $\mathbb{Z}[i]$, funguje také pro Eisensteinova celá čísla.

25. Dokažte, že v oborech $\mathbb{Z}[\sqrt{2}]$ a $\mathbb{Z}[\sqrt{3}]$ lze dělit se zbytkem. (*Návod: Sice schází geometrická představa, nicméně funguje podobný algoritmus dělení založený na zaokrouhlování koeficientů podílu. Důkaz odhadu normy zbytku je o něco komplikovanější.*)