Resumo (um pouco entediante) sobre Teoria de Grupos

Jonas Gomes

29 de março de 2014

Essas notas sobre teoria de grupos foram escritas como um resumo pessoal para estudo. Elas podem (e provavelmente é o caso de) conter diversos erros[1].

1 Exemplos de Grupos

O conceito de grupo surge como abstração natural de algumas propriedades observadas em diferentes estruturas matemáticas. Vamos começar o texto analisando algumas dessas estruturas.

1.1 $S(C)$: O conjunto das bijeções de C em C

Seja C um conjunto e $S(C)$ o conjunto de todas as bijeções de C sobre C. Então, para quaisquer $f, g, h \in S(C)$ temos:

$$(f \circ g)(x) \equiv f(g(x)) \in S(C)$$

[Se $(f \circ g)(a) = (f \circ g)(b)$ então, pela definição $f(g(a)) = f(g(b))$ e como f é bijetora, $g(a) = g(b)$. Como g é bijetora, $a = b$, o que mostra que $(f \circ g)$ é injetora. Se $y \in C$, então existe $zemC$ tal que $f(z) = y$ e existe $x \in C$ tal que $g(x) = z$, de forma que $(f \circ g)(x) = y$, o que mostra que $f \circ g$ também é sobrejetora]

$$f \circ (g \circ z) = (f \circ g) \circ z = f(g(z(x))) \tag{1}$$

$$Id \circ f = f \circ Id = f \tag{2}$$

$$\text{Existe } f^{-1} \text{ tal que } f \circ f^{-1} = f^{-1} \circ f = Id \tag{3}$$

1.2 Os números inteiros

Seja $\mathbb{Z}$ o conjunto dos números inteiros. Então, com a operação de soma habitual, temos as seguintes propriedades válidas para quaisquer $a, b, c \in \mathbb{Z}$

[1] Frases humorísticas não serão consideradas erros. Para outros assuntos, me avise no jrenan@gmail.com

$$a + (b + c) = (a + b) + c \tag{4}$$
$$a + 0 = 0 + a = a \tag{5}$$
$$\text{Existe } (-a) \text{ tal que } a + (-a) = (-a) + a = 0 \tag{6}$$

1.3 O Grupo Linear Geral

Seja $GL(n)$ o conjunto das matrizes nxn com entradas reais (ou complexas) e determinante diferente de zero, i.e., das matrizes invertíveis. Para quaisquer $M, N, O \in GL(n)$ temos:

$$M.(N.O) = (M.N).O \tag{7}$$
$$M.Id_n = Id_n.M = M \tag{8}$$
$$\text{Existe } (M^{-1}) \text{ tal que } M.M^{-1} = M^{-1}.M = Id_n \tag{9}$$

2 Definição e Propriedades Básicas

Como pudemos observar nos exemplos anteriores, embora os conjuntos possam divergir fortemente quanto a sua natureza, existem propriedades algébricas muito similares, que fundamentam a idéia de grupo.

Definição 2.1 (Grupo)**.** *Seja G um conjunto não vazio, $.: G \times G \to G$ uma operação binária e $e \in G$. Se para todo $a, b, c \in G$*

$$a(b.c) = (a.b).c \qquad \text{(Associatividade)}$$
$$a.e = e.a = e \qquad \text{(Elemento Neutro)}$$
$$\textit{Existe } (a^{-1}) \textit{ tal que } a.a^{-1} = a^{-1}.a = e \qquad \text{(Inverso)}$$

Então dizemos que o par ordenado $(G,.)$ é um grupo

Frequentemente iremos escrever apenas G ao invés de $(G,.)$, esperando que a operação esteja subentendida. É imediato que todos os exemplos da primeira seção são grupos. Vamos provar agora alguns fatos elementares sobre grupos:

Proposição 2.2 (Lei do Cancelamento)**.** *Se G for um grupo e $a.x = b.x$ então $a = b$. Se $x.a = x.b$, então $a = b$*

Demonstração. Se $a.x = b.x$, então necessariamente $(a.x).x^{-1} = (b.x).x^{-1}$, pela propriedade Associativa $a.(x.x^{-1}) = b.(x.x^{-1})$. Pela propriedade do inverso $a.e = b.e$, e finalmente, pela propriedade do elemento neutro $a = b$. O caso em que $x.a = x.b$ é similar. □

Embora a lei do cancelamento seja válida em todo grupo, não é verdade que todo conjunto que obedece a lei do cancelamento seja um grupo. Por exemplo,

$(\mathbb{N}, +)$ obedece a lei do cancelamento, mas não é um grupo (pois nenhum natural diferente de 0 possui inverso). No entanto, todo conjunto finito que tenha uma operação associativa em que vale a lei do cancelamento é um grupo.

Proposição 2.3. *Seja G um conjunto finito, . uma operação associativa em G tal que vale a lei do cancelamento. Então G é um grupo.*

Demonstração. Fixe $a \in G$ e considere $\phi_a \colon G \to G$ que $x \mapsto a.x$. Pela lei do cancelamento, ϕ_a deve ser injetora. Pelo princípio da casa dos pombos, ϕ também deve ser sobrejetora (e é aqui que usamos a finitude de G). Assim, existe $e_a \in G$ tal que $\phi_a(e_a) = a$. Mas então, $a.e_a = a$, ou ainda $(a.e_a).e_a = a.e_a$. Pela lei associativa, $a.(e_a.e_a) = a.e_a$, de forma que $e_a.e_a = e_a$. Como valem as leis do cancelamento, para qualquer $x \in G$: $x.e_a = (x.e_a).e_a$ e, logo $x = x.e_a$. Da mesma forma, provamos que $e_a.x = x$. Vamos abandonar a notação e_a e escrever simplesmente e doravante, uma vez que e age como elemento neutro de G.

