Zápočtová písemka z Algebry I

19. 12. 2002 — oprava — výsledky

1. (6 bodů) Jsou dány permutace $f, g \in \mathbb{S}_{10}$. Platí

$$f = (1,3,7) \circ (2,6,9), \quad g = (1,3) \circ (2,8,5,6) \circ (1,7,3,2).$$

Zapište permutace f^{-1}, g^{16}, $h = (f^8 \circ g^{-4})^{20}$ ve tvaru součinu nezávislých cyklů.

U každé z permutací f, g, h, určete její paritu a řád.

Napište permutaci f a g jako součin osmi transpozic. Pokud to nelze, zdůvodněte proč.

— $f^{-1} = (1,7,3) \circ (2,9,6)$, $g^{16} = (2,3,8,5,6)$, $h = (1,3,5) \circ (2,7,8)$. *Permutace f a h jsou sudé permutace řádu 3, g je lichá permutace řádu* 10.

Součin osmi transpozic je sudá permutace, proto g v tomto tvaru psát nelze;
$f = (1,7) \circ (1,3) \circ (2,9) \circ (2,6) \circ (1,2)^4$.

2. (1 bod) V grupě $(\mathbb{Z}_{17}^*, \cdot)$ určete řád prvku $[3]_{17}$.

— *Řád prvku* $[3]_{17}$ *je* 16.

3. (1 bod) Určete která z grup $(\mathbb{Z}_{75}^*, \cdot)$ a $(\mathbb{Z}_{88}^*, \cdot)$ má více prvků.

— $|\mathbb{Z}_{75}^*| = \varphi(75) = 40 = \varphi(88) = |\mathbb{Z}_{88}^*|$.

4. (2 body) V grupě $(\mathbb{Z}_{427}^*, \cdot)$ nalezněte prvek inverzní k prvku $[195]_{427}$.

— $[195]_{427}^{-1} = [-127]_{427} = [300]_{427}$.

5. (2 body) Určete zbytek po dělení čísla 6^{6^6} číslem 14.

— *Protože* $6^{6^6} \equiv 0 \pmod 2$ *a* $6^{6^6} \equiv 1 \pmod 7$, *zbytek po dělení čísla* 6^{6^6} *číslem* 14 *je* 8.

6. (2 body) Popište všechny podgrupy grupy $(\mathbb{Z}_7^*, \cdot)$.

— *Podgrupy jsou* 4 *a to :* Z_7^*, $\quad \{[1]_7, [2]_7, [4]_7\}$, $\quad \{[1]_7, [6]_7\}$, $\quad \{[1]_7\}$.

7. (2 body) Najděte nějakou permutaci $f \in \mathbb{S}_{10}$, která má ze všech prvků $\mathbb{S}_{10}$ největší řád.

— Permutace $(1,2) \circ (3,4,5) \circ (6,7,8,9,10)$ má maximální možný řád 30.

8. (4 body) Nechť $n \geq 2$ je přirozené číslo.

(a) Dokažte, že předpis $\alpha_n([a]_{2n}) = [a]_n$, kde $a \in \mathbb{Z}$, definuje korektně zobrazení $\alpha_n : \mathbb{Z}_{2n}^* \longrightarrow \mathbb{Z}_n^*$.

(b) Dokažte, že α_n je surjektivní homomorfismus grup.

(c) Ukažte, že zobrazení α_{17} je izomorfismus a zobrazení α_{18} není izomorfismus.

— *(a) Pro libovolná $a, b \in \mathbb{Z}$ platí $[a]_{2n} = [b]_{2n} \implies 2n \mid a - b \implies n \mid a - b \implies [a]_n = [b]_n$. Proto je zobrazení α_n korektně definováno.*

(b) Pro libovolná $a, b \in \mathbb{Z}$ platí $\alpha_n([a]_{2n} \cdot [b]_{2n}) = \alpha_n([ab]_{2n}) = [ab]_n = [a]_n \cdot [b]_n = \alpha_n([a]_{2n}) \cdot \alpha_n([b]_{2n})$ a zobrazení α_n je tedy homomorfismus. Ukážeme, že je surjektivní: nechť $[a]_n \in \mathbb{Z}_n^*$, tj. $a \in \mathbb{Z}$, $(a,n) = 1$. Pokud n je sudé, pak a je liché a máme $(a, 2n) = 1$, tj. $[a]_{2n} \in \mathbb{Z}_{2n}^*$ a $[a]_n = \alpha_n([a]_{2n})$. Pokud n je liché, pak právě jedno z čísel a a $a+n$ je liché, přičemž obě jsou nesoudělná s n. Proto buď $(a, 2n) = 1$ nebo $(a+n, 2n) = 1$ a tedy $[a]_{2n}$ či $[a+n]_{2n}$ je prvkem $\mathbb{Z}_{2n}^*$ a tudíž vzorem prvku $[a]_n$ v homomorfismu α_n.

(c) Protože $\varphi(17) = 16 = \varphi(34)$, mají grupy $\mathbb{Z}_{17}^*$ a $\mathbb{Z}_{34}^*$ stejný počet prvků. Protože je α_{17} surjektivní zobrazení mezi konečnými množinami o stejném počtu prvků, je α_{17} bijekce, a tudíž izomorfismus.
Podobně $\varphi(18) = 6 \neq 12 = \varphi(36)$ a grupy $\mathbb{Z}_{18}^*$ a $\mathbb{Z}_{36}^*$ nemohou být izomorfní, neboť mají rozdílný počet prvků.