Druhá vnitrosemestrální písemná práce MB204 3.5.2013

1. Dokažte, že zobrazení $[a]_6 \mapsto [3]_7^a$ je izomorfismus grup $(\mathbb{Z}_6, +)$ a $(\mathbb{Z}_7^*, \cdot)$ a že zobrazení $[a]_6 \mapsto ([a]_2, [a]_3)$ je izomorfismus okruhů $(\mathbb{Z}_6, +, \cdot)$ a $(\mathbb{Z}_2, +, \cdot) \times (\mathbb{Z}_3, +, \cdot)$.

Řešení. Označme první zobrazení jako $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_7^*$. Klíčem k úspěchu je si všimnout, že $[3]_7$ je generátor grupy $\mathbb{Z}_7^*$. Nejdříve musíme ověřit, zda vůbec je φ zobrazení (nezáleží na volbě reprezentanta a). Grupa $\mathbb{Z}_7^*$ má šest prvků, tedy z *Legendreovy věty* je $[3]_7^6 = [1]_7$. Tedy pokud platí $[a]_6 = [b]_6$, pak také $[3]_7^a = [3]_7^{b+6k} = [3]_7^b \cdot [3]_7^{6k} = [3]_7^b \cdot [1]_7 = [3]_7^b$. Vskutku je φ zobrazení; je také homomorfismus grup, o čemž se přesvědčíme výpočtem:

$$\varphi([x]_6 + [y]_6) = \varphi([x+y]_6) = [3]_7^{x+y} = [3]_7^x \cdot [3]_7^y$$

Protože je $[3]_7$ generátor (*primitivní kořen*), je zobrazení φ na $\mathbb{Z}_7^*$ (surjektivní). Obě grupy mají 6 prvků, tedy zobrazení musí být nutně bijektivní. Máme izomorfismus.

Druhé zobrazení si označme $\theta : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$. Postupujme stejně jako výše. Korektnost: Je jasné, že pokud $[a]_6 = [a+6k]_6$, pak také $\theta([a+6k]_6) = ([a]_2, [a]_3)$, poněvadž dvojka i trojka dělí šestku. Že je θ homomorfismus se ověří jednoduše, pouze se použije definice součinu okruhů (tj. sčítá a násobí se po složkách a jedničkou je prvek, který má na všech pozicích příslušnou okruhovou jedničku). Jako výše, oba okruhy mají stejný počet prvků; bude tedy pro bijektivnost θ stačit ověřit, že je prosté (či na). Koukněme se na $\ker\theta$. Je-li v jádru $[x]_6$ musí být $2, 3 \mid x$, což (mod 6) splňuje pouze $x = 0$. θ je injektivní, proto izomorfismus. □

2. Určete řády prvků $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ a $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ v grupě invertibilních matic $GL(\mathbb{Z}_3)$. Určete inverze těchto prvků a spočítejte $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{2013}$ a $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{2014}$.

Řešení. V tomto příkladu si procvičíme násobení matic. Označme si $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ a $B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ matice nad tělesem $\mathbb{Z}_3$. Zdálo by se, že bychom měli ještě předem ověřit, zda jsou matice vůbec prvky dané grupy - jsou-li vůbec invertibilní. Toto nám ale vyskočí jako vedlejší produkt, když nalezneme konečný řád matice: obecně v monoidu platí, že pokud $x^n = e$, pak $x^{n-1} = x^{-1}$, kde e je neutrální prvek. Tedy prvky konečného řádu jsou invertibilní. Spočítejme řády A a B:

$$A \cdot A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ A^2 \cdot A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$B^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2E \Rightarrow B^4 = E,\ B^2 \cdot B = 2E \cdot \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

Řád A je 3 a $A^{-1} = A^2$; řád B je 4 a $B^{-1} = B^3 = 2 \cdot B$. Zbytek příkladu napočítejme s využitím toho, že již známe řády:

$$A^{2013} = A^{1+3\cdot 671} = A \cdot E^{671} = A,\ B^{2014} = B^{2+4\cdot 503} = B^2 \cdot E^{503} = 2E$$

□

3. Mějme permutaci $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 4 & 2 & 1 & 6 \end{pmatrix}$. Určete řád σ v grupě $(S_7, \circ)$, inverzi k σ a σ^{2013}. Ukažte, že σ nekomutuje s transpozicí $\tau = (2, 3)$.