Como ϕ_a é sobrejetora, existe um único $a^{-1} \in G$ tal que $\phi_a(a^{-1}) = e$. Mas então $a.a^{-1} = e$, ainda $(a.a^{-1}).(a.a^{-1}) = a.(a^{-1})$. Usando a propriedade associativa, $a.(a^{-1}(a.a^{-1})) = a.a^{-1}$, pela lei do cancelamento: $a^{-1}(a.a^{-1}) = a^{-1}$. Mais uma vez, pela propriedade associativa $(a^{-1}.a).a^{-1} = a^{-1}$, ou ainda $(a^{-1}.a).a^{-1} = e.a^{-1}$e novamente pela lei do cancelamento: $a^{-1}.a = e$, o que mostra que a^{-1} é elemento inverso de a. Como a foi arbitrário, todo $x \in G$ tem elemento inverso e, logo, G é grupo. □

Proposição 2.4 (Unicidade do Inverso)**.** *Seja G um grupo e $a \in G$ tal que b e c são elementos inversos de a. Então $b = c$*

Demonstração. Como $a.b = e = a.c$ o resultado segue da lei do cancelamento. □

Proposição 2.5 (Unicidade do Elemento Neutro)**.** *Seja G um grupo e $e, e' \in G$ elementos neutros. Então $e = e'$*

Demonstração. $e = e.e' = e'$ □

Vimos nas demonstrações anteriores que aplicações sucessivas da associatividade podem ser tediosas. Vamos nos poupar do trabalho provando a

Proposição 2.6 (Lei da Associatividade Generalizada)**.** *Se G for um grupo e $x_1, \ldots, x_n$ forem elementos de G, então não importa como distribuamos os parênteses, o resultado é único.*

Demonstração. Utilizaremos o Princípio da Indução Finita. Para $n = 3$, $x_1.(x_2.x_3) = (x_1.x_2).x_3$ (pela associatividade de G) e essas são as únicas formas de distribuir os parênteses. Suponha que a Lei da Associatividade Generalizada valha para $n < p$, e para $n = p$ podemos ter o parêntese antes de x_1 ou imediatamente após x_1. Aplicando a lei associativa ao primeiro caso caímos no segundo. Como o que segue depois de x_1 tem $p - 1$ fatores, utilizamos a hipótese de indução, de forma que nos resta apenas $x_1.(x_2 \ldots x_p)$.

Suponha agora que haja duas formas diferentes de distribuir esses parênteses, isso é $(x_1.....x_k)(x_{k+1}.....x_p)$ e $(x_1.....x_s)(x_{s+1}.....x_p)$. Vamos supor, sem perda da generalidade, que $k > s$. Assim $(x_1.....x_k) = (x_1 \dots x_s)(x_{s+1}.... x_k)$.

Mas então $(x_1.....x_k)(x_{k+1}.....x_p) = ((x_1 \dots x_s)(x_{s+1}.... x_k)).(x_{k+1}.....x_p)$ e usando a propriedade associativa $= (x_1 \dots x_s)((x_{s+1}.... x_k).(x_{k+1}.....x_p))$. Como $p - (s + 1) < p$, a hipótese de indução vale para o segundo fator e finalmente temos $(x_1.....x_k)(x_{k+1}.....x_p) = (x_1.....x_s)(x_{s+1}.....x_p)$. □

Tendo nos livrado da necessidade de usar parênteses, continuamos aliviados o texto. Contribuindo de sobremaneira com nosso alívio, utilizaremos frequentemente ab ao invés de $a.b$ e no que se segue, exceto quando dito explicitamente o contrário, G será um grupo. Existe um último fato básico sobre grupos que gostaríamos de expor antes de prosseguir por essas notas:

Proposição 2.7. *O inverso do inverso de um elemento é o próprio elemento (ou, em linguagem menos enigmática:* $(a^{-1})^{-1} = a$*)*

Demonstração. $a.a^{-1} = e = (a^{-1})^{-1}.a^{-1}$ e o resultado segue da lei do cancelamento □

Podemos não ter sido completamente sinceros anteriormente: existe um outro fato básico sobre grupos, a saber:

Proposição 2.8. $(x_1.....x_n)^{-1} = {x_n}^{-1}.....{x_1}^{-1}$

Demonstração. Vamos fazer por indução. Para $n = 1$ é óbvio. Suponha que vale para $n < p$, para $n = p$ temos:

$$(x_1.....x_p)^{-1} = ((x_1.....x_{p-1})x_p)^{-1}$$

Chame $b = x_1.... x_{p-1}$, e seja h o inverso de $b.x_p$, então $b.x_p.h = e$ ou ainda $x_p.h = b^{-1}$, logo $h = b^{-1}.{x_p}^{-1}$. Ora, como em b temos $p - 1$ fatores vale nossa hipótese de indução, de forma que

