Aula 08

P-GRUPOS E O TEOREMA DE CAUCHY

META

Conceituar p-grupos e estabelecer o Teorema de Cauchy

OBJETIVOS

Definir p-grupos e aplicar suas propriedades na resolução de problemas.

Reconhecer o teorema de Cauchy sobre ordens de grupos finitos e aplicá-lo na resolução de problemas.

PRÉ-REQUISITO

As aulas 4,5,6 e 7.

INTRODUÇÃO

Olá caro aluno, vamos a mais uma aula sobre a teoria dos grupos. Espero que você esteja gostando e aprendendo, pois precisamos dos conteúdos das anteriores para compreender os conteúdos da presente aula.

Como sabemos, quando um grupo G *é finito e* H *é um subgrupo de* G*, o teorema de Lagrange afirma que* $|H|\,\big|\,|G|$*. O recíproco do Teorema de Lagrange não é em geral verdadeiro. Nesta aula estudaremos os primeiros resultados que estabelecem hipóteses segundo as quais, para um divisor positivo* d *da ordem de um grupo finito* G*, existe um subgrupo* H *de* G *cuja ordem é* d*.*

CLASSES DE CONJUGAÇÃO E P-GRUPOS

Seja G *um grupo. Vamos definir em* G *uma relação binária do seguinte modo: dados* $a, b \in G$*,* a *é conjugado de* b *e indicamos "*$a \sim b$*" se existe um* $g \in G$ *tal que* $b = g^{-1}ag$

Notemos que: $a = e^{-1}ae \Rightarrow a \sim a \ \forall a \in G$*. Se* $a \sim b$ *então existe* $g \in G$ *tal que* $b = g^{-1}ab \Rightarrow a = (g^{-1})^{-1}bg^{-1} \Rightarrow b \sim a$*.*

Se $a \sim b$ *e* $b \sim c$ *então existem* $g, h \in G$ *tais que* $b = g^{-1}ag$ *e* $e = h^{-1}bh$*. Logo* $e = h^{-1}(g^{-1}ag)h = (h^{-1}g^{-1})a(gh) = (gh)^{-1}a(gh) \Rightarrow a \sim c$*.*

Provamos que a relação binária "$\sim$*" é uma relação de equivalência em* G*.*

Definição 1. Dado $a \in G$*, chamamos classe de conjugação de elemento* a *em* G*, e indicamos por* C_a *à classe de equivalência de* a*, módulo a relação de equivalência acima definida.*

Assim, $G = \underset{a \in G}{\uplus} C_a$ *e* $|G| = \sum_{a \in G} |C_a|$

Notemos que $a \in \mathbb{Z}(G)$ *se, e somente se,* $\forall g \in G, g^{-1}ag = g^{-1}ga = a$*, ou seja,* $a \in \mathbb{Z}(G) \Leftrightarrow C_a = \{a\}$*. Segue daqui, que* $|G| = |\mathbb{Z}(G)| + \sum_{a \in \mathbb{Z}(G)} |C_a|$

Esta é a chamada equação das classes e a usaremos a seguir em alguns teoremas.

Proposição 1. Seja G *um grupo finito,* $a \in G$ *e* $H = C_G(a)$ *(o centralizador de* a *em* G*).*

Então $[G : H] = |C_a|$ *e conseqüentemente* $|C_a|\,\big|\,|G|$*.*

Demonstração: Vamos considerar a aplicação ψ *de* $G/_H$ *em* C_a *dada por* $\psi(Hg) = g^{-1}ag$*.*

Notemos que se $Hg_1 = Hg_2$ *então* $g_1g_2^{-1} \in C_G(a)$ *ou seja que* $g_1g_2^{-1}a = ag_1g_2^{-1} \Rightarrow g_2^{-1}ag_2 = g_2^{-1}ag_1$ *ou melhor* $\psi(Hg_1) = \psi(Hg_2)$, *portanto* ψ *está bem definida.*

Se $\psi(Hg_1) = \psi(Hg_2)$ *então* $g_1^{-1}ag_1 = g_2^{-1}ag_2 \Rightarrow ag_1g_2^{-1} = g_1g_2^{-1}a \Rightarrow g_1g_2^{-1} \in C_G(a) = H \Rightarrow g_1 \equiv g_2(modH)$ *ou seja* $Hg_1 = Hg_2$ *donde segue que* ψ *é injetiva.*

Como dado $b \in Ca$, $\exists g \in G;\ b = g^{-1}ag$ *temos que* $\psi(Hg) = b$ *ou seja* ψ *é sobrejetiva.*

Sendo ψ *uma bijeção de* ${}^{G}/_{H}$ *em* C_a *para cada* $a \in G$, *temos que* $|{}^{G}/_{H}| = |C_a|$, *com queríamos demonstrar.*

Definição 2. Dizemos que um grupo finito G *é um p-grupo se* $|G| = p^n$ *onde* p *é um primo positivo e* $n \in \mathbb{Z}_+$.

