1. Druhá vnitrosemestrální práce 16.5.2014

1.1. (2b.) Určete řády všech prvků v grupách $\mathbb{Z}_8$, $\mathbb{Z}_{12}$, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$ a $\mathbb{Z}_{14}^\times$ a určete generátory těchto grup. Dokažte, že $\mathbb{Z}_8^\times \cong \mathbb{Z}_{12}^\times$.

Řešení.

$\mathbb{Z}_8$	1	2	3	4	5	6	7
řád	8	4	8	2	8	4	8

$\mathbb{Z}_{12}$	1	2	3	4	5	6	7	8	9	10	11
řád	12	6	4	3	12	2	12	3	4	6	12

Generátory jsou prvky s maximálním řádem, tj. nesoudělné s 8 resp. 12 (a je jich v obou případech $\varphi(8) = \varphi(12) = 4$).

$\mathbb{Z}_8^\times$	1	3	-3	-1
řád	1	2	2	2

$\cong$

$\mathbb{Z}_{12}^\times$	1	5	-5	-1
řád	1	2	2	2

$\mathbb{Z}_{14}^\times$	1	3	5	-5	-3	-1
řád	1	6	6	3	3	2

$\mathbb{Z}_8^\times$ a $\mathbb{Z}_{12}^\times$ nemají generátor, pro $\mathbb{Z}_{14}^\times$ je generátor 3 a 5 (jsou to vlastně primitivní kořeny modulo 14, je jich $\varphi(\varphi(14)) = \varphi(6) = 2$). Izomorfismus $\mathbb{Z}_8^\times \cong \mathbb{Z}_{12}^\times$ je dán přiřazením $\pm 1 \mapsto \pm 1$ a $\pm 3 \mapsto \pm 5$. Obě grupy jsou komutativní a mají neutrální prvek a tři prvky řádu 2, jsou tedy obě izomorfní $\mathbb{Z}_2 \times \mathbb{Z}_2$.

1.2. (2b.) Dokažte, že předpis φ zadává zobrazení, které je homomorfismem grup. Určete jeho jádro a obraz, rozhodněte o surjektivitě a injektivitě φ a popište faktorgrupu $\mathbb{A}_4/\operatorname{im}(\varphi)$.

$$\varphi : \mathbb{Z}_3 \to \mathbb{A}_4, \varphi([a]_3) = (1,2,4) \circ (1,3,2)^a \circ (1,4,2)$$

Řešení. Předpis zadává zobrazení, protože z $a \equiv b \pmod 3$ plyne $(1,3,2)^a = (1,3,2)^b$, a proto i $\varphi([a]_3) = \varphi([b]_3)$. Jedná se o homomorfismus, protože

$$(1,2,4)\circ(1,3,2)^{a+b}\circ(1,4,2) = (1,2,4)\circ(1,3,2)^a\circ(1,4,2)\circ(1,2,4)\circ(1,3,2)^b\circ(1,4,2)$$

a

$$(1,2,4) \circ (1,3,2)^0 \circ (1,4,2) = \mathrm{id}\,.$$

Jádro je nulové, jedna se tedy o injektivní homomorfismus. Surjektivní není, protože obrazem je identita a permutace

$$(1,2,4) \circ (1,3,2)^1 \circ (1,4,2) = (2,3,4),$$

$$(1,2,4) \circ (1,3,2)^2 \circ (1,4,2) = (2,4,3),$$

tj. $\operatorname{im}(\varphi) = (2,3,4)^k, k = 0,1,2$. Je to normální podgrupa v grupě sudých permutací $\mathbb{A}_4$. Ta je tvořena permutacemi, které jsou tvořeny právě jedním cyklem délky 3 nebo dvěmi nezávislými transpozicemi. Její řád je $|\mathbb{A}_4| = \frac{1}{2}4! = 12$. Faktorgrupa $\mathbb{A}_4/\operatorname{im}(\varphi)$ má řád $|\mathbb{A}_4/\operatorname{im}(\varphi)| = \frac{12}{4} = 4$. Prvky faktorgrupy jsou reprezentovány právě třemi permutacemi danými součinem dvou transpozic a identitou, tj. jsou to třídy $\{\mathrm{id}, (2,3,4), (2,4,3)\}$, $\{(1,2)\circ(3,4), (1,2,4), (1,2,3)\}$, $\{(1,3)\circ(2,4), (1,3,2), (1,3,4)\}$, $\{(1,4)\circ(2,3), (1,4,3), (1,4,2)\}$.