$$(x_1.....x_p)^{-1} = {x_p}^{-1}.{x_{p-1}}^{-1}.....{x_1}^{-1}$$

□

Definição 2.9. *Se* $a \in G$*, então* a^n *será definido por*

$$a^n = a \text{ se } n = 1$$
$$a^n = a.a^{n-1} \text{ se } n > 1$$

Proposição 2.10. *Para todo* $n, m \in \mathbb{Z}$*:*

$$a^{(n+m)} = a^n.a^m$$
$$a^{(n.m)} = (a^n)^m$$

Demonstração. [2]Faremos por indução (dupla!). Primeiro vamos provar que vale para $m = 1$. $a^{1+n} = a.a^{1+n-1} = a^1.a^n$. Suponha agora que o resultado vale para $m < k$, para $m = k$ vamos usar outra indução. Para $n = 1$ temos $a^{1+k} = a.a^{1+k-1} = a^1.a^k$. Suponha que vale para $n < p$, para $n = p$ temos $a^{p+k} = a.a^{p+k-1}$. Pela hipótese de indução (em p) $a^{p+k} = a.a^{p-1}.a^k = a^p.a^k$ e logo vale para $n = p$. E assim, vale para $m = k$.

A segunda equação segue de forma similar. □

A sutileza de termos passado de $\mathbb{N}$ na definição 2.9 para $\mathbb{Z}$ na proposição 2.10 passa na escolha de notação para o inverso, para n natural, $a^{(-n)} = (a^{-1})^n$, onde a^{-1} aqui representa o elemento inverso. Também, é claro, $a^0 = e$.

Definição 2.11 (Grupo Abeliano)**.** *Se G satisfaz: $a.b = b.a$ para todos $a, b \in G$, então G é dito abeliano (ou comutativo).*

Dos exemplos da seção 1, apenas $\mathbb{Z}$ é abeliano.

3 Subgrupos

Definição 3.1 (Subgrupo)**.** *Se $H \subset G$ for um subconjunto de um grupo G e . restrita a $H \times H$ munir H com uma estrutura de grupo, dizemos que H é subgrupo de G e escrevemos $H < G$*

É muito importante que a imagem $.(H, H) = H$ (isto é, que H seja fechado em relação ao produto).

Existe uma caracterização básica de subgrupos que utilizaremos em todo o texto, que será a

Proposição 3.2. *$H \subset G$ é subgrupo de G se, e somente se para todo $a, b \in H$ $ab^{-1} \in H$.*

Demonstração. Se H é subgrupo, para todo $b \in H$, $b^{-1} \in H$, de forma que para todo a, $a.b^{-1} \in H$. Para a volta, observe que . restrita a H continua sendo associativa. Se $a \in H$, tomando $b = a$, vemos que $e = a.a^{-1} \in H$, de forma que o elemento neutro está em H. Ainda, tomando $a = e$, vemos que se $x \in H$ então $x^{-1} \in H$ e, logo, H é subgrupo de G. □

3.1 Exemplos de Subgrupos

1. Seja C um conjunto qualquer e $S(C)$ o conjunto de todas as suas bijeções em si mesmo. Dado $a \in C$, H definido por $H = \{f \in S(C) | f(a) = a\}$, o conjunto das bijeções que fixam a, é subgrupo de $S(C)$.

   Demonstração. Sejam $f, g \in H$, então $(f \circ g^{-1})(a) = f(g^{-1}(a)) = f(a) = a$, de forma que $f \circ g^{-1} \in H$, o que mostra que H é subgrupo □

[2]Aqui pedimos desculpas pela demonstração enfadonha! Lembre-se que essas notas foram feitas para (meu) estudo e há anos não fazia uma indução dupla :)

2. Dado $m \in \mathbb{Z}$, seja $H = \{x \in \mathbb{Z} | x = k.m\}$ o conjunto dos múltiplos de m. Então H é subgrupo:

   Demonstração. Sejam $a, b \in H$, então $a = k_a.m$ e $b = k_b.m$, de forma que $a + (-b) = k_a.m + (-k_b.m) = (k_a - k_b).m$, de forma que $a + (-b) \in H$ e H é subgrupo □

3. Seja $SL(n) = \{M \in GL(n) | \det(M) = 1\}$, então $SL(n)$ é subgrupo:

   Demonstração. Se $M, N \in SL(n)$ então $\det(M.N^{-1}) = \det(M)\det(N^{-1}) = \det(M)\frac{1}{\det(N)} = 1$ e assim $M.N^{-1} \in SL(n)$, o que prova o desejado □

3.2 Mais sobre subgrupos

Definição 3.3 (Grupo Gerado por um elemento)**.** *Se $a \in G$, chamaremos $< a >= \{a^k, k \in \mathbb{Z}\}$ o subgrupo cíclico gerado por a*

Verificar que $< a >$ é subgrupo é simples:

Demonstração. Se $x, y \in < a >$ então existem $k_1, k_2 \in \mathbb{Z}$ tais que $x = a^{k_1}$ e $y = a^{k_2}$. Note que

$$y.a^{-k_2} = a^{k_2}.a^{-k_2} = a^0 = e$$

e assim $y^{-1} \in < a >$. Além disso $x.y^{-1} = a^{k_1}.a^{-k2} = a^{k_1 - k_2} \in < a >$ □

Se G for um grupo tal que $G =< a >$ para algum a, dizemos que G é **cíclico**. Subgrupos cíclicos são especialmente interessantes, pois são abelianos. No entanto, nem todo grupo abeliano é cíclico, por exemplo, $\mathbb{R}^*$ com a multiplicação usual não é cíclico apesar de ser abeliano.

