MB104 – 3. demonstrovaná cvičení
Okruhy a tělesa

Masarykova univerzita
Fakulta informatiky

12.3. 2007

Příklad 1. *Určete všechny podgrupy grupy invertibilních čtvercových matic nad $\mathbb{Z}_2$ (vzhledem k násobení matic), viz Sada 1. Je tato grupa isomorfní grupě S_3? Zdůvodněte (buď najděte isomorfismus, nebo udejte důvod, proč neexistuje).*

Příklad 1. *Určete všechny podgrupy grupy invertibilních čtvercových matic nad $\mathbb{Z}_2$ (vzhledem k násobení matic), viz Sada 1. Je tato grupa isomorfní grupě S_3? Zdůvodněte (buď najděte isomorfismus, nebo udejte důvod, proč neexistuje).*

Řešení. Grupy jsou isomorfní, transposice odpovídají prvkům řádu 2. Podgrupy pak odpovídají podgrupám S_3 □

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*
7. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*
7. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$
8. *není zobrazení*

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*
7. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$
8. *není zobrazení*
9. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [4a]_{\mathbb{Z}_{15}^*}$

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*
7. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$
8. *není zobrazení*
9. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [4a]_{\mathbb{Z}_{15}^*}$
10. *je bijekce, není isomorfismus*

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*
7. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$
8. *není zobrazení*
9. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [4a]_{\mathbb{Z}_{15}^*}$
10. *je bijekce, není isomorfismus*
11. $f : (\mathbb{Z}_k^*, \cdot) \to (\mathbb{Z}_k^*, \cdot)$, $f([a]_{\mathbb{Z}_k^*}) = [l \cdot a]_{\mathbb{Z}_k^*}$, $k, l \in \mathbb{N}, k, l > 1$

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*
7. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$
8. *není zobrazení*
9. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [4a]_{\mathbb{Z}_{15}^*}$
10. *je bijekce, není isomorfismus*
11. $f : (\mathbb{Z}_k^*, \cdot) \to (\mathbb{Z}_k^*, \cdot)$, $f([a]_{\mathbb{Z}_k^*}) = [l \cdot a]_{\mathbb{Z}_k^*}$, $k, l \in \mathbb{N}, k, l > 1$
12. *je bijekce pro* $(k, l) = 1$ *(pro* $l \equiv 1 \mod k$*), jinak není zobrazení*

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*
7. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$
8. *není zobrazení*
9. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [4a]_{\mathbb{Z}_{15}^*}$
10. *je bijekce, není isomorfismus*
11. $f : (\mathbb{Z}_k^*, \cdot) \to (\mathbb{Z}_k^*, \cdot)$, $f([a]_{\mathbb{Z}_k^*}) = [l \cdot a]_{\mathbb{Z}_k^*}$, $k, l \in \mathbb{N}, k, l > 1$
12. *je bijekce pro* $(k, l) = 1$ *(pro* $l \equiv 1 \mod k$*), jinak není zobrazení*
13. $f : S_k \to S_k$, $f(\sigma) = \sigma^2$

Příklad 2. *Rozhodněte (se zdůvodněním) o následujících předpisech, zda jsou zobrazeními, případně homomorfismy či isomorfismy grup:*

1. $f : (\mathbb{Z}_7, +) \to (\mathbb{Z}_8, +)$, $f([a]_{\mathbb{Z}_7}) = [a]_{\mathbb{Z}_8}$
2. *není zobrazení*
3. $f : (\mathbb{Z}_7^*, \cdot) \to (\mathbb{Z}_{14}^*, \cdot)$, $f([a]_{\mathbb{Z}_7^*}) = [a]_{\mathbb{Z}_{14}^*}$
4. *není zobrazení*
5. $f : (\mathbb{Z}_{14}^*, \cdot) \to (\mathbb{Z}_7^*, \cdot)$, $f([a]_{\mathbb{Z}_{14}^*}) = [a]_{\mathbb{Z}_7^*}$
6. *je isomorfismus*
7. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [3a]_{\mathbb{Z}_{15}^*}$
8. *není zobrazení*
9. $f : (\mathbb{Z}_{15}^*, \cdot) \to (\mathbb{Z}_{15}^*, \cdot)$, $f([a]_{\mathbb{Z}_{15}^*}) = [4a]_{\mathbb{Z}_{15}^*}$
10. *je bijekce, není isomorfismus*
11. $f : (\mathbb{Z}_k^*, \cdot) \to (\mathbb{Z}_k^*, \cdot)$, $f([a]_{\mathbb{Z}_k^*}) = [l \cdot a]_{\mathbb{Z}_k^*}$, $k, l \in \mathbb{N}, k, l > 1$
12. *je bijekce pro* $(k, l) = 1$ *(pro* $l \equiv 1 \mod k$*), jinak není zobrazení*
13. $f : S_k \to S_k$, $f(\sigma) = \sigma^2$
14. *je zobrazení, je homomorfismem pouze pro* $k = 2$

