**Алгебра, октобар 2008.** *18. септембар 2008.*

Име и презиме: Број индекса:

| 1 | 2 | 3 | 4 | 5 | Σ |
|---|---|---|---|---|---|
| | | | | | |

**1** Нека су $H$ и $K$ подгрупе групе $G$. Показати да је релација $\sim$ скупа $G$, дата са: $x \sim y \Leftrightarrow (\exists h \in H)(\exists k \in K)\, y = hxk$, релација еквиваленције, и наћи класе еквиваленције.

Решење:

рефлексивност: Како су $H$ и $K$ подгрупе, то $e \in H, K$, па је $x \sim x$, јер $x = exe$.

симетричност: Претпоставимо да је $x \sim y$. Тада за неке $h \in H$, $k \in K$, $y = hxk$. Множењем слева и сдесна са $h^{-1}$ и $k^{-1}$, добијамо $x = h^{-1}yk^{-1}$, па како $h^{-1} \in H$, а $k^{-1} \in K$, јер су $H$ и $K$ подгрупе, закључујемо $y \sim x$.

транзитивност: Претпоставимо $x \sim y$, $y \sim z$. Тада постоје $h_1, h_2 \in H$, $k_1, k_2 \in K$, тако да је $y = h_1xk_1$ и $z = h_2yk_2$. Али тада је $z = h_2h_1xk_2k_2$, и како $h_2h_1 \in H$ и $k_1k_2 \in K$, јер су $H$ и $K$ подгрупе, закључујемо $x \sim z$.

Одредимо класе. $y \in C_x$ ако и само ако $x \sim y$ а то је ако и само ако постоје $h \in H$ и $k \in K$ тако да је $y = hxk$. Одатле закључујемо $C_x = HxK$. □

**2** Показати да $7 \mid 2222^{5555} + 5555^{2222}$.

Решење: Користимо Ојлерову теорему, $\varphi(7) = 6$. Најпре приметимо да је $2222 =_7 3$ и $5555 =_7 4$, па је $2222^{5555} =_7 3^{5555}$ и $5555^{2222} =_7 4^{2222}$. Како је $(3,7) = 1$ и $(4,7) = 1$ можемо користити Ојлерову теорему, па како имамо $5555 =_6 5$ и $2222 =_6 2$, то је $3^{5555} =_7 3^5 =_7 3^3 3^2 =_7 6 \cdot 2 =_7 5$ и $4^{2222} =_7 4^2 =_7 2$. Коначно $2222^{5555} + 5555^{2222} =_7 5 + 2 =_7 0$. □

**3** Показати да група реда 150 није проста.

Решење: Нека је $G$ групе реда $150 = 2 \cdot 3 \cdot 5^2$. Нека је $H$ $S_5$-подгрупа од $G$, која постоји по Силовљевој првој теореми. Она је индекса $|G : H| = 6$, па можемо користити $n!$ теорему. Имамо $Core H \lhd G$ и показујемо да није тривијална и да је права подгрупа. Она јесте права јер $Core H < H \lneqq G$, а јесте и нетривијална, јер ако би била тривијална, имали бисмо $|G : Core H| = 150$, па према $n!$ теореми би $150 \mid 6! = 720$, што није тачно. □

**4** Одредити нормалну и елементарну форму Абелове група $G$, која је дата генераторима $a$, $b$, $c$ и релацијама:

$$\begin{array}{rrrcl} -12a & +18b & -18c & = & 0, \\ & 15b & -27c & = & 0, \\ -6a & +3b & +3c & = & 0. \end{array}$$

Одредити број елемената реда 6. Који је максималан ред елемента у $G$? Колико има елемената максималног реда?

