$H = h\mathbb{Z}$, $N = m\mathbb{Z}$

$H \cap N = [h,m]\cdot\mathbb{Z}$, $H\cdot N = (h,m)\cdot\mathbb{Z}$

$$\frac{h\mathbb{Z}}{[h,m]\mathbb{Z}} \simeq \frac{(h,m)\mathbb{Z}}{m\mathbb{Z}}$$

$hm = [h,m]\cdot(h,m)$

17.04.2018

CURS 7

Grupuri finite

Def: Fie $(G,\cdot)$ un grup. Definim noțiunile:

a) dacă $x \in G$, mulțimea $C(x) = \{g \in G \mid g\cdot x = x\cdot g\}$ s.n. COMUTATORUL LUI x.

b) $Z(G) = \{x \in G \mid \forall g \in G, gx = xg\}$ s.n. CENTRUL LUI G

c) relația omogenă pe G definită de:

$$x \sim y \iff \exists\, g \in G \text{ a.î. } g^{-1}\cdot x\cdot g = y$$ s.n. RELAȚIE DE CONJUGARE PE G

Propoziție

Sunt adevărate afirmațiile:

a) $\forall x \in G$, $C(x) \leq G$

b) $Z(G) \trianglelefteq G$ și $Z(G) = \bigcap_{x \in G} C(x)$

c) relația de conjugare este o relație de echivalență pe G și $\forall x \in G$, clasa de echivalență a lui x este:

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

d) $\forall x \in G$, $|Cl(x)| = |G : C(x)|$

e) $|Cl(x)| = 1 \iff x \in Z(G)$

Dem: e)

a), b) temă

c) (R) $\forall x \in G$, $x = 1^{-1}\cdot x\cdot 1 \Rightarrow \forall x \in G$, $x \sim x$

(T) Fie $x, y, z \in G$ a.î. $x \sim y$ și $y \sim z \Rightarrow \exists\, g, h \in G$ a.î. $\left.\begin{array}{l} y = g^{-1}xg \\ z = h^{-1}yh \end{array}\right\} \Rightarrow$

$\Rightarrow z = h^{-1}g^{-1}xg\cdot h = (g\cdot h)^{-1}\cdot x(gh) \Rightarrow x \sim z$

(S) Fie $x, y \in G$ a.î. $x \sim y \Rightarrow \exists\, g \in G$ a.î. $g/y = g^{-1}xg/_{g^{-1}} \Rightarrow gyg^{-1} = x \Rightarrow$

$\Rightarrow (g^{-1})^{-1}y(g^{-1}) = x \Rightarrow y \sim x$

$\Rightarrow \sim$ relație de echivalență

d) $Cl(x) = \{y \in G \mid x \sim y\} = \{y \in G \mid \exists\, g \in G \text{ a.î. } y = g^{-1}xg\} = \{g^{-1}xg \mid g \in G\}$

$G/_{\rho_{C(x)}} = \{C(x)\cdot g \mid g \in G\}$, $C(x)\cdot g = C(x)\cdot h \iff g\cdot h^{-1} \in C(x) \iff (gh^{-1})x = x(gh^{-1})$

Fie $f : \{g^{-1}xg \mid g \in G\} \longrightarrow G/_{\rho_{C(x)}}$, $f(g^{-1}xg) = C(x)\cdot g$

$h/g^{-1}xg = h^{-1}xh/_{g^{-1}} \iff (hg^{-1})x = x(hg^{-1}) \iff h\cdot g^{-1} \in C(x) \iff C(x)\cdot h = C(x)\cdot g$ (*)

Folosind „$\Rightarrow$" din (*), obținem că f este bine definită

Folosind „$\Leftarrow$" din (*), obținem că f este injectivă

f surjectivă (evident)

$\Rightarrow f$ e bijectivă $\Rightarrow |Cl(x)| = |G : C(x)|$

Corolar

Dacă G - finit și $x \in G \Rightarrow |Cl(x)| \mid |G|$

Dem:

$|G| = |Cl(x)| \cdot \underbrace{|G : Cl(x)|}_{= Cl(x)}$

Exemplu:

$G = D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$Cl(1) = \{g^{-1} \cdot 1 \cdot g \mid g \in D_4\} = \underline{\{1\}}$

$Cl(r) = \{1^{-1} r 1, r^{-1} r r, r^{-2} r r^2, r^{-3} r r^3, s^{-1} \cdot r \cdot s, (sr)^{-1} \cdot r \cdot (sr), \dots\}$

$= \underline{\{r, r^3\}}$

$s^{-1} r s = s r s = s \cdot s r^3 = r^3$

$Cl(r^2) = \underline{\{r^2\}}$

$Cl(s) = \underline{\{s, sr^2\}}$

$Cl(sr) = \underline{\{sr, sr^3\}}$

$Z(D_4) = \{1, r^2\}$

$C(r) = \{1, r, r^2, r^3\}$

Teoremă (ecuația claselor)

Fie $(G, \cdot)$ grup finit și $x_1, x_2, \dots, x_k$ o familie de reprezentanți pentru clasele de conjugare $Cl(x)$ care au cel puțin două elemente.

