Grupos e Corpos

Prof. Lucas Calixto

Aula 7 - Os teoremas de Sylow

Ideia: reciproca do teorema de Lagrange para grupos satisfazendo certas condições

Teorema (Cauchy): Se p (primo) divide $|G|$, então G contem subgrupo de ordem p

Prova: Indução sobre $n = |G|$. Se $n = p \Rightarrow G$ é o subgrupo que queremos

Suponha que todo grupo de ordem $k < n$ tal que $p \mid k$ admite subgrupo de ordem p

Equação de classe $\Rightarrow |G| = |Z(G)| + \sum_{i=1}^{l} [G : C(x_i)]$. Lembrem: para $x \in G$, temos que $C(x) = \{g \in G \mid gx = xg\}$ = centralizador de x

- Se $\exists\ i$ tal que $p \mid |C(x_i)| \Rightarrow$ resultado segue por indução em $|C(x_i)|$
- Se $\nexists\ i$ tal que $p \mid |C(x_i)|$

$|G| = |C(x_i)|[G : C(x_i)] \Rightarrow p \mid [G : C(x_i)]\ \forall i \Rightarrow p \mid |Z(G)|$

TFGAF $\Rightarrow Z(G) \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_t^{r_t}} \Rightarrow \exists\ i$ tal que $p \mid |\mathbb{Z}_{p_i^{r_i}}| \Rightarrow \mathbb{Z}_{p_i^{r_i}} = \mathbb{Z}_{p^{r_i}}$

Logo, $\langle p^{r_i - 1} \rangle \leq \mathbb{Z}_{p^{r_i}}$ dá um subgrupo de G cuja ordem é p

O próximo resultado generaliza o Lema 2 da Aula 5 para grupos finitos gerais

Corolário: Um grupo finito G é um p-grupo $\Leftrightarrow |G| = p^n$

Prova: ($\Leftarrow$) Óbvia

($\Rightarrow$) Suponha q primo, $q \neq p$, e q divide $|G|$

Teorema de Cauchy $\Rightarrow \exists\ H \leq G$, $|H| = q \Rightarrow |h| = q,\ \forall\ h \in H \Rightarrow G$ não é p-grupo

Exemplo: $|A_5| = 5!/2 = 60 = 2^2 \cdot 3 \cdot 5 \Rightarrow A_5$ admite subgrupos de ordem $2, 3$ e 5

Primeiro Teorema de (1ºTS)

Teorema (1ºTS): Se p^r (primo) divide $|G|$, então G contem subgrupo de ordem p^r

Prova: Indução sobre $n = |G|$. Se $n = p \Rightarrow G$ é o subgrupo que queremos

Suponha que todo grupo de ordem $k < n$ tal que $p^r \mid k$ admite subgrupo de ordem p^r

$|G| = |Z(G)| + \sum_{i=1}^{l} [G : C(x_i)]$

• $\exists\ i$ tal que $p \nmid [G : C(x_i)] \Rightarrow p^r \mid |C(x_i)|$ resultado segue por indução em $|C(x_i)|$

• $p \mid [G : C(x_i)]|\ \forall i \Rightarrow p \mid |Z(G)|$. Teorema de Cauchy $\Rightarrow Z(G)$ tem elemento g de ordem p. Seja $N = \langle g \rangle \leq Z(G)$

$N \subset Z(G) \Rightarrow N \lhd G$ e $|G/N| = p^{r-1}$

Indução $\Rightarrow G/N$ possui subgrupo $\bar{H}$ de ordem p^{r-1}

Teorema de correspondência $\Rightarrow \bar{H} = H/N$, onde $H \leq G$ e $N \subset H$

$|H| = p^r$ (por que?)

