Notas de Aula do Seminário Semanal de Álgebra

Pedro Henrique Cavalcanti da Silva[1], Igor dos Santos Lima[2]
[1]Graduando em Matemática da Universidade Federal de Goiás - UFG - Campus Catalão e Bolsista do PIBIC/CNPq.
[2]Doutor em Matemática pela Universidade Estadual de Campinas UNICAMP e Professor do Departamento de Matemática da Universidade Federal de Goiás - UFG - Campus Catalão

Parte 1 - Preliminares

Definição 0.1. *Seja um conjunto G, e uma operação binária *. Dizemos, denotando por (G,*) que G é* ***GRUPO*** *se:*

1. *Houver associatividade com a operação *;*
2. *Existir Elemento neutro, denotado por e_G;*
3. *Existir Inverso para todo elemento, denotado por a', para algum elemento a.*

Definição 0.2. *Seja H um subconjunto de G, sendo G um grupo. Diz-se H subgrupo, denotado por $H \leq G$, se:*

- $H \neq \varnothing$;
- $h_1 * h_2 \in H$, $\forall h_1, h_2 \in H$;
- *Possuir também as propriedades do Grupo G.*

Definição 0.3. *Seja G um grupo, chamamos de centro, denotando por $Z(G)$, o subconjunto dos elementos de G que comutam com todos os elementos de G.* $Z(G) = \{x \in G | xg = gx, \forall g \in G\}$.

Definição 0.4. *Seja G um grupo e H um subconjunto não vazio de G. Dizemos centralizador, o subgrupo dos elementos do grupo que comutam com H.* $C_G(H) = \{g \in G | h*g = g*h, h \in H\}$.

Definição 0.5. *Se $S \leq G$, então o índice, denotado por $[G : H]$, é o número de classes laterais a direita de S em G.*

Proposição 0.6. *Se G é um grupo finito e H um subgrupo de G então, a ordem de H divide a ordem de G.(Teorema de Lagrange).*

Definição 0.7. *Sejam um Grupo G, H um subgrupo de G e $aa \in G$. Os subconjuntos de G, $aH = \{ah, h \in H\}$ e $Ha = \{ha, h \in H\}$ são chamados, respectivamente, de classe lateral a esquerda e a direita de H.*

Definição 0.8. *Seja G um grupo finito, e $|G| = p^n$, com p primo e $n \in \mathbb{Z}$, chamamos este grupo de $p - Grupo$.*

Definição 0.9. *Seja φ uma aplicação de G para F, sendo G e F grupos, com as respectivas operações + e * . Chamamos φ de Homomorfismo, se:* $\varphi(a + b) = \varphi(a) \times \varphi(b)$.

Observação 0.10. *Um aplicação como a anterior, que seja sobrejetora e injetora é dita Isomórfica.*

Parte 2 - Equação de Classes

Definição 0.11. *Seja G um grupo, $a, b \in G$. Dizemos que a é conjugado de b, denotado por $a \circ b$, se para algum $g \in G$ é possível obter $b = g^{-1}ag$.*

Proposição 0.12. *Um conjunto G, com a operação anterior é grupo.*

Demonstração 0.13. *A operação é associativa, pois: $a \circ b$ e $b \circ c$, $\exists k, l \in G | b = k^{-1}ak$ e $c = l^{-1}bl \Rightarrow c = l^{-1}k^{-1}akl = (kl)^{-1}a(lk) \Rightarrow a \circ c$.*
Existe elemento neutro, de forma que: $a = e_G^{-1}ae_G \Rightarrow a \circ a$.
Existe elemento inverso: $a \circ b \Rightarrow b = g^{-1}ag \Rightarrow a = (g^{-1})^{-1}bg{-}1$.

Definição 0.14. *Seja $a \in G$, chamamos de classe de conjugação de a em G, denotado por C_a, a classe de equivalencia em relação a a.*
Daí, $G = \dot{\cup}_{a \in G} C_a$ e $|G| = \sum_{a \in Z(G)} C_a$ Note que se $a \in Z(G)$, então $\forall g \in G, a = g^{-1}ag = g^{-1}ga = a$, de forma mais clara, $a \in Z(G) \Leftrightarrow C_a = \{a\}$. Assim, $|G| = |Z(G)| + \sum_{a \notin Z(G)} C_a$.

Proposição 0.15. *Seja G um grupo finito, $a \in G$ e $H = C_g(a)$. Então $[G : H] = |C_a|$, e por sua vez $|C_a|||G|$.*

Demonstração 0.16. *Seja φ uma aplicação de G/H em C_a dada por $\varphi(Hg) = g^{-1}ag$.*
Assim, se $Hg_1 = Hg_2$ então $g_1g_2^{-1} \in C_G(a)$ ou seja, $g_1g_2^{-1}a = ag_1g_2^{-1} \Rightarrow g_2^{-1}ag_1 = g_2^{-1}ag_1$, isso nos diz que, $\varphi(Hg_1) = \varphi(Hg_2)$, portanto φ é bem definida.
Se $\varphi(Hg_1) = \varphi(Hg_2)$ então $g_1^{-1}a_g1 = g_2^{-1}ag_2 \Rightarrow ag_1g_2^{-1} = g_1g_2^{-1}a \Rightarrow g_1g_2^{-1} \in C_g(a) = H \Rightarrow g_1 \equiv g_2 (modH)$.
φ é sobrejetiva, pois, sendo $b \in C_a, \exists g \in G$ tal que $b = g^-1ag$, ou seja $\varphi(Hg) = b$.
Assim, $|\frac{G}{H}| = |C_a|$, e mais, $|C_a|||G|$.

Proposição 0.17. *Seja G um p-grupo finito e $|G| > 1$, então $Z(G)$ também é um p-grupo e $|Z(G)| > 1$.*

Demonstração 0.18. *Por hipótese, temos que $|G| = p^n > 1$, e que $Z(G) \leq G$. Do Teorema de Lagrange, $Z(G)||p^n$, logo $\exists m \in Z_+, 0 \leq m \leq n$ tal que $|Z(G)| = p^m$.*
Para cada $a \notin Z(G)$ temos $|C_a||p^m$, da equação de classes. Daí temos que $\sum_{a \notin Z(G)} |C_a|$ é multiplo de p. Como $p^n = |G| = |Z(G)| + \sum_{a \notin Z(G)} |C_a|$. Temos então $p||Z(G)| \Rightarrow p|p^m \Rightarrow m \geq 1$.

Assim,

$$|Z(G)| - p^m > 1$$

Proposição 0.19. *Seja G um p-grupo finito e $|G| = p$, então $Z(G) = G$.*

Demonstração 0.20. *Da proposição anterior a esta, temos que $|Z(G)| \neq 1$, fazendo com que $|Z(G)| = p$ ou p^2. Portanto $(G : Z(G)) = 1$, temos que G é abeliano. Se $(G : Z(G)) = p$ temos que o grupo quociente é cíclico. Se $xZ(G)$ é um gerador deste grupo, temps que $G =< xZ(G) >$ e como x comuta com todo elemento, temos que G é abeliano.*

Referências Bibliográficas

[1] A. Garcia e Y. Lequain, Elementosde Álgebra, IMPA, 2nd ed., 2003.

[2] J.J.Rotman, Advanced Modern Algebra, Prentice Hall, revised 2nd ed., 2003.

[3] N. O. Dantas,Estruturas Algébricas I, CESAD-UFS, 2009.

[4] C. Polcino Milies, , Grupos Nilpotentes: Uma Introdução, IME-USP, 2003.