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

Dem:

$G/_{\sim} = \{Cl(x) \mid x \in Z(G)\} \cup \{Cl(x) \mid |Cl(x)| \geq 2\}$

partiție pentru G

$\Rightarrow |G| = \sum_{x \in Z(G)} \underbrace{|Cl(x)|}_{=1} + \sum_{i=1}^{k} \underbrace{|Cl(x_i)|}_{= |G : C(x)|} = |Z(G)| + \underbrace{\sum_{i=1}^{k} \underbrace{|G : C(x)|}}_{\geq 2}$

$G = \{1\} \cup \{r^2\} \cup Cl(r) \cup Cl(s) \cup Cl(sr)$

r, s, sr - sistem de reprezentanți pentru clasele de conjugare cu cel puțin 2 elemente.

Obs Dacă G comutativ $\Rightarrow G = Z(G)$

Def: Fie p un număr prim. Spunem că un grup finit G este un p-grup dacă $\exists\, k \in \mathbb{N}^*$ a.î. $|G| = p^k$

Propoziție

Dacă G este un p-grup, atunci $Z(G) \neq \{1\}$

Dem:

Caz 1: G - abelian $\Rightarrow Z(G) = G \neq \{1\}$ $(|G| = p^k \geq 1)$

Caz 2: G - nu este abelian $\Rightarrow G \neq Z(G) \Rightarrow \exists\, x \in G \setminus Z(G) \Rightarrow$

$\Rightarrow \exists\, x \in G$ a.î. $|Cl(x)| = |G : C(x)| \geq 2$

Scriem ec. claselor: $|G| = |Z(G)| + \sum_{i=1}^{k} \underbrace{|G : C(x_i)|}_{\geq 2}$ unde $x_1, \dots, x_k \in G$ sunt elemente c în enunțul teoremei

$\forall\, i = \overline{1,k}$: $\underbrace{|G|}_{= p^k} = |C(x_i)| \cdot \underbrace{|G : C(x_i)|}_{\geq 2} \Rightarrow$

$\Rightarrow \forall\, i = \overline{1,k}$, $\exists\, k_i \geq 1$ a.î. $|G : C(x_i)| = p^{k_i}$

$\Rightarrow$ ecuația claselor devine

Teoremă (Cauchy)

Fie G - grup finit și p un număr prim a.î. $p \mid |G|$.

Atunci G are un element de ordin p.

Dem:

$|G| = n$. Inducție completă după n

Verificare

$n=1$ - proprietatea este evidentă (prin lipsă)

Pp. că $n>1$ și că $\forall H$ grup cu $|H|<|G|$, H are proprietatea din enunț.

• Caz 1: G - nu e comutativ $\Rightarrow G \neq Z(G)$

Scriem ecuația claselor:

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C(x_i)| \quad , x_1, \dots, x_k \notin Z(G) \text{ reprezentanți}$$

- Caz a) $\exists\, i = \overline{1,k}$ a.î. $\left.\begin{array}{l} p \mid |C(x_i)| \\ C(x_i) \neq G \end{array}\right\} \Rightarrow |C(x_i)| < |G| \Rightarrow \exists\, g \in C(x_i)$ cu $ord(g) = p \Rightarrow$

$\Rightarrow \exists\, g \in G$ a.î. $ord(g) = p$ (pt. că $C(x_i) \subseteq G$)

- Caz b) $\left.\begin{array}{l} \forall\, i = \overline{1,k}, \ p \nmid |C(x_i)| \\ p \mid |G| = |C(x_i)| \cdot |G : C(x_i)| \end{array}\right\} \Rightarrow \forall\, i = \overline{1,k}, \ p \mid |G : C(x_i)| \Rightarrow$

$\Rightarrow p$ divide toți termenii de forma $|G : C(x_i)|$ din ecuația claselor $\left.\begin{array}{l} \\ p \mid |G| \end{array}\right\} \Rightarrow p \mid |Z(G)|$