Řešení. Toto je jednoduché. Zprvu si σ napišme jako součin nezávislých cyklů, bude to výhodné pro naše manipulace: $\sigma = (1, 3, 7, 6)(2, 5)(4)$. Řád součinu nezávislých cyklů je nejmenší společný násobek řádů oněch nezávislých činitelů. Zároveň řád cyklu je roven jeho délce. Proto dohromady máme, že řád σ je roven 4, tj. $\sigma^4 = \mathrm{id}$. Lehce nyní spočítáme $\sigma^{2013} = \sigma^{1+4\cdot 503} = \sigma$. Inverze je také velmi jednoduchá,

poněvadž stačí pouze *převrátit pořadí* v nezávislých cyklech: $\sigma^{-1} = (1,6,7,3)(2,5)(4)$. Kdyby σ a τ komutovaly, muselo by platit $\tau\sigma\tau = \sigma\tau^2 = \sigma$, ale to neplatí. Stačí zkusit aplikovat součin na prvek 2:

$$(\tau\sigma\tau)(2) = \tau(\sigma(\tau(2))) = \tau(\sigma(3)) = \tau(7) = 7 \neq 5 = \sigma(2)$$

□

4. Rozložte $p(x) = 2x^5 + 3x^4 - x^3 - 5x^2 - 6x - 2$ a $q(x) = x^4 + x^3 - 2x - 4$ na ireducibilní polynomy v $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Z}[x], \mathbb{Z}_5[x], \mathbb{Z}_7[x]$, když víte, že mají společný kořen a p má navíc racionální kořen.

Řešení. Nejprve najděme onen racionální kořen p. Podle známého tvrzení může být nenulové číslo $\frac{a}{b}$, $(a,b) = 1$ kořenem p, jen když a, b dělí číslo 2. Máme možnosti $\frac{a}{b} \in \{\pm\frac{1}{2}, \pm 1, \pm 2\}$. Tyto možnosti postupně ověříme, například použitím *Hornerova schématu* - které je výhodné, poněvadž zároveň dostaneme i podíl p podle příslušného kořenového činitele. Vychází, že kořen je $-\frac{1}{2}$, dokonce $p = (2x+1)(x^4 + x^3 - x^2 - 2x - 2) = (2x+1)p'$. Všimněme si, že $-\frac{1}{2}$ není kořen q, tedy společný kořen je kořenem p'. Tento společný kořen také nuluje největší společný dělitel $(p', q) = g$. (Protože $g = Ap' + Bq$). Euklidovým algoritmem a trpělivostí zjistíme, že $g = x^2 - 2$.

$$p' : g = x^2 + x + 1 = m, \quad q : g = x^2 + x + 2 = n$$

Tyto podíly mají záporné diskriminanty, proto jsou ireducibilní v $\mathbb{R}[x]$ a $\mathbb{Z}[x]$.

Ještě se zabývejme situací nad konečnými tělesy. Zprvu si povšimněme, že jsme v úpravách nepoužili nic, co by bylo nelegální modulo 5 či 7. V aritmetice $\mod 5$ není 2 kvadratický zbytek, zatímco $\mod 7$ ano: $3^2 \equiv (-3)^2 \equiv 2 \pmod 7$. Tedy celkově $g = x^2 - 2$ v $\mathbb{Z}_5[x]$ je ireducibilní a $g = (x-3)(x+3)$ v $\mathbb{Z}_7[x]$ Co ale ireducibilita m a n? Stačí se podívat, zda v příslušných tělesech jsou jejich diskriminanty kvadratické zbytky.