Considere $\mathcal{S} = \{K \leq G\}$. Para $H \leq G$, temos que H age em $\mathcal{S}$ via conjugação

$$H \times \mathcal{S} \to \mathcal{S}, \quad h \cdot K = hKh^{-1} \quad \text{(nessa aula a ação será denotada por } \cdot\text{)}$$

Defina $N(H) = \{g \in G \mid gHg^{-1} = H\} =$ normalizador de H em G

Exercício: Prove que $N(H)$ é o maior subgrupo de G tal que $H \lhd N(H)$

Um p-subgrupo de G que é maximal no conjunto dos p-subgrupos de G é chamado um p-subgrupo de Sylow. Defina $\text{Syl}_p(G) = \{P \leq G \mid P \text{ é } p\text{-subgrupo de Sylow}\} \subset \mathcal{S}$

Pelo Corolário do slide 3, $P \in \text{Syl}_p \Leftrightarrow |P| = p^l$ para algum l

Lema 1: Seja $|G| = p^r m$ com $mdc(p, m) = 1$. Então $\text{Syl}_p(G) = \{P \leq G \mid |P| = p^r\}$

Prova: ($\supset$) Suponha $|P| = p^r$ e tome $Q \in \text{Syl}_p(G)$ tal que $P \subset Q$. Então, $|Q| = p^l$

p^l divide $|G| = p^r m$ e $mdc(p, m) = 1 \Rightarrow p^l \leq p^r \Rightarrow p^l = p^r \Rightarrow Q = P$

($\subset$) Seja $P \in \text{Syl}_p(G)$. Se $|P| = p^l < p^r \Rightarrow |G/P| = p^{r-l}m$. ($1^{\text{o}}$TS) + (teorema de correspondência) $\Rightarrow \exists\, Q \leq G$ tal que $|Q/P| = p^{r-l} > 1 \Rightarrow P \subsetneq Q$

$p^{r-l} = |Q/P| = |Q|/|P| \Rightarrow |Q| = p^r \Rightarrow Q$ é p-subgrupo e $P \subsetneq Q$ (contradição)

Lema 2: Seja $P \in \mathrm{Syl}_p(G)$ e $x \in G$, $|x|$ é potência de p. Se xPx^{-1}, então $x \in P$

Prova: $x \in N(P)$ e $\langle xP \rangle \leq N(P)/P$ é subgrupo cíclico cuja ordem é potência de p

$\langle xP \rangle = H/P$, onde $H \leq N(H)$ e $P \subset H$

$|\langle xP \rangle| = |H/P| = |H|/|P| \Rightarrow |H|$ é potência de p

Se $P \in \mathrm{Syl}_p(G)$, Lema 1 $\Rightarrow P = H \Rightarrow H/P = \{e\} \Rightarrow x \in P$

Lema 3: Se $H \times \mathcal{S} \to \mathcal{S}$ é como no slide anterior $\Rightarrow |O_K| = [H : N(K) \cap H],\ \forall K \in \mathcal{S}$

Prova: orbita-estabilizador $\Rightarrow |O_K| = [H : H_K]$, onde H_K é o estabilizador de K

Como $H_K = \{h \in H \mid hKh^{-1} = K\} = H \cap N(K)$ o resultado segue

Suponha que G age em X. Tal ação é dita transitiva se $X = O_x, \forall x \in X$

Seja p primo que divide $|G|$ e considere $\mathrm{Syl}_p(G)$. Note que

$$G \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G), \quad g \cdot P = gPg^{-1}$$

é bem definida, pois $P \cong gPg^{-1},\ \forall g \in G$

2º Teorema de Sylow (2ºTS): Suponha que p divide $|G|$. Então, a ação $G \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G)$ por conjugação é transitiva. Equivalentemente, quaisquer dois p-subgrupos de Sylow de G são conjugados um do outro.

