7. Grupuri finite (10 aprilie 2019)

7.1. **Relaţia de conjugare. Ecuaţia claselor.**

Definiţia 7.1. Fie G un grup. Atunci

(i) pentru orice $x \in G$, mulţimea

$$C(x) = \{g \in G \mid gx = xg\}$$

se numeşte *comutatorul lui* x.

(ii) mulţimea

$$Z(G) = \{x \in G \mid \forall g \in G,\ xg = gx\}$$

se numeşte *centrul lui* G.

(iii) relaţia omogenă pe G definită de

$$x \sim y \Leftrightarrow \exists g \in G \text{ astfel încât } g^{-1}xg = y$$

se numeşte *relaţia de conjugare* în grupul G.

Propoziţia 7.2. *Fie G un grup. Sunt adevărate afirmaţiile:*

(1) *Pentru orice $x \in G$, $C(x) \leq G$.*
(2) *$Z(G) \trianglelefteq G$ şi $Z(G) = \bigcap_{x\in G} C(x)$.*
(3) *Relaţia de conjugare este o relaţie de echivalenţă pe G şi pentru orice $x \in G$ clasa de echivalenţă a lui x este*

$$\mathbf{Cl}(x) = \{g^{-1}xg \mid g \in G\}.$$

(4) *pentru orice $x \in G$ avem*

$$|\mathbf{Cl}(x)| = |G : C(x)|.$$

(5) $|\mathbf{Cl}(x)| = 1 \Leftrightarrow \mathbf{Cl}(x) = \{x\} \Leftrightarrow x \in Z(G)$.

Demonstraţie. (1), (2) Temă.

(3)

$\square$

Definiţia 7.3. Dacă G este un grup şi $x \in G$, atunci $\mathbf{Cl}(x)$ se numeşte *clasa de conjugare a lui* x.

Corolarul 7.4. *Dacă G este un grup finit şi $x \in G$, atunci $|\mathbf{Cl}(x)|$ divide $|G|$.*

Teorema 7.5. ***(Ecuaţia claselor)***
Fie G un grup finit şi $x_1, \ldots, x_k$ o familie de reprezentaţi pentru clasele de conjugare (ale elementelor lui G) care au cel puţin două elemente. Atunci

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C(x_i)|.$$

Demonstraţie.

$\square$

7.2. p-grupuri şi teorema lui Cauchy.

Definiţia 7.6. Fie p un număr prim. Spunem că un grup finit G este un p-grup dacă $|G| = p^k$, unde $k \in \mathbb{N}^*$.

Corolarul 7.7. *Dacă G este un p-grup, atunci $Z(G) \neq 1$.*

Demonstraţie.

$\square$

Teorema 7.8. ***(Cauchy)***

Fie G un grup finit şi p un număr prim astfel încât p divide $|G|$. Atunci G are un element de ordin p.

Demonstraţie.

$\square$

Corolarul 7.9. *Dacă G este un grup finit şi există p prim astfel încât*

$$\forall x \in G \ \exists k \in \mathbb{N} \ \textit{a.î.} \ \operatorname{ord}(x) = p^k,$$

atunci G este un p-grup.

7.3. **Teoremele lui Sylow.**

Teorema 7.10. ***(prima teoremă a lui Sylow)***

Fie G un grup finit, p un număr prim şi $n \in \mathbb{N}$ astfel încât p^n divide $|G|$. Atunci G are un subgrup de cardinal p^n.

Demonstraţie.

$\square$

Definiţia 7.11. Fie G un grup finit, p un număr prim. Spunem despre un subgrup $H \leq G$ că este p-subgrup Sylow dacă există $n \in \mathbb{N}^*$ astfel încât $|H| = p^n$, p^n divide $|G|$, dar p^{n+1} nu divide $|G|$.

Teorema 7.12. ***(a doua teoremă a lui Sylow)***

Fie G un grup finit, p un număr prim astfel încât p divide $|G|$.

(a) *Dacă $H \leq G$ şi $|H| = p^k$ cu $k \in \mathbb{N}^*$, atunci există un p-subgrup Sylow $K \leq G$ astfel încât $H \leq K$.*

(b) *Dacă $L, K \leq G$ sunt p-subgrupuri Sylow ale lui G, atunci există $g \in G$ astfel încât $L = g^{-1}Kg$* (spunem că subgrupurile K şi L sunt *conjugate*).

(c) *Dacă n_p reprezintă numărul p-subgrupurilor Sylow ale lui G, atunci*
   - (i) $p \mid n_p - 1$;
   - (ii) $n_p \mid |G|$.

7.4. **Teorema fundamentală a grupurilor abeliene finite.**

Lema 7.13. *Fie* $(A, +)$ *un grup abelian şi* p *un număr prim. Atunci*

$$A_p = \{a \in A \mid \exists v \in \mathbb{N} : \ \mathrm{ord}(a) = p^v\}$$

este un subgrup al lui A*.*

Definiţia 7.14. A_p se numeşte p*-componenta lui* A.

Teorema 7.15. *Fie* $(A, +)$ *un grup abelian finit cu cel puţin două elemente.*

(a) ***(descompunerea în factori invarianţi)***
Există $k_1, \ldots, k_m \in \mathbb{N}^*$ *astfel încât*
  (i) $k_1 \mid k_2 \mid \ldots \mid k_m$;
  (ii) $A \cong \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_m}$.

(b) *Dacă* $p_1, \ldots, p_s$ *sunt toate numerele prime care divid* $|A|$*, atunci*
  (i) *pentru orice* $a \in A$ *există un unic element* $(a_1, \ldots, a_s) \in A_{p_1} \times \cdots \times A_{p_s}$ *astfel încât*

$$a = a_1 + \cdots + a_s;$$

  (ii) $A \cong A_{p_1} \times \cdots \times A_{p_s}$.
  (iii) *Dacă* A *este un* p*-grup, unde* p *este un număr prim, atunci* A *este izomorf cu un produs direct de* p*-grupuri ciclice.*

Exemplul 7.16.