Решење:

$$\begin{pmatrix} -12 & 18 & -18 \\ 0 & 15 & -27 \\ -6 & 3 & 3 \end{pmatrix} \sim \begin{pmatrix} 24 & 18 & -36 \\ 30 & 15 & -42 \\ 0 & 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 24 & 0 & -36 \\ 30 & 0 & -42 \\ 0 & 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 24 & 0 & -36 \\ 6 & 0 & -6 \\ 0 & 3 & 0 \end{pmatrix} \sim \begin{pmatrix} -12 & 0 & -36 \\ 0 & 0 & -6 \\ 0 & 3 & 0 \end{pmatrix} \sim \begin{pmatrix} -12 & 0 & 0 \\ 0 & 0 & -6 \\ 0 & 3 & 0 \end{pmatrix}$$

Из горњих једнакости видимо да је нормална форма групе $G = \mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{12}$. Из ње се види да је максималан ред елемента 12. Елементарна форма групе $G$ је $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Сваки елемент из $G$ је облика $(a, b, c, d, e)$, и важи $r(a) \in \{1, 2\}$, $r(b) \in \{1, 2, 4\}$, $r(c), r(d), r(e) \in \{1, 3\}$. Како је $r(a, b, c, d, e) =$ НЗС $(r(a), r(b), r(c), r(d), r(e))$, то имамо неколико могућности:

| $r(a)$ | $r(b)$ | $r(c)$ | $r(d)$ | $r(e)$ | има их |
|---|---|---|---|---|---|
| 1 | 2 | 1 | 1 | 3 | 2 |
| 1 | 2 | 1 | 3 | 1 | 2 |
| 1 | 2 | 1 | 3 | 3 | 4 |
| 1 | 2 | 3 | 1 | 1 | 2 |
| 1 | 2 | 3 | 1 | 3 | 4 |
| 1 | 2 | 3 | 3 | 1 | 4 |
| 1 | 2 | 3 | 3 | 3 | 8 |
| 2 | 1 | 1 | 1 | 3 | 2 |
| 2 | 1 | 1 | 3 | 1 | 2 |
| 2 | 1 | 1 | 3 | 3 | 4 |
| 2 | 1 | 3 | 1 | 1 | 2 |

| $r(a)$ | $r(b)$ | $r(c)$ | $r(d)$ | $r(e)$ | има их |
|---|---|---|---|---|---|
| 2 | 1 | 3 | 1 | 3 | 4 |
| 2 | 1 | 3 | 3 | 1 | 4 |
| 2 | 1 | 3 | 3 | 3 | 8 |
| 2 | 2 | 1 | 1 | 3 | 2 |
| 2 | 2 | 1 | 3 | 1 | 2 |
| 2 | 2 | 1 | 3 | 3 | 4 |
| 2 | 2 | 3 | 1 | 1 | 2 |
| 2 | 2 | 3 | 1 | 3 | 4 |
| 2 | 2 | 3 | 3 | 1 | 4 |
| 2 | 2 | 3 | 3 | 3 | 8 |
| | | | | укупно: | 78 |

Слично се добија да је број елемената максималног реда једнак 104. □

**5** Дат је полином $f(x) = x^3 + 2x^2 + 2x + 2 \in \mathbb{Z}_5[x]$.
**(а)** Показати да је $f(x)$ несводљив над $\mathbb{Z}_5$.
**(б)** Нека је $E$ скуп остатака полинома из $\mathbb{Z}_5[x]$ по модулу полинома $f(x)$. Показати да је $E$ поље.
**(в)** У пољу $E$ израчунати $\frac{1}{x^2+2x+2}$.

Решење: Како је $f(0), f(1), f(2), f(3), f(4) \neq 0$ у $\mathbb{Z}_5$, полином је несводљив. Стандардним поступком показује се да је $E$ поље. Приметимо да је $f(x) = x^3 + 2x^2 + 2x + 2 = x(x^2 + 2x + 2) + 2$, па је $f(x) - 2 = x(x^2 + 2x + 2)$. Одатле је $\frac{1}{x^2+2x+2} = \frac{x}{x(x^2+2x+2)} = \frac{x}{f(x)-2} = \frac{x}{3} = 2x$. $\square$