Prova: Suponha $|G| = p^r m$ com $mdc(p, m) = 1$

Seja $P \in \mathrm{Syl}_p(G)$. Afirmamos que $G \cdot P = \{P = P_1, P_2, \ldots, P_k\} = \mathrm{Syl}_p(G)$

Lema 3 $\Rightarrow k = |G \cdot P| = [G : N(P)]$

Lagrange $\Rightarrow p^r m = |G| = |N(P)|[G : N(P)] = |N(P)|k$

$P \leq N(P) \Rightarrow p^r$ divide $|N(P)| \Rightarrow p \nmid k$ (pois $mdc(p, m) = 1$)

Tome $Q \in \mathrm{Syl}_p(G)$ qualquer, e considere a ação $Q \times G \cdot P \to G \cdot P$, $q \cdot P_i = qP_iq^{-1}$

Lema 3 $\Rightarrow |Q \cdot P_i| = [Q : N(P_i) \cap Q]$

Lema 1 + Lagrange $\Rightarrow p^r = |Q| = [Q : N(P_i) \cap Q]|N(P_i) \cap Q| \Rightarrow |Q \cdot P_i| = p^{l_i}$

$G \cdot P = Q \cdot P_{i_1} \dot{\cup} \cdots \dot{\cup}\, Q \cdot P_{i_t} \Rightarrow k = |G \cdot P| = p^{l_{i_1}} + \cdots + p^{l_{i_t}}$

$p \nmid k \Rightarrow \exists\ l_{ij} = 0 \Rightarrow Q \cdot P_{i_j} = P_{i_j} \Rightarrow qP_{i_j}q^{-1} = P_{i_j},\ \forall q \in Q$

Lema 3 $\Rightarrow Q \subset P_{i_j} \Rightarrow Q = P_{i_j}$ já que $|Q| = p^r = |P_{i_j}| \Rightarrow Q \in G \cdot P$

Como $Q \in \mathrm{Syl}_p(G)$ foi arbitrário, temos que $\mathrm{Syl}_p(G) = G \cdot P$

3º Teorema de Sylow (3ºTS) Suponha que p divide $|G|$. Então,

1. $|\mathrm{Syl}_p(G)|$ divide $|G|$
2. $|\mathrm{Syl}_p(G)| \equiv 1\ (mod\ p)$

Prova: (1): Seja $P \in \mathrm{Syl}_p(G)$ e $G \cdot P = \{P = P_1, P_2, \ldots, P_k\}$

orbita-estabilizador $\Rightarrow |G \cdot P| = [G : G_P]$ que divide $|G|$, por Lagrange

2ºTS $\Rightarrow |\mathrm{Syl}_p(G)| = |G \cdot P| \Rightarrow$ afirmação 1

(2): da prova do 2ºTS, temos

$$\mathrm{Syl}_p(G) = G \cdot P = P \cdot P_1 \dot{\cup} \cdots \dot{\cup}\ P \cdot P_k \Rightarrow |\mathrm{Syl}_p(G)| = p^{l_1} + \cdots + p^{l_k},$$

onde $|P \cdot P_i| = p^{l_i}$

Lema 2 $\Rightarrow |P \cdot P_i| = 1 \Leftrightarrow i = 1 \Rightarrow |\mathrm{Syl}_p(G)| \equiv 1\ (mod\ p)$

Corolário: Se $|G| = p^r m$ com $mdc(p, m) = 1$, então $|\mathrm{Syl}_p(G)|$ divide m

Prova: Exercício

Aplicações

Exemplo: Como $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$, 1^{o}TS $\Rightarrow$ A_5 tem subgrupos de ordem $2, 4, 3$ e 5

Os p-subgrupos de Sylow de A_5 tem ordem $3, 4$ e 5

Afirmamos que $|\text{Syl}_5(A_5)| = 2$. De fato,

3^{o}TS $\Rightarrow$ $|\text{Syl}_5(A_5)|$ divide 12 e $|\text{Syl}_5(A_5)| \equiv 1 \ (mod\ 5) \Rightarrow |\text{Syl}_5(A_5)| = 1$ ou 6