Exemplo. $G = \{e\}$, $D_4 = \{e, r, \theta, r\theta\}$ *e* $G = \mathbb{Z}p$ *têm ordens* $p^0, 2^2$ *e* p^1 *respectivamente portanto são p-grupos.*

Proposição 2. Se G *é um p-grupo e* $|G| > 1$ *então* $\mathbb{Z}(G)$ *também é um p-grupo e* $|\mathbb{Z}(G)|>1$.

Demonstração: Seja $|G| = p^n > 1$. *Como* $\mathbb{Z}(G) \leq G$, *do teorema de Lagrange,* $|\mathbb{Z}(G)| \big| p^m$, *logo,* $\exists\ n \in \mathbb{Z}_+$, $0 \leq n \leq m$ *tal que* $|\mathbb{Z}(G)| = p^n$.

Para cada $a \notin \mathbb{Z}(G), |C_a| > 1$ *e da proposição anterior,* $|C_a| \big| p^m$ *logo,* $\sum_{a \notin p} |C_a|$, *é um múltiplo de* p.

Como $p^m = |G| = \mathbb{Z}(G)| + \sum_{a \in G} |C_a|$ *temos que* $p \big| |\mathbb{Z}(G)| \Rightarrow p \big| p^n \Rightarrow n \geq 1$ *ou seja* $|\mathbb{Z}(G)| = p^n > 1$.

Exemplo 1. Se $|G| = p^2$ *onde* p *é um primo positivo, então* G *é abeliano. Da proposição acima,* $|\mathbb{Z}(G)| > 1$ *e divide* p^2, *logo,* $|\mathbb{Z}(G)| = p^2$ *e conseqüentemente* $G = \mathbb{Z}(G)$ *ou seja,* G *é abeliano.*

O TEOREMA DE CAUCHY

Proposição 3. Sejam G *um grupo finito e* $p \in \mathbb{Z}_+$ *um primo. Se* $p \big| |G|$ *então existe um elemento* $a \in G$ *tal que* $O(a) = p$, *ou melhor,* G *tem um subgrupo cíclico de ordem* p.

Demonstração: Vamos usar indução sobre $n = |G|$. *Se* $n = 2$, *como já sabemos,* $\exists a \in G$ *tal que* $G =< a >= \{e, a\}$ *e o teorema é verdadeiro.*

Vamos por hipótese de indução supor que o teorema é verdadeiro para todo grupo que tenha ordem $< n = |G|$ e considerar os três casos:

1º Caso – G é cíclico. Neste, $\exists b \in G$ tal que $G =< b >= \{e, b, \ldots, b^{n-1}\}$ e seja $p \in \mathbb{Z}_+$ um divisor primo de n. Escrevendo $n = p^m.q$ onde $m \geq 1$ e $q \in \mathbb{Z}_+$, para $a = b^{p^{n-1}.q}$, temos $a^p = (b^{p^{n-1}.q})^p = b^n = e$ e, além disto, $a \neq e$ pois $O(b) = n > \frac{n}{p}$. Portanto $< a >$ é um subgrupo cíclico de ordem p, como queríamos.

2º Caso – G não é cíclico, mas é abeliano. Sejam p um divisor primo de n e $b \in G\backslash\{e\}$. Se $p|O(b)$ então p divide a ordem do subgrupo cíclico $< b >$ de G e, pelo 1º caso existe um $a \in < b >$ tal que $O(a) = p$. Como $p\Big|\,| < b > |$ e $| < b > \Big|n$ segue que $p|n$.

Se $p \nmid O(b)$, escrevendo $n =< b >$ e lembrando que $|G| = n = |N| \cdot |\frac{G}{N}|$, segue que $p\Big||\frac{G}{N}|$. Como $\left|\frac{G}{N}\right| < n$, por hipótese de indução, existe $Nc \in \frac{G}{N}\backslash\{N\}$ tal que $O(Nc) = p$.

Assim, $c \notin N$ e $(Nc)^p = Nc^p = N \Longrightarrow c \notin N$ e $c^p \in N$. Seja $m = O(b) = O(N)$, estão $(c^p)^m = (c^m)^p = e \Longrightarrow O(c^m) = 1$ ou $O(c^m) = p$.

Se fosse, $O(c^m) = 1$, teríamos $Nc^n = N \Longrightarrow (Nc)^m = N \Longrightarrow p|m$ uma contradição.

Logo, $O(c^m) = p$. Tomando $a = c^m$, temos que $a \in G$ e $O(a) = p$.

3º Caso – G não é abeliano. Neste caso, consideremos a equação das classes $|G| = |\mathbb{Z}(G)| + \sum_{a \notin \mathbb{Z}(G)} |C_a|$ e seja $p \in \mathbb{Z}_+$ um primo divisor de $|G|$.