$\left.\begin{array}{l} p \mid |Z(G)| \\ Z(G) \neq G \end{array}\right\} \Rightarrow |Z(G)| < G \xrightarrow[\text{ind}]{\text{ip}} \exists\, g \in Z(G)$ a.î. $ord(g) = p \Rightarrow$

$\Rightarrow \exists\, g \in G$ a.î. $ord(g) = p$

• Caz 2: $G = Z(G) \Rightarrow G$ - abelian $\Rightarrow \forall\, H \leq G$, $H \trianglelefteq G$

$|G| \geq 2 \Rightarrow \exists\, x \in G \setminus \{1\}$. Fie $k = ord(x)$

- Caz a) $p \mid k \Rightarrow$ pt. $y = x^{\frac{k}{p}}$ avem $ord(y) = p$

- Caz b) $p \nmid k \Rightarrow (p, k) = 1$ (pt. că p - prim)

$$\langle x \rangle \trianglelefteq G \Longrightarrow \underbrace{|G|}_{\vdots\, p} = \underbrace{|\langle x \rangle|}_{k} \cdot |G/\langle x \rangle| \Rightarrow p \mid |G/\langle x \rangle|$$

$|\langle x \rangle| \geq 2 \Rightarrow |G/\langle x \rangle| < |G| \xrightarrow[\text{ind}]{\text{ip}} \exists\, y \in G$ a.î. $ord(y\langle x \rangle) = p \Rightarrow (y \cdot \langle x \rangle)^p = \langle x \rangle \Rightarrow$

$\Rightarrow y^p \cdot \langle x \rangle = \langle x \rangle \Rightarrow y^p \in \langle x \rangle \Rightarrow \exists\, a = \overline{0,k}$ a.î. $y^p = x^a$

$\Rightarrow (y^k)^p = (y^p)^k = (x^a)^k = (x^k)^a = 1^a = 1$

$\Rightarrow \left.\begin{array}{l} (y^k)^p = 1 \\ (k, p) = 1 \end{array}\right\} \Rightarrow y^k \neq 1$, altfel $ord(y\langle x \rangle) \neq p$ contradicție

$\Rightarrow \exists\, g = y^k$ a.î. $ord(g) = p$

Teoremă (Sylow)

Dacă G - grup finit și p este prim a.î. $p^n \mid |G| \Rightarrow G$ are un subgrup de ordin p^n

Dem:

- utilizează ec. claselor și corespondența dintre subgrupurile unui grup factor și subgrupurile grupului inițial

Obs: Dacă punem $n=1 \Rightarrow G$ are un subgrup de ordin $p \Rightarrow$ acel subgrup trebuie să fie generat de un element de ordin p. (vezi seminar)

Def: Fie G - grup finit și p - prim. Dacă $p^n \mid |G|$ și $p^{n+1} \nmid |G|$, atunci orice subg al lui G de cardinal p^n s.n. p-subgrup Sylow.

Teoremă (Sylow)

Fie G - grup finit, p - prim a.î. $p \mid |G|$.

a) $H \leq G$ și $|H| = p^k \Rightarrow \exists\, S \leq G$ un p-subgrup Sylow a.î. $H \subseteq S$

b) Orice două p-subgrupuri Sylow sunt conjugate, adică

$H, K \leq G$ p-subgrupuri Sylow $\Rightarrow \exists\, g \in G$ a.î. $K = g^{-1} H g$

c) Dacă n_p = numărul p-subgrupurilor Sylow ale lui G atunci

(i) $p \mid n_p - 1$

(ii) $n_p \mid |G|$

Teoremă (teorema fundamentală a grupurilor abeliene finite)

Fie $(A, +)$ un grup abelian finit.

a) (descompunerea în factori invarianți)

$\exists\, k_1, k_2, \dots, k_m \in \mathbb{N}^*$ a.î. $k_1 \mid k_2 \mid k_3 \mid \dots \mid k_m$ și $A \simeq \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \dots \times \mathbb{Z}_{k_m}$ (produs cartez

b) $\exists\, p_1, \dots, p_s$ - nr. prime și $A_{p_1}, A_{p_2}, \dots, A_{p_s}$ grupuri abeliene a.î.

$\forall\, i = \overline{1,s}$, A_{p_i} este un p_i-grup și $A \simeq A_{p_1} \times \dots \times A_{p_s}$

Mai mult, $\forall\, i = \overline{1,s}$, $A_{p_i} \simeq$ cu un produs de p_i-grupuri ciclice

$A_{p_i} \simeq \mathbb{Z}_{p_i^{\alpha_1}} \times \mathbb{Z}_{p_i^{\alpha_2}} \times \dots$