É conveniente notar que se G for finito, então também o é $< a >$, de forma que existem $n, m \in \mathbb{Z}$ e por conveniência $n > m$ tais que $a^n = a^m$ ou ainda $a^{n-m} = e$, ou seja, existe $k \in \mathbb{Z}$ tal que $a^k = e$.

Definição 3.4 (Ordem de um Elemento)**.** *Se $a \in G$, chamamos de ordem de a o menor inteiro positivo m tal que $a^m = e$*

O que dissemos anteriormente é que: em um conjunto finito a ordem de todos os seus elementos é finita.

Proposição 3.5. *Para todo $a \in G$, a ordem de a é igual $a \mid < a > \mid$*

Demonstração. Seja n a ordem de a. Então, suponha que $a^x = a^y$ para algum par $0 < x < y < n$. Mas então $a^{(y-x)} = e$, absurdo, já que $y - x < n$. Com isso concluímos que necessariamente $\{e, a^1, \ldots, a^{n-1}\} \subset < a >$. Vamos supor agora que existe algum outro $a^k \in < a >$. Escrevendo $k = n.m + r$, com $0 \leq r < n$ (Algoritmo de Euclides), vamos ter $a^p \neq a^k$, ou seja, $a^p \neq a^{n.m}.a^p$, mas $a^{n.m} = (a^n)^m = e^m = e$, assim temos que $a^p \neq a^p$, absurdo. □

Na definição anterior, chamamos $< a >$ de grupo gerado por um elemento, dando a entender que existem grupos gerados por vários elementos. O que nós gostaríamos é que o subgrupo gerado por um grupo S fosse o menor subgrupo que contivesse S, mas ele poderia, a princípio, não existir. Para provar a sua existência precisamos da próxima proposição:

Proposição 3.6. *Se $\{H_i, i \in I\}$ for uma família (não vazia) de subgrupos de G, então $\bigcap_{i\in I} H_i$ é subgrupo de G.*

Demonstração. Seja $H = \bigcap_{i\in I} H_i$ onde $H_i < G$ para todo $i \in I$. Vamos mostrar que H é subgrupo. Se a e b pertencem a H, então $a \in H_i$ e $b \in H_i$ para todo $i \in I$. Como cada H_i é subgrupo, temos que $a.b^{-1} \in H_i$ para todo H_i, mas então $a.b^{-1} \in H$, de forma que H é subgrupo. □

Feito isso, definiremos

Definição 3.7. *Se $S \subset G$, $< S >$ é o menor subgrupo (na ordem da inclusão) tal que $S \subset < S >$*

A luz da proposição 3.6 é fácil provar a existência de $< S >$, basta tomar $< S >= \bigcap\{x \subset G | x \text{ é subgrupo e } S \subset x\}$

Agora, daremos uma caracterização de $< S >$ algébrica:

Proposição 3.8. *Se $S \subset G$ então*[3] $< S >= \{x_1 \dots x_n | x_i \in S \text{ ou } (x_i)^{-1} \in S \text{ para } i \in \{1, \dots, n\}\}$

Demonstração. O conjunto da direita está contido em $< S >$, pois, se $x_1, \dots, x_n$ são tais que $x_i \in S$, então $x_i \in < S >$ e, como $< S >$ é grupo, $(x_i)^{-1} \in < S >$. Além disso, o produto de elementos de $< S >$ deve estar em $< S >$, de forma que a inclusão está garantida. Para a inclusão contrária, basta notar que o conjunto da direita é um subgrupo que contém S. □

Agora vamos abordar o conceito de coclasses (*or* cosets *if you prefer*). As coclasses surgem naturalmente do fato de que a relação $a \equiv b \Leftrightarrow a.b^{-1} \in H$ é uma relação de equivalência em G.

3.3 Coclasses e o Teorema de Lagrange

Definição 3.9 (Coclasse)**.** *Se $a \in G$ e $H < G$,*

$$Ha = \{ha | h \in H\}$$

Ha é chamada de coclasse a direita de H

Vamos relacionar a coclasse com aquela relação de equivalência citada anteriormente:

Proposição 3.10. *Dados $a, b \in G$, $Ha = Hb$ se, e somente se, $ab^{-1} \in H$*

[3] Rigorosamente, deveria haver uma união sobre n acima, mas vamos aproveitar que essas notas não são sobre teoria dos conjuntos e não carregar tanto a notação, certo?

Demonstração. Se $Ha = Hb$, então, dado $h_1 a \in Ha$ existe $h_2 b$ em Hb tal que $h_1 a = h_2 b$, de forma que $ab^{-1} = {h_1}^{-1} h_2$. Como H é subgrupo, é claro que ${h_1}^{-1} h_2 \in H$, de forma que $ab^{-1} \in H$. Para a volta, suponha que $ab^{-1} \in H$ e seja $h_1 a \in aH$, mas, tome $h_2 = h_1 ab^{-1} \in H$ e note que $h_1 a = h_2 b$, de forma que $aH \subset bH$. Para inclusão contrária, dado $bh_2 \in bH$, note que $a^{-1} b \in H$, de forma que $h_1 = a^{-1} bh_2 \in H$ e $ah_1 = bh_2$. □

Proposição 3.11. *Se $Ha \neq Hb$ então $Ha \cap Hb = \emptyset$*

Demonstração. Vamos pela contrapositiva: Suponha que $Ha \cap Hb \neq \emptyset$, então existem $h_1, h_2 \in H$ tais que $ah_1 = bh_2$, de forma que $ab^{-1} \in H$ e, pela proposição anterior $Ha = Hb$ □