Consideremos as duas possibilidades:

1ª Possibilidade: $p\Big||\mathbb{Z}(G)|$. Neste caso, como $\mathbb{Z}(G)$ é abeliano, pelas partes anteriores, existe $a \in \mathbb{Z}(G)$ tal que $O(a) = p$.

2ª Possibilidade: $p\nmid|\mathbb{Z}(G)|$. Agora, como $p\Big||G|$, considerando a equação das classes, temos que existe pelo menos um $b \notin \mathbb{Z}(G)$ tal que $p\nmid|C_b|$.

Como $|C_b| = [G : C_G(b)]$ e $|G| = |C_G(b)|.[G : C_G(b)]$ segue que $p\Big||C_G(b)$. Sendo $|C_G(b)| < |G|$ por hipótese de indução existe $a \in C_G(b)$ tal que $O(a) = p$, concluindo com isto a nossa demonstração.

CLASSIFICAÇÃO DOS GRUPOS FINITOS DE ORDENS ≤ 6.

Já sabemos que os grupos de ordens 1,2,3 *e* 5 *são todos cíclicos e conseqüentemente abelianos.*

Seja G *um grupo de ordem* 4. G *pode ser cíclico, por exemplo,* $G = \{1, i, i^2, i^3\} = \{1, i, -1, -i\}$, *munido da multiplicação dos números complexos é um grupo cíclico de ordem* 4.

Se $\forall a \in G, a \neq e, < a > \neq G$ *então,* $\{e\} \subsetneq < a > \subsetneq G$, *logo* $a^2 = 2$, *ou seja,* $\mathcal{O}(a) = 2$.

Neste caso se $a, b \in G$, $ab = (ab)^{-1} = b^{-1}.a^{-1} = ba$, *ou seja* G *é abeliano. Notemos que estes grupos existem, veja o grupo* $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

Podemos então afirmar que todo grupo de ordem ≤ 5 *é abeliano.*

Agora, seja G *um grupo de ordem* 6. *Do teorema de Cauchy, existem* $a, b \in G$ *tais que* $\mathcal{O}(a) = 2$ *e* $\mathcal{O}(b) = 3$. *Seja* $N = < b >$, *como* $[G : N] = 2$ *sabemos da aula anterior que* $N \trianglelefteq G$. *Logo,* $\forall c \in G$, $c^{-1}bc \in \{e, b, b^2\}$. *Assim,* $c^{-1}bc = b \Longrightarrow bc = cb$ *ou* $c^{-1}bc = b^{-1}$ *e neste caso* $G = \{e, b, b^2, a, ab, ab^2\}$.

No primeiro caso, se $g = ab$ *então* $\mathcal{O}(g) = 6$ *e* $G = \{e, a, \dots, a^5\} = < a >$ *é cíclico.*

No segundo caso, $G = D_3 = S_3 = < b, a > = \{e, b, b^2, a, ab, ab^2\}$.

Uma das ocupações dos estudiosos da teoria dos grupos é estudar as possíveis naturezas dos grupos finitos de uma mesma ordem. É uma tarefa difícil e trabalhosa.

RESUMO

Nesta aula definimos os p-grupos e estabelecemos o teorema de Cauchy, onde começamos apresentando as classes de conjugação e sua equação que é um conteúdo fundamental na demonstração que fizemos do teorema, de Cauchy, acima referido.

ATIVIDADES

1. Calcule todas as classes de conjugação de S_n *e de* D_4 .

2. Se G *é um* p*-grupo tal que* $|G| = p^3$, *prove que* $|Z(G)| = p$.

3. Se G *é um grupo finito que tem exatamente duas classes de conjugação, provar que* G *é abeliano.*

4. Se G tem três classes de conjugação, calcule as possibilidades para a ordem de G.

5. Sejam $\psi : G \longrightarrow G'$ um homomorfismo injetivo de G em G' e $p \in \mathbb{Z}_+$ um primo tal que $p \bigm| |G|$. Prove que existe $H' \leq G'$ tal que $|H'| = p$.

COMENTÁRIO DAS ATIVIDADES

Na primeira atividade, você deve ter começado olhando os elementos dos centros e depois tomado elementos fora do centro e obtendo distintamente seus conjugados.

Na segunda atividade, você deve ter percebido que para $a \in G \backslash Z(G)$, $Z(G) \leq C_G(a) \leq G$ e usado este fato.

Na segunda e terceira atividades, você deve ter usado a equação das classes e que $\forall a \in G.$ $|C_a| \bigm| |G|$.

Na quinta atividade, você deve ter usado o teorema de Cauchy e o primeiro teorema dos isomorfismos (ou o da correspondência).

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de algebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).