3. Algebrou za meteorologické jaro

Okruhy, obory a tělesa

Definice a příklady

1. Rozhodněte, zda jsou následující struktury komutativním okruhem, oborem nebo tělesem (co je nula a jednotka těchto okruhů?):

   (a) množina $\mathbb{Z}$ se standardními operacemi $+, -$ a s operací $x \cdot y = 0$,
   [s takto definovaným násobením nemůže existovat jednotka, takže nejde o komutativní okruh]

   (b) množina $\mathbb{Z} \times \mathbb{Z}$ se standardními operacemi $+, -, \cdot$ po složkách,
   [je to komutativní okruh, ale ne obor, například $(0,1) \cdot (1,0) = (0,0)$]

   (c) sudá celá čísla se standardními operacemi. [není to okruh, protože neobsahuje jednotku]

2. Buď $\mathbf{R}$ komutativní okruh a $a \in R$ splňující $a^n = 0$. Dokažte, že je prvek $1 - a$ invertibilní v $\mathbf{R}$.
   [Inverzním prvkem je $\sum_{i=0}^{n-1} a^i$.]

3. Buď $\mathbf{R}$ komutativní okruh a $a \in R$ splňující $a^3 = 0$. Dokažte, že je prvek $1 + a$ invertibilní v $\mathbf{R}$.
   [Inverzním prvkem je $a^2 - a + 1$.]

Podokruhy

4. Rozhodněte, zda následující podmnožiny tvoří podokruh tělesa $\mathbb{C}$: $\{a+b\sqrt{2} : \ a, b \in \mathbb{Z}\}$, $\{a+b\sqrt{2}+c\sqrt{3} : a, b, c \in \mathbb{Z}\}$. [$\{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}$ ano, $\{a + b\sqrt{2} + c\sqrt{3} : \ a, b, c \in \mathbb{Z}\}$ ne.]

5. Rozhodněte, zda následující podmnožiny tvoří podtěleso tělesa $\mathbb{C}$: $\{a+b\sqrt{2} : \ a, b \in \mathbb{Q}\}$, $\{a+b\sqrt[3]{2}+c\sqrt[3]{4} : a, b \in \mathbb{Q}\}$. [$\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$ ano, $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b \in \mathbb{Q}\}$ ano]

6. Dokažte pečlivě, že prvookruh je skutečně podokruhem. Který axiom k tomu využíváte zvlášť intenzivně? [Distributivitu.]

Izomorfismus

7. Ukažte, že zobrazení z příkladu na str. 18 skript, který ukazuje, že podílové těleso oboru $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ lze ztotožnit s tělesem $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, je opravdu izomorfismus, aneb:

   (a) ukažte, že jde o homomorfismus (tj. splňuje definici ze str. 16 skript)

   (b) ukažte, že je bijektivní.

   Nápověda: Pro počítání může pomoci všimnout si, že zobrazení tak, jak je definováno, se dá zapsat i jako $f(\frac{a}{b}) = \frac{a \cdot \bar{b}}{b \cdot \bar{b}}$*; nezapomeňte ověřit, že je dobře definováno!*

Polynomy

Dělení polynomů se zbytkem

8. Dělte se zbytkem polynomy $x^4 + 3x^3 + 4x^2 + x + 3$ a $x^2 + 2$ v oborech $\mathbb{Z}[x]$ a $\mathbb{Z}_5[x]$.
[$x^2 + 3x + 2$, zbytek $-5x - 1$ v $\mathbb{Z}[x]$ a 4 v $\mathbb{Z}_5[x]$]

9. Dělte se zbytkem polynomy $x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + x$ a $x + 1$ v $\mathbb{Z}_2[x]$.
[$x^9 + x^6 + x^5 + x^2 + 1$, zbytek 1]

10. Buď $m, n \in \mathbb{N}$. Dokažte, že $x^m - 1 \mid x^n - 1$ v $\mathbb{Z}[x]$ právě tehdy, když $m \mid n$. (*Návod:* dělte se zbytkem.)

Kořeny a dělitelnost

11. Najděte polynom $f \in \mathbb{Z}[x]$ co nejmenšího stupně takový, že čísla 1 a i jsou jeho kořenem a $f(3) = f(4)$.
[$f = (-31x^2 + 175x - 144)(x^2 + 1)$]

12. Najděte polynom $f \in \mathbb{Z}_{15}[x]$ stupně 3, který má aspoň 9 různých kořenů v okruhu $\mathbb{Z}_{15}$.
[Například $x(x + 2)(x + 4)$.]

A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:

13. Buď T těleso, $f \in T[y]$ a $h \in T[x, y]$. Dokažte, že $(x - f) \mid h$ v $T[x, y]$ právě tehdy, když $h(f, y) = 0$. [Díky distributivitě násobení víme, že $(T[x])[y] = T[x, y] = (T[y])[x]$. Na h se stačí dívat jako na polynom v proměnné x nad oborem $T[y]$ a použít Tvrzení 3.3 ze skript.]

14. Rozhodněte, zda jsou následující struktury komutativním okruhem, oborem nebo tělesem (co je nula a jednotka těchto okruhů?):
   (a) množina $\mathbb{R}^3$ se standardními operacemi $+, -$ po složkách a se standardním vektorovým násobením $x \times y = ||x|| \cdot ||y|| \cdot \sin\theta \cdot n_{x,y}$, [není ani okruh, násobení není asociativní]
   (b) množina $P(X) = (\{Y : Y \subseteq X\}, \triangle, -, \cap, \emptyset, X)$ s operacemi symetrické diference $\triangle$, průniku $\cap$ a s odčítáním $-Y = Y$, [komutativní okruh s nulou $\emptyset$ a jedničkou X, není obor: $Y \cap (X \triangle Y) = \emptyset$]
   (c) $(\mathbb{Q}^+, \cdot, ^{-1}, +, 1)$, kde $\mathbb{Q}^+ = \{a \in \mathbb{Q} : a > 0\}$. [není ani okruh, $+$ není operace na $\mathbb{Q}^+$]

15. Buď n charakteristika okruhu $\mathbf{R}$. Je-li $n = 0$, jeho prvookruh je nekonečný. Je-li $n > 0$, prvookruh má n prvků. Dokažte.

16. Dokažte, že komutativita sčítání plyne z ostatních axiomů komutativních okruhů.

17. Dokažte pečlivě, že prvookruh je skutečně podokruhem. Který axiom k tomu využíváte zvlášť intenzivně? [Distributivitu.]

18. Rozhodněte, zda množiny $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}$ a $\{a + b\zeta : \ a, b \in \mathbb{Z}\}$, kde $\zeta = e^{\pi i/4}$, tvoří podokruh tělesa $\mathbb{C}$. [ne, nejsou uzavřené na násobení]

19. Buď $u \in T$ kořen polynomu $f = \sum_{i=0}^{n} f_i x^i \in T[x]$, jehož absolutní člen je nenulový. Vyjádřete u^{-1} jako lineární kombinaci mocnin prvku u (s nezáporným exponentem). [$u^{-1} = -f_0^{-1} \sum_{i=1}^{n} f_i u^{i-1}$]

20. Dokažte, že různé polynomy určují nad nekonečným tělesem různá polynomiální zobrazení. (*Návod:* uvažujte rozdíl a počet kořenů.)