1.3. (2b.) Určete počet obarvení vrcholů rovnostranného trojúhelníka třemi barvami, považujeme-li za stejná obarvení, která na sebe přejdou při nějaké symetrii trojúhelníka.

Řešení. Grupa symetrií trojúhelníka je D_6, složená z identity, tří osových symetrií o a dvou rotací r (o $\pm\frac{2}{3}\pi$). Množina pevných bodú identity je celá množina všech různých obarvení, tj. $|S_{\mathrm{id}}| = |S| = 3^3 = 27$. Počet prvků množiny pevných bodú pro osové symetrie je $|S_o| = 3^2 = 9$ a pro rotace $|S_o| = 3$. Počet orbit akce grupy symetrií na S, tj. náš hledaný počet odlišných obarvení, je pak

$$N = \frac{27 + 3 \cdot 9 + 2 \cdot 3}{1 + 3 + 2} = \frac{60}{6} = 10.$$

1.4. (2b.) Rozložte polynom $x^4 - x^2 - 2$ na součin ireducibilních prvků v oborech $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_5[x]$, $\mathbb{Z}_3[x]$.

Řešení. Evidentně $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$. Rozklad nad $\mathbb{C}$ je $(x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i)$, nad $\mathbb{R}$ je $(x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)$, nad $\mathbb{Q}$ je $(x^2 - 2)(x^2 + 1)$. V $\mathbb{Z}_5$ ani $\mathbb{Z}_3$ polynom $x^2 - 2$ nemá kořen a je tedy ireducibilní. Stejně tak je $x^2 + 1$ ireducibilní v $\mathbb{Z}_3$. V $\mathbb{Z}_5$ je ovšem $x^2 + 1 = (x - 2)(x + 2)$.

1.5. (2b.) Mějme lineární $(8, 3)$ kód generovaný polynomem $x^5 + x^4 + x^2 + 1$. Určete generující matici a matici parity. Dále zakódujte zprávu 111 a naopak určete odeslanou zprávu, jestliže jste obdrželi kódové slovo 01010010 a předpokládáte, že došlo k nejmenšímu možnému počtu chyb.

Řešení. Spočítáme

$$\begin{aligned} 1 &\mapsto x^5 \equiv x^4 + x^2 + 1 \\ x &\mapsto x^6 \equiv x^5 + x^3 + x \equiv x^4 + x^3 + x^2 + x + 1 \\ x^2 &\mapsto x^7 \equiv x^4 + x^3 + x \end{aligned}$$

Odtud máme generující matici a matici parity

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Zakódovanou zprávu dostaneme vynásobením zaprávy maticí G, tj. $111 \mapsto 10000111$. Obdržená zpráva odpovídá polynomu $01010010 \leftrightarrow x + x^3 + x^6$. Tento polynom vydělíme se zbytkem generujícím polynomem:

$$x^6 + x^3 + x : x^5 + x^4 + x^2 + 1 = x, rem = x^5$$

Nejbližší kódové slovo tedy dostaneme změnou bitu na šesté pozici, tj. odesílaná zpráva byla 110.

1.6. (1b.) Vyřešte soustavu následujících polynommiálních rovnic. Tvoří tyto polynomy Gröbnerovu bázi ideálu, který generují?

$$\begin{aligned} x^3 - 2xy &= 0 \\ x^2y + x - 2y^2 &= 0 \end{aligned}$$

Řešení. Vedoucí člen prvního a druhého polynomu vzhledem k lexikografickému uspořádání s $x > y$ je x^3 respektive x^2y. Vytvořením S–polynomu získáme

$$y(x^3 - 2xy) - x(x^2y + x - 2y^2) = -x^2.$$

Ze soustavy pak plyne, že levá strana je nulová, a proto i $x = 0$ a tedy i $y = 0$. Vyhovuje jí tedy jediný bod $(0, 0)$. Báze není Gröbnerova, protože $x^2 \notin \langle x^3, x^2y \rangle$.