$$\left(\frac{1^2 - 4 \cdot 1}{5}\right) = \left(\frac{2}{5}\right) = -1 \text{ a } \left(\frac{1^2 - 4 \cdot 1}{7}\right) = \left(\frac{4}{7}\right) = 1$$
$$\left(\frac{1^2 - 4 \cdot 2}{5}\right) = \left(\frac{3}{5}\right) = -1 \text{ a } \left(\frac{1^2 - 4 \cdot 2}{7}\right) = \left(\frac{7}{7}\right) = 0$$

Polynomy m i n jsou ireducibilní v $\mathbb{Z}_5[x]$. Platí $2^2 \equiv 4 \mod 7$, podle středoškolských vzorečků na kořeny kvadratické rovnice použitých v $\mathbb{Z}_7[x]$ máme $m = (x-4)(x-2)$ a $n = (x-3)^2$ Naše zjištění si můžeme zapsat do přehledné tabulky:

$$\begin{aligned}
\text{v } \mathbb{C}[x] : p &= (x - \sqrt{2})(x + \sqrt{2})(2x + 1)(x + \frac{1 - \iota\sqrt{3}}{2})(x + \frac{1 + \iota\sqrt{3}}{2}) \\
q &= (x - \sqrt{2})(x + \sqrt{2})(x + \frac{1 - \iota\sqrt{7}}{2})(x + \frac{1 + \iota\sqrt{7}}{2}) \\
\text{v } \mathbb{R}[x] : p &= (x - \sqrt{2})(x + \sqrt{2})(2x + 1)(x^2 + x + 1) \\
q &= (x - \sqrt{2})(x + \sqrt{2})(x^2 + x + 2) \\
\text{v } \mathbb{Z}[x] : p &= (2x + 1)(x^2 - 2)(x^2 + x + 1) \\
q &= (x^2 - 2)(x^2 + x + 2) \\
\text{v } \mathbb{Z}_5[x] : p &= (2x + 1)(x^2 - 2)(x^2 + x + 1) \\
q &= (x^2 - 2)(x^2 + x + 2) \\
\text{v } \mathbb{Z}_7[x] : p &= (2x + 1)(x + 3)^2(x - 3)(x - 2) \\
q &= (x + 3)(x - 3)^3
\end{aligned}$$

□

5. Uvažme polynomy $f = x^3 + z^2 - xy, g = y^2 + z^2 - 1$ a $h = x^3y - y^3 - xy^2 - zy^2 + y + z - 1$ v $\mathbb{R}[x, y, z]$. Seřaďte monomy v polynomech podle lexikografického uspořádání s $x > y > z$ a vydělte polynom h polynomy f a g. Výsledek použijte na určení algebraické variety v $\mathbb{R}^3$ dané ideálem generovaným polynomy f, g, h, tj. na vyřešení soustavy rovnic $f = g = h = 0$.

Řešení. Použijme algoritmus na dělení polynomů. Pro ověření zde uvedeme i některé mezivýsledky:

$$\begin{aligned} x^3y - xy^2 - y^3 - y^2z + y + z - 1 &= f \cdot y - (y^3 + y^2z + yz^2 - y - z + 1) = \\ &= f \cdot y - (g \cdot y + y^2z - z + 1) = \\ &= f \cdot y - g \cdot (y + z) + z^3 - 1 \end{aligned}$$

Prvky variety určené polynomy f, g, h jsou právě jejich společné nulové body. Náš výpočet ukazuje, že musí platit $z^3 = 1$, což v $\mathbb{R}$ platí pouze pro $z = 1$. Tedy již víme, že ve varietě musí být pouze body tvaru $[x, y, 1]$. Dosaďme, $0 = g[x, y, 1] = y^2 + 1^2 - 1 = y^2$; máme $y = 0$. Dále $0 = f[x, 0, 1] = x^3 + 1 \Rightarrow x = -1$. Tedy celkově jsme získali, že určená varieta je jednoprvková; obsahuje pouze bod $[-1, 0, 1]$. □