Proposição 3.12. *Todas as coclasses de H tem a mesma cardinalidade*

Demonstração. Sejam aH e bH duas coclasses quaisquer de H e considere $\phi : aH \to bH$ dada por $\phi(ah) = bh$. Se $\phi(ah_1) = \phi(ah_2)$ então $bh_1 = bh_2$ de forma que $h_1 = h_2$ e $ah_1 = ah_2$, ou seja, ϕ é injetora. Para todo $bh \in bH$, $\phi(ah) = bh$, de forma que ϕ também é sobrejetora e assim, todas as coclasses de H tem a mesma cardinalidade. □

Caso o número de coclasses seja finito, nós o escrevemos como $[G : H]$ e este número é chamado de **índice de H em G**. Agora estamos preparados para provar nosso primeiro teorema!

Teorema 3.13 (de Lagrange)**.** *Se G é finito e $H < G$, então $|H|[G : H] = |G|$*

Demonstração. Dado $x \in G$ e $h \in H$, vemos que $x \in (xh^{-1})H$, de forma que todo elemento de G está em alguma coclasse de H. Como elas são disjuntas, não pode acontecer de estar em mais de uma e assim $|G|$ é igual a soma de todas as $|aH|$ não repetidas. Como todas as coclasses tem o mesmo número de elementos, que é a mesma de H (porque $H = eH$), $|G| = [G : H]|H|$. □

Com o Teorema de Lagrange em mãos já podemos colher alguns resultados de nossa teoria. Vejamos um exemplo interessante:

Corolário 3.14. *Se G é finito, para todo $a \in G$, a ordem de a divide $|G|$*

Corolário 3.15. *Se G é finito, para todo a, $a^{|G|} = e$*

Demonstração. Sabemos que a ordem de a divide $|G|$, ou seja $|G| = k.| < a > |$. Então $a^{|G|} = a^{|<a>|^k} = e^k = e$ □

Corolário 3.16. *Se $G \neq \{e\}$ só admite como subgrupos os grupos triviais (G e $\{e\}$), então G é finito de ordem prima e somente nesse caso.*

Demonstração. Vamos supor que $|G|$ só admite como subgrupos os grupos triviais. Se $a \in G$, $a \neq e$, então $< a >$ é subgrupo e logo só pode ser $\{e\}$ ou G, Assim $G =< a >$. Se G não for finito, considere $< a^2 >= G$, então $a \in< a^2 >$, de forma que $a = a^{2l}$, isso é $a^{2l-1} = e$, o que implica que a ordem de a é finita e logo $|G|$, absurdo. Suponha que $|G| = k = rt$, com $1 < r, t$. Assim, a ordem de a é rt. Considere $< a^r >$. Obrigatoriamente, $< a^r >= G$, logo $a = a^{rs}$, para $1 \leq s \leq t-1$ e assim $a^{rs-1} = e$, o que é absurdo, já que $rs - 1 < rt$. Logo k é primo.

Suponha agora que G é finito de ordem prima. Seja H um subgrupo de G. Como $|H|$ divide $|G|$, então $|H| = |G|$ e nesse caso $H = G$ ou $|H| = 1$ e nesse caso $H = \{e\}$. □

Exemplo 3.17[Inteiros relativamente primos a n] Seja $n \in \mathbb{Z}$ e seja $X = \{x \in \mathbb{Z} | x < n \text{ e } mdc(x, n) = 1\}$ e em $\mathbb{Z}$ considere a seguinte relação $a \equiv b(mod n) \Leftrightarrow a - b$ é divisível por n. Vamos mostrar que essa relação é de equivalência:

- $a \equiv a(mod n)$ já que 0 é divisível por n
- Se $a \equiv b(mod n)$ então $a - b$ é divisível por n, assim $a - b = kn$, logo $b - a = (-k)n$ e assim $b \equiv a(mod n)$
- Se $a \equiv b(mod n)$ e $b \equiv c(mod n)$ então $a - b = kn$ e $b - c = ln$, isso é, $a - c = (k - l)n$ e assim $a \equiv c(mod n)$

Dado $m \in \mathbb{Z}$ seja $[m] = \{x \in \mathbb{Z} | x \equiv m(mod n)\}$ e seja $G = \{[x] | x \in X\}$, ou seja, G é o conjunto de todas as classes de equivalência de n dos números que são relativamente primos com n.

Em G seja a operação $.: G \times G \to G$ dada por $[a].[b] = [a.b]$. Vamos mostrar que essa operação está bem definida: Se $[a].[b] = [a.b] = \{x \in \mathbb{Z} | x \equiv a.b(mod n)\}$, seja c e d tais que $[a] = [c]$ e $[b] = [d]$ ou seja $x - ab = kn$, mas como $a - c = ln$ e $b - d = sn$, temos: $x - (ln + c)(sn + d) = kn$ ou ainda $x - cd = (lsn + ld + sc)n$ e assim $[a.b] = [c.d]$, de forma que a nossa operação está bem definida.