Se $\text{Syl}_5(A_5) = \{P_5\} \Rightarrow P_5 \lhd G$ (pois $G \cdot P_5 = \{P_5\}$ pelo 2^{o}TS), o que contradiz o fato de A_5 ser simples

Logo, $|\text{Syl}_5(A_5)| = 6$

Teorema: Sejam $p < q$ primos tais que $|G| = pq$. Então,

1. G possui um único subgrupo Q cuja ordem é q
2. Q é normal em G (em particular, G não é simples)
3. se $q \not\equiv 1 \ (mod\ p)$, então G é cíclico

Prova: 1^{o}TS $\Rightarrow \exists\ P, Q \leq G$ tal que $|P| = p$ e $|Q| = q$

3^{o}TS $\Rightarrow |\mathrm{Syl_q(G)}|$ divide p e $|\mathrm{Syl_q(G)}| = 1 + kq$, para algum $k \in \mathbb{Z}$

$q > p \Rightarrow k = 0 \Rightarrow \mathrm{Syl_q(G)} = \{H\}$

2^{o}TS $\Rightarrow G \cdot Q = \{Q\} \Rightarrow Q \lhd G$

3^{o}TS $\Rightarrow |\mathrm{Syl_p(G)}|$ divide q e $|\mathrm{Syl_p(G)}| = 1 + kp$, para algum $k \in \mathbb{Z} \Rightarrow 1 + kp = 1$ ou q

$q \not\equiv 1 \ (mod\ p) \Rightarrow 1 + kp = 1 \Rightarrow k = 0 \Rightarrow \mathrm{Syl_p(G)} = \{P\}$

2^{o}TS $\Rightarrow G \cdot P = \{P\} \Rightarrow P \lhd G$

Exercício:

(1) Se $H \lhd G,\ K \lhd G$ e $H \cap K = \{e\}$, então $hk = kh,\ \forall h \in H,\ k \in K$

(2) Prove que P, Q no teorema satisfazem os critérios para que $G \cong P \times Q$

Logo, $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq} \Rightarrow G$ é cíclico

Exemplo: Se $|G| = 15$, então G é cíclico. De fato, $|G| = 3 \cdot 5$ e $5 \not\equiv 1\ (mod\ 3)$

Exemplo: Suponha que $|G| = 99 = 3^2 \cdot 11$

3^{o}TS $\Rightarrow |\mathrm{Syl}_3(\mathrm{G})| = 1 + 3k$, e $|\mathrm{Syl}_3(\mathrm{G})|$ divide $11 \Rightarrow |\mathrm{Syl}_3(\mathrm{G})| = 1$

Analogamente, $|\mathrm{Syl}_{11}(\mathrm{G})| = 1$

2^{o}TS $\Rightarrow P_3$ e P_{11} são normais em G

$|P_3| = 9 = 3^2 \Rightarrow P_3$ é abeliano $\Rightarrow P_3 \cong \mathbb{Z}_9$ ou $P_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Também $P_{11} \cong \mathbb{Z}_{11}$

Exercício acima $\Rightarrow G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$ ou $G \cong \mathbb{Z}_9 \times \mathbb{Z}_{11}$

Checando simplicidade

Exemplo: Se $|G| = 20 = 2^2 \cdot 5$, então G não é simples

3^{o}TS $\Rightarrow |\mathrm{Syl}_5(\mathrm{G})| \equiv 1 \pmod 5$ e divide $4 \Rightarrow |\mathrm{Syl}_5(\mathrm{G})| = 1 \Rightarrow \mathrm{P}_5 \lhd \mathrm{G}$

Exemplo: Se $|G| = p^r$, então G não é simples

Nesse caso $Z(G)$ é não trivial $\Rightarrow G$ não é simples

Exemplo: Se $|G| = 56 = 2^3 \cdot 7$, então G não é simples

3^{o}TS $\Rightarrow |\mathrm{Syl}_7(G)| = 1$ ou 8, e $|\mathrm{Syl}_2(G)| = 1$ ou 7. Se $|\mathrm{Syl}_7(G)| = 1 \Rightarrow$ OK