Příklad 3. *Ukažte, že pro libovolný cyklus σ v S_n je $\tau\sigma\tau^{-1}$ opět cyklus (pro libovolné $\tau \in S_n$). Rozhodněte, zda jsou podgrupy generované*

- *cyklem $(1, 2, 3)$ v S_3,*
- *cyklem $(1, 2, 3, 4)$ v S_4*
- *cyklem $(1, 2, 3)$ v A_4*

normální. V posledním případě určete pravé třídy rozkladu A_4 podle uvažované podgrupy. Určete, kdy je podmnožina všech cyklů délky n podgrupou grupy S_n. Ukažte, že se pak jedná o normální podgrupu.

Řešení.

- Jde o normální podgrupu A_3.
- Není to normální podgrupa ($(1,2)(1,3)(2,4)(1,2) = (4,1)(2,3)$).
- Podgrupa není normální. Pravé třídy rozkladu jsou pak $\{(124),(243),(13)(24)\}$, $\{(142),(143),(14)(23)\}$, $\{(234),(12)(34),(134)\}$, $\{\mathrm{Id},(123),(132)\}$.

Podmnožina je podgrupou pouze pro $n = 3$. Potom jde o podgrupu sudých permutací v S_3. (pro jiná n snadno najdeme dva cykly délky n jejichž složením není cyklus délky n). □

Eulerova funkce $\varphi : \mathbb{N} \to \mathbb{N}$

Udává počet čísel nepřevyšujících n s číslem n nesoudělných. Je-li $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ rozklad přirozeného čísla n na prvočísla, pak

$$\phi(n) = \prod_{i=1}^{s} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$$

Eulerova funkce $\varphi : \mathbb{N} \to \mathbb{N}$

Udává počet čísel nepřevyšujících n s číslem n nesoudělných. Je-li $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ rozklad přirozeného čísla n na prvočísla, pak

$$\phi(n) = \prod_{i=1}^{s} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$$

Eulerova věta. Pro nesoudělná (a, m) platí

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Nalezněte největšího společného dělitele polynomů
$x^9 + x^8 + x^7 + x^6 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ a
$x^3 + 2x^2 + 2x + 2$ nad $\mathbb{Z}_1 1$

V oboru komplexních čísel nalezněte kořeny polynomu

1. $x^3 + 2x^2 - 4x - 8$,

V oboru komplexních čísel nalezněte kořeny polynomu

1. $x^3 + 2x^2 - 4x - 8$,
2. $4x^4 + 3x^3 + 5x^2 + 2x + 1$.

Eisensteinovo kriterium ireducibility.

Udává, kdy je polynom nad okruhem $\mathbb{Z}$ nerozložitelný nad $\mathbb{Q}$ (což je stejné, jako nerozložitelnost nad $\mathbb{Z}$):
Buď

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

polynom nad $\mathbb{Z}$ a dále nechť existuje prvočíslo p tak, že

- p dělí a_j, $j = 0 \ldots n-1$,
- p nedělí a_n,
- p^2 nedělí a_0,

pak je $f(x)$ nerozložitelný nad $\mathbb{Z}$ ($\mathbb{Q}$)

Rozložte polynom

$$x^4 + 2x^2 + 2$$

na ireducibilní faktory nad

- $\mathbb{Q}$

Rozložte polynom

$$x^4 + 2x^2 + 2$$

na ireducibilní faktory nad

- $\mathbb{Q}$
- $\mathbb{R}$

Rozložte polynom

$$x^4 + 2x^2 + 2$$

na ireducibilní faktory nad

- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$

Rozložte polynom

$$x^4 + 2x^2 + 2$$

na ireducibilní faktory nad

- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{Z}_5$

Rozložte polynom

$$x^4 + 2x^2 + 2$$

na ireducibilní faktory nad

- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{Z}_5$
- $\mathbb{Z}_3$.

Nalezněte všechny ireducibilní mnohočleny stupně menšího než pět nad $\mathbb{Z}_2$.