Algebra — cvičení 2

Základní příklady

1. Dokažte, že podílové těleso oboru $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ lze ztotožnit s tělesem $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ (nejprve tvrzení přesně zformulujte).

2. Vydělte se zbytkem polynomy

   (a) $x^4 + 3x^3 + 4x^2 + x + 3$ a $x^2 + 2$ v $\mathbb{Z}[x]$ a v $\mathbb{Z}_5[x]$; [$x^2 + 3x + 2$, zbytek $-5x - 1 \in \mathbb{Z}[x]$, resp. zbytek $4 \in \mathbb{Z}_5[x]$]

   (b) $x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + x$ a $x + 1$ v $\mathbb{Z}_2[x]$. [$x^9 + x^6 + x^5 + x^2 + 1$, zbytek 1]

3. Nechť $\mathbf{T}$ je těleso a $f, g \in \mathbf{T}[x]$. Ukažte, že pokud $f \mid g$ a $g \mid f$ (jinými slovy f dělí g beze zbytku a g dělí f beze zbytku), pak existuje nenulové $u \in T$ takové, že $f = ug$.

   Pro hledání NSD v $\mathbf{T}[x]$, kde $\mathbf{T}$ je těleso, lze analogicky jako nad oborem celých čísel využít Eukleidův algoritmus, resp. jeho rozšířenou verzi, chceme-li se navíc dobrat i Bézoutových koeficientů. K tomu je potřeba si ujasnit jen pár drobností. Předně, že algoritmus skončí, jelikož při dělení polynomů se zbytkem je stupeň zbytku vždy ostře menší než stupeň dělitele. Dále, že NSD je ze všech společných dělitelů ten největší vzhledem k relaci $|$, a tudíž je určen až na násobek nenulovým prvkem $u \in T$, jak plyne ze cvičení výše. Nakonec: Bézoutovy koeficienty budou obecně prvky z $\mathbf{T}[x]$, nikoliv pouze z $\mathbf{T}$.

4. Spočtěte $\mathrm{NSD}(f, g)$ a příslušné Bézoutovy koeficienty pro polynomy

   (a) $f = x^3 + x^2 + x + 1$ a $g = x^2 + 2x + 2$ v oboru $\mathbb{Z}_3[x]$ a v oboru $\mathbb{Z}_5[x]$; [$2 = (2x+1)f + (x^2 + x + 2)g$ v $\mathbb{Z}_3[x]$ a $x + 3 = f + (4x + 1)g$ v $\mathbb{Z}_5[x]$]

   (b) $f = x^3 - x^2 - x - 2$ a $g = x^3 - 2x^2 + 3x - 6$ v oboru $\mathbb{Q}[x]$. [$7x - 14 = (-x - 2)f + (x + 3)g$]

Další počítání

5. Najděte všechny kořeny polynomu $f = x^2 + x \in \mathbb{Z}_6[x]$ v okruhu $\mathbb{Z}_6$ a napište všechny rozklady (až na pořadí) tohoto f na součin kořenových činitelů, tj. na součin tvaru $(x - a)(x - b)$, kde a, b jsou kořeny. [$0, 2, 3, 5$, $x^2 + x = x(x - 5) = (x - 3)(x - 2)$]

6. V okruhu $\mathbb{Z}_{10}[x]$ nalezněte polynom stupně 2 mající maximální možný počet (po dvou různých) kořenů. [např. $5x^2 + 5x = 5x(x + 1)$ má 10 kořenů]

7. Ukažte, že žádný okruh nemůže být sjednocením dvou svých vlastních podokruhů.

8. Nechť $\mathbf{R}$ je komutativní okruh s jednotkou. Pro libovolné $a \in R$ uvažujme zobrazení $f_a : R \to R$ definované vztahem $f_a(r) = ar$.

   (a) Pro jaká $a \in R$ je f_a endomorfismem okruhu R, tj. homomorfismem z R do R? [jen pro $a = 1$]

   (b) Co to pro prvek $a \in R$ znamená, když je zobrazení f_a prosté, resp. na? [a lze krátit, resp. lze jím v R (byť třeba nejednoznačně) vydělit]

9. Najděte příklad nekonečného tělesa kladné charakteristiky. [např. podílové těleso $\mathbb{Z}_p(x)$ oboru $\mathbb{Z}_p[x]$, kde p je prvočíslo]

A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:

10.⋆ Najděte všechna $x, y, z, w \in \mathbb{Z}$ splňující $x^2+y^2+z^2 = 15w^2$ (návod: řešte nejprve kongruenci modulo 8). [pouze triviální nulové řešení]

11.⋆ Řekneme, že (ne nutně komutativní) okruh $\mathbf{R}$ je *booleovský*, pokud $(\forall r \in R)\, r^2 = r$. Dokažte, že booleovské okruhy jsou komutativní.

12.⋆ Ať $\mathbf{R}$ je (komutativní) obor prvočíselné charakteristiky p a $n \in \mathbb{N}_0$. Ukažte, že potom pro každé $a, b \in \mathbf{R}$ platí $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. Jako důsledek odvoďte, že „mocnění na p“ je prostý endomorfismus oboru $\mathbf{R}$ (říká se mu *Frobeniův*).

13.⋆ Ukažte, že nenulový polynom nad (komutativním) oborem má nejvýše tolik kořenů, kolik je jeho stupeň.

14.⋆ Je-li $\mathbb{Q}[\pi]$ nejmenší podokruh tělesa $\mathbb{R}$ obsahující $\mathbb{Q} \cup \{\pi\}$, dokažte, že jsou okruhy $\mathbb{Q}[x]$ a $\mathbb{Q}[\pi]$ izomorfní. (Využít můžete faktu, že π není kořenem žádného nenulového polynomu s racionálními koeficienty.)