Suponha $\mathrm{Syl}_7(G) = \{P_1, \ldots, P_8\}$

$P_i \cong \mathbb{Z}_7$ para todo $i \Rightarrow P_i \cap P_j = \{e\} \Rightarrow$ os P_i's nos dão $8 \cdot 6 = 48$ elementos

Se $Q \in \mathrm{Syl}_2(G) \Rightarrow Q \cap P_j = \{e\}$ para todo i

Isso já nós dá os $48 + 7 + 1 = 56$ elementos de $G \Rightarrow \mathrm{Syl}_2(G) = \{Q\} \Rightarrow Q \lhd G$

Lema: Se $H, K \leq G$, então $|HK| = \frac{|H||K|}{|H \cap K|}$

Prova: Sejam $H = \{h_i \mid i \in I\}$, $K = \{k_j \mid j \in J\}$ e $HK = \{h_i k_j \mid i \in I,\ j \in J\}$

Contando as repetições de $h_{i_1} k_{j_1}$ em HK:

$h_{i_1} k_{j_1} = h_{i_2} k_{j_2} \Leftrightarrow a = h_{i_2}^{-1} h_{i_1} = k_{j_2} k_{j_1}^{-1} \in H \cap K$

Logo, repetições de $h_{i_1} k_{j_1} \leq |H \cap K|$

Reciprocamente, cada $b \in H \cap K$ nos dá uma repetição de $h_{i_1} k_{i_1}$. De fato, se $h_{i_2} = h_{i_1} b^{-1}$ e $k_{j_2} = b k_{i_1}$, então $h_{i_1} k_{j_1} = h_{i_2} k_{j_2}$

Além disso, $h_{i_2} = h_{i_1} b^{-1}$ e $h_{i_2} = h_{i_1} a^{-1} \Leftrightarrow a = b \Rightarrow$ elementos diferentes de $H \cap K$ nos dão repetições diferentes de $h_{i_1} k_{j_1}$

Logo, $|H \cap K| \leq$ repetições de $h_{i_1} k_{j_1}$

Assim, cada $h_i k_j$ aparece exatamente $|H \cap K|$ vezes em HK

Portanto, $|HK| = |H||K|/|H \cap K|$

Exemplo: Se $|G| = 48 = 2^4 \cdot 3$, então G não é simples

3^{o}TS $\Rightarrow |\mathrm{Syl}_2(G)| = 1$ ou 3. Se é 1, OK

Suponha $|\mathrm{Syl}_2(G)| = 3$ e tome $H, K \in \mathrm{Syl}_2(G)$ (ambos com ordem $2^4 = 16$)

Afirmamos que $H \cap K \lhd G$

$H \cap K \leq H, K \Rightarrow |H \cap K| = 1, 2, 4, 8, 16$ (16 não pode pois $H \neq K$)

$|H \cap K| \leq 4 \Rightarrow |HK| = \frac{16 \cdot 16}{|H \cap K|} = 64 \geq 48$ (contradição)

Assim, $|H \cap K| = 8 \Rightarrow H \cap K \lhd H$ e $H \cap K \lhd K$ (pois são subgrupos de índice 2)

$H \neq K \Rightarrow H$ e K estão propriamente contidos no normalizador $N(H \cap K)$

Logo, $16 = |H| = |K|$ divide $|N(H \cap K)|$

$|N(H \cap K)| > 16$

$|N(H \cap K)|$ divide 48

$\Rightarrow |N(H \cap K)| = 48 \Rightarrow N(H \cap K) = G \Rightarrow H \cap K \lhd G$

Exercícios:

1, 2, 3, 4, 5, 7, 8, 10, 11, 12, 13, 14, 18, 22, 23, 26