Algebrou proti koronaviru I

(cvičení cihlovou barvou jsme udělali na cvičení, a tak je můžete vynechat)

Okruhy & obory II

1. Dokažte (například sporem jako na cviku), že okruhy $\mathbb{Q}[\sqrt{3}]$ a $\mathbb{Q}[\sqrt{2}]$ jsou neizomorfní. [Kdyby měl existovat izomorfismus $\varphi : \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{2}]$, pak by muselo platit $\varphi(3) = \varphi(\sqrt{3}\sqrt{3}) = \varphi(\sqrt{3}) \cdot \varphi(\sqrt{3})$, tj. prvek $\varphi(\sqrt{3}) \in \mathbb{Q}[\sqrt{2}]$ by fungoval jako odmocnina ze tří.]

2. 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 racionálního polynomu). [Zobrazení $\varphi : p(x) \mapsto p(\pi)$ je homomorfismus oborů a fakt, že π není kořenem žádného nenulového racionálního polynomu, je třeba k důkazu prostoty.]

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

   (b) Pro jaká $a \in R$ je f_a homomorfismus (z R do R)? [jen pro $a = 0, 1$, v ostatních případech selže podmínka $f_a(b \cdot c) = f_a(b) \cdot f_a(c)$]

Podílové těleso

4. Ukažte, že zobrazení z příkladu na str. 8, 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. 6)

   (b) ukažte, že je bijektivní (nebo najděte inverzní homomorfismus).

   [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!]

Okruhy polynomů & dělení polynomů se zbytkem

5. Vydělte se zbytkem polynomy

   (a) $x^4 + 3x^3 + 4x^2 + x + 3$ a $x^2 + 2$ v $\mathbb{Z}_5[x]$; [$x^2 + 3x + 2$, 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]

6. 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 $u \in T$ (tedy „číslo“) takové, že $f = ug$. [Protože $f \mid g$ je ekvivalentní rovnosti $f = p(x) \cdot g$ pro nějaké $p(x) \in \mathbf{T}[x]$ a podobně i pro druhý vztah máme $g = q(x) \cdot p$, dostáváme $f = p(x)q(x)f$ a porovnáním stupňů na obou stranách rovnosti zjistíme, že polynom $p(x)q(x)$ musí mít stupeň 0, tj. jde o prvek (prvky) $\mathbf{T}$.]

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 $\mid$, 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 $\mathbf{T}$.

7. Spočtěte NSD(f, g) a příslušné Bézoutovy koeficienty pro polynomy

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

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

Věta 2.4 ze skript říká něco pro polynomy nad oborem, inspirací pro následující dvě otázky by ale mohla dát Poznámka za ní.

8. 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. $[0, 2, 3, 5,\ x^2 + x = x(x - 5) = (x - 3)(x - 2)]$

9. 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]

A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:

10.* (Ještě k minulému cviku, komu nestačilo:) Najděte všechna $x, y, z, w \in \mathbb{Z}$ splňující $x^2+y^2+z^2 = 15w^2$ (Nápověda: 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. [Spočítáme, že $(a+b)^2 = ab+ba$, a z rozepsání $(r+r)^2$ zjistíme, že $2r = 0$, tj. $r = -r$ pro každé $r \in R$.]

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

13.* Vydělte se zbytkem polynomy $x^4+3x^3+4x^2+x+3$ a x^2+2 v $\mathbb{Z}[x]$ (pozor, $\mathbb{Z}$ není těleso!) [x^2+3x+2, zbytek $-5x-1 \in \mathbb{Z}[x]$]

14.* Spočtěte NSD(f, g) a příslušné Bézoutovy koeficienty pro polynomy $f = x^3+x^2+x+1$ a $g = x^2+2x+2$ v oboru $\mathbb{Z}_5[x]$; [$x+3 = f+(4x+1)g$ v $\mathbb{Z}_5[x]$]