Vamos mostrar que . é associativa:

$$[a].([b].[c]) = [a].([b.c]) = [a.b.c] = [a.b].[c] = ([a].[b]).[c]$$

Vamos mostrar que valem as leis do cancelamento: sejam $[a], [b], [x] \in G$ tais que $[a].[x] = [b].[x]$, mas então $[a.x] = [b.x]$. Como $ax \in [ax]$ isso implica que $ax \equiv bx(mod n)$, ou seja $(a - b)x$ é divisível por n. Como $mdc(n, x) = 1$, isso implica que n divide $(a - b)$. e assim $a \equiv b(mod n)$ de forma que $[a] = [b]$. A outra lei do cancelamento segue da comutatividade de $\mathbb{Z}$. Como G é finito, segue da proposição 2.3 que G é grupo.

Seja $x \in G$, então pelo corolário 3.15 a ordem de x divide $|G|$. A quantidade de números relativamente primos com n é dada por $\phi(n)$. Nessa linguagem, temos o

Corolário 3.18 (Teorema de Euler)**.** [4] *Se x é relativamente primo com n, então*

$$a^{\phi(n)} \equiv 1 (mod n)$$

Corolário 3.19 (Pequeno Teorema de Fermat)**.** *Se p é primo e a é um inteiro qualquer*

$$a^{p-1} \equiv 1 (mod p)$$

Demonstração. Basta notar que $\phi(p) = p - 1$ e que todo número inteiro é relativamente primo com qualquer outro inteiro menor que ele mesmo. □

3.4 Procriação de Subgrupos

Dados dois grupos H e K podemos, conforme provamos na proposição 3.6 trabalhar com sua intersecção e ela será novamente um subgrupo. A próxima proposição fala sobre o índice desse subgrupo:

Proposição 3.20. *Se $H < G$ e $K < G$ forem tais que $[G : H]$ e $[G : K]$ são finitos, então $[G : H \cap K] \leq [G : H][G : K]$*

Demonstração. Se $[G : H]$ e $[G : K]$ são finitos, seja R_H um subconjunto de G que contém apenas um elemento de cada coclasse de H e R_K um subconjunto de G que contém apenas um elemento de cada coclasse de K. Seja $x \in G$, vamos escrever $x = Ha$ e $x = Kb$, com $a \in R_H$ e $b \in R_K$ e seja $\phi \colon G \to R_H \times R_K$ tal que $x \mapsto (a, b)$. Se x e y são tais que $\phi(x) = \phi(y)$ então vamos provar que x e y estão na mesma coclasse de $H \cap K$:

Se $\phi(x) = \phi(y)$ então $x \in Ha$ e $y \in Ha$ e também $x \in Kb$ e $y \in Kb$, isso é, $xy^{-1} \in H$ e $xy^{-1} \in K$, de forma que $xy^{-1} \in H \cap K$ e x e y estão na mesma coclasse de $H \cap K$. Ou, dito de outra forma, se x e y estão em diferentes coclasses de $H \cap K$, $\phi(x) \neq \phi(y)$, de forma que $H \cap K$ tem no máximo $[G : H][G : K]$ coclasses distintas. □

Dados dois subgrupos H e K, nem sempre é o caso de $HK = \{hk | \ h \in H$ e $k \in K\}$ formarem um subgrupo. Se $hk \in HK$ então $k^{-1}h^{-1} \in HK$, e isso não é verdade no geral. No entanto, basta garantir que $HK = KH$ e claramente $k^{-1}h^{-1} \in HK$. Veremos que essa condição não é só suficiente como também necessária:

Proposição 3.21. *Se $H < G$ e $K < G$ então $HK < G$ se, e somente se $HK = KH$*

Demonstração. Suponha que $HK = KH$, então para se $h_1k_1 \in HK$ e $h_2k_2 \in HK$, mas como $HK = KH$, existem $k'h' \in KH$ tal que $h_2k_2 = k'h'$ e assim temos que $h_1k_1(h_2k_2)^{-1} = h_1k_1(k'h')^{-1} = h_1(k_1h'^{-1})k'^{-1}$. Mas $k_1h'^{-1} \in KH$ e logo $k_1h'^{-1} = h''k''$ e assim $h_1k_1(h_2k_2)^{-1} = (h_1h'')(k''k'^{-1}) \in HK$, de forma que HK é subgrupo.

[4] Dizer *Pelo Teorema de Euler* é uma coisa vaga em matemática, já que existem pelo menos sete teoremas completamente distintos que respondem por esse nome. Confira nesse link uma lista deles

Suponha agora que HK e seja $kh \in KH$. É claro que $h \in HK$ porque $h = h.e$ e $k \in HK$, afinal $k = e.k$. Assim também temos que h^{-1} e k^{-1} pertencem a HK. Logo $h^{-1}k^{-1} \in HK$, de forma que $(h^{-1}k^{-1})^{-1} = kh \in HK$, o que prova que $KH \subset HK$. Seja agora $hk \in HK$, usando o mesmo argumento que anteriormente, $k^{-1}h^{-1} \in HK$, de forma que existem $h'k'$ tais que $k^{-1}h^{-1} = h'k'$, ou ainda $hk = k'^{-1}h'^{-1}$, de forma que $hk \in KH$ e $HK \subset KH$, provando que $HK = KH$ □

Se H e K forem dois subgrupos finitos, então é de se esperar que HK também o seja. Se $H \cap K = \{e\}$ então teremos $|HK| = |H||K|$, mas esse nem sempre é o caso.

Proposição 3.22. *Sejam $H < G$ e $K < G$ tais que $HK < G$, então $|HK| = \frac{|H||K|}{|H \cap K|}$*

Demonstração. $HK = \bigcup_{h \in H} hK$. Quando é o caso de $h_1K = h_2K$? Quando $h_1h_2^{-1} \in K$. Para cada elemento de $h_0 \in H \cap K$, $h_1K = h_1h_0K$ e assim cada coclasse está repetida $|H \cap K|$ vezes. Assim $|HK| = \frac{|H||K|}{|H \cap K|}$ □

4 Quociente e Homomorfismos

4.1 Subgrupos Normais

Apesar de sempre ser possível lidar com as classes de equivalência da relação $ab^{-1} \in H$, para algum $H < G$, nem sempre o conjunto dessas classes de equivalência tem propriedades algébricas agradáveis, isso é, nem sempre eles podem ser transformados em grupos. O que nós gostaríamos é que, naturalmente $Ha.Hb = Hab$. Mas isso nos traz a:

Proposição 4.1. *Se $H < G$, são equivalentes as seguintes afirmações*

1. *Para todo $a, b \in G$ $Ha.Hb = Hab$*
2. *Para todo $a \in G$ $aHa^{-1} \subset H$*
3. *Para todo $a \in G$ $aHa^{-1} = H$*
4. *Para todo $a \in G$ $Ha = aH$*

Demonstração. $1 \Rightarrow 2$ Tome $b = a^{-1}$ e então, para todo $h, h' \in H$ existe h'' tal que $h'aha^{-1} = h''aa^{-1}$ ou seja $aha^{-1} = h'^{-1}h''$ e assim $aHa^{-1} \subset H$

$2 \Rightarrow 3$ Dado $a \in G$, $h \in H$, $aHa^{-1} \subset H$ mas também $a^{-1}Ha \subset H$, mas então $H = a(a^{-1}Ha)a^{-1} \subset aHa^{-1}$

$3 \Rightarrow 4$ Dado $a \in G$, $h \in H$, existe h' tal que $aha^{-1} = h'$ ou $ah = h'a$, assim $aH \subset Ha$. Como $a^{-1}Ha = H$, também segue que $Ha \subset aH$, de forma que $aH = Ha$

$4 \Rightarrow 1$ $Ha.Hb = H(aH)b = H(Ha)b = HHab = Hab$ □

Definição 4.2 (Subgrupo Normal)**.** *Se H satisfaz qualquer uma das quatro propriedades equivalentes da Proposição 4.1, dizemos que H é **normal** em G e escrevemos $H \trianglelefteq G$*

Antes de prosseguirmos, no entanto, vamos provar alguns fatos básicos sobre subgrupos normais. Vimos na Proposição 3.21 que HK é subgrupo apenas no caso de $HK = KH$. Mas sempre que H ou K forem normais a situação se torna muito mais simples:

Proposição 4.3. *Se $H < G$ e $K \trianglelefteq G$ então $HK < G$.*

Demonstração. A luz da proposição 3.21 precisamos provar que $HK = KH$. Mas $KH = \bigcup_{h\in H} Kh = \bigcup_{h\in H} hK = HK$. □

No caso de H e K serem normais, então $aHK = HaK = HKa$, de forma que HK também é normal. Esse fato no entanto não merece uma proposição.

Tendo criado o ambiente apropriado para munir as classes de equivalência da estrutura de grupo, vamos definir quociente por um subgrupo normal:

Definição 4.4 (Grupo Quociente)**.** *Se G é grupo e $N \trianglelefteq G$ então $G/N = \{Na | a \in G\}$*

Segue da proposição 4.1 que G/N tem estrutura de grupo.

4.2 Homomorfismos

Agora iremos tratar dos morfismos da categoria dos grupos, que são as funções entre dois grupos que preservam a estrutura de grupos.

Definição 4.5 (Homomorfismo)**.** *Se $(G,*)$ e $(G',*')$ são dois grupos, $\phi\colon G \to G'$ é um homomorfismo se*

$$\phi(a * b) = \phi(a) *' \phi(b)$$

Quando ϕ é bijetor, dizemos que G e G' são isomorfos e escrevemos $G \cong G'$

Vamos provar alguns fatos básicos sobre homomorfismos:

Proposição 4.6. *Se $\phi\colon A \to B$ for homomorfismo então*

1. *$\phi(e_A) = e_B$*
2. *$\phi(a^{-1}) = (\phi(a))^{-1}$*
3. *ϕ é isomorfismo somente se $Ker(\phi) = \{x \in A | \phi(x) = e_B\} = \{e_A\}$*
4. *$Ker(\phi) \trianglelefteq A$*
5. *Se $H < A$, $\phi(H) < B$*
6. *Se $H \trianglelefteq B$, $\phi^{-1}(H) \trianglelefteq A$*

Demonstração. 1. $\phi(e_A) = \phi(e_A * e_A) = \phi(e_A).\phi(e_A)$ e assim $\phi(e_A) = e_B$

2. $e_B = \phi(e_A) = \phi(a * a^{-1}) = \phi(a).\phi(a^{-1})$ e assim $(\phi(a))^{-1} = \phi(a^{-1})$

3. Suponha que ϕ é isomorfismo, então ϕ é bijetora e logo $Ker(\phi) = e_A$.

4. Se $g \in A$. Para qualquer $k \in Ker(\phi)$, $\phi(gkg^{-1}) = \phi(g).\phi(k).(\phi(g))^{-1} = e_B$ e assim $gkg^{-1} \in Ker(\phi)$

5. Se $a, b \in H$ então $\phi(a), \phi(b) \in \phi(H)$ e $\phi(a).(\phi(b))^{-1} = \phi(ab^{-1}) \subset \phi(H)$ e assim $\phi(H) < B$

6. Se $a \in A$, para qualquer $x \in \phi^{-1}(H)$ tal que $\phi(x) = h \in H$, temos que $\phi(a\phi^{-1}(x)a^{-1}) = \phi(a).\phi(h)\phi(a^{-1}) = \phi(aha^{-1}) \subset \phi(H)$ e assim $a\phi^{-1}(x)a^{-1} \in \phi^{-1}(H)$ e $\phi^{-1}(H) \trianglelefteq A$

□

Agora estamos prontos para provar o

Teorema 4.7 (Primeiro Teorema do Homomorfismo)**.** *Se G e G' são grupos e ϕ um homomorfismo,*

$$G/Ker(\phi) \cong Im(\phi) \subset G'$$

Demonstração. Pela proposição 4.6 $Ker(\phi) \trianglelefteq G$ de forma que existe $G/Ker(\phi)$. Seja $\phi(aKer(\phi)) = \phi(a)$. Vamos mostrar que ϕ é isomorfismo sobre sua imagem:

[Bem-definida] Se $ab^{-1} \in Ker(\phi)$ então $\phi(aKer(\phi)) = \phi(a) = \phi(b) = \phi(bKer(\phi))$

[Injetora] Se $\phi(a) = \phi(b)$ então $\phi(ab^{-1}) = e'$ de forma que $ab^{-1} \in Ker(\phi)$ e portanto $a = b$

[Sobrejetora] Trivial, já que restringimos o contradomínio de ϕ

□

Proposição 4.8 (Segundo Teorema do Isomorfismo)**.** *Dados dois grupos H e K tais que $H \trianglelefteq G$ e $K < G$ então: $H \cap K \trianglelefteq K$ e $K/H \cap K \cong HK/H$*

Demonstração. Como $H \trianglelefteq G$, então $H \trianglelefteq HK$. Seja $\phi : K \to HK/H$ dada por $\phi(x) = xH$. Se $\phi(x) = e$ então $xH = eH$ ou seja $x \in H \cap K$. Mas ϕ é homomorfismo, logo $Ker(\phi) = H \cap K \trianglelefteq K$ Do primeiro teorema do isomorfismo, concluímos o desejado. □

Proposição 4.9 (Terceiro Teorema do Isomorfismo)**.** *Se $K < H \trianglelefteq G$ e $K \trianglelefteq G$ então $G/H \cong (G/K)/(H/K)$*

Demonstração. Seja ϕ: $G/K \to G/H$ dada por $\phi(aK) = aH$. Se $ab^{-1} \in K$ então $ab^{-1} \in H$ e assim $\phi(aH) = \phi(bH)$ (e nossa ϕ) está bem definida. Se $\phi(x) = eH$ então $x = xK$ e $x \in H$, de forma que $x \in H/K$, o que mostra que $Ker(\phi) \subset H/K$. Para a inclusão contrária, tome $x = hK$, então $\phi(hH) = eH$ de forma que $Ker(\phi) = H/K$. Assim, pelo Primeiro Teorema do Isomorfismo, temos que $G/H \cong (G/K)/(H/K)$

O isomorfismo de grupos nos permite *traduzir* um grupo em outro através da bijeção que preserva estruturas. Nos será de grande interesse daqui pra frente classificar vários grupos a menos de isomorfismos.

Proposição 4.10. *Dois grupos cíclicos finitos são isomorfos se, e somente se, possuem a mesmo número de elementos*

Demonstração. Sejam A e B dois grupos finitos cíclicos isomorfos. Então existe uma bijeção entre ambos, de forma que eles possuem o mesmo número de elementos. Sejam A e B dois grupos finitos cíclicos com o mesmo número de elementos. Suponha que $A =< a >$ e $B =< b >$ e considere $\phi\colon A \to B$ tal que $\phi(a^j) = b^j$. É imediato que ϕ é homomorfismo, porque $\phi(a^j a^k) = \phi(a^{j+k}) = b^{j+k} = b^j b^k = \phi(a^j)\phi(a^k)$. Vamos mostrar que ϕ é uma bijeção. Suponha que, existem $0 < j < k$ menores que a ordem de A tais que $\phi(a^j) = \phi(a^k)$, mas então $b^j = b^k$ ou ainda $b^{k-j} = e$, mas $k - j$ é menor que a ordem de A e portando é menor que a ordem de B. Absurdo, logo ϕ é injetora. Seja agora $b^j \in B$, com j menor que a ordem de B. Então $\phi(a^j) = b^j$, já que j também é menor que a ordem de A. □

Corolário 4.11. *Se G é finito e cíclico então $G \cong \mathbb{Z}_{|G|}$*

Proposição 4.12. *Se G é um grupo abeliano de ordem p^2, com p primo, então $G \cong \mathbb{Z}_{p^2}$ ou $G \cong \mathbb{Z} \times \mathbb{Z}$*

Demonstração. Se G é abeliano e cíclico a conclusão segue do Corolário 4.11. Suponha agora que G não é cíclico. Seja $a \in G$ e $a \neq e$. Então $| < a > | = p$, pelo teorema **??**, já que $p^2 > | < a > | > 1$ e $| < a > |$ divide p^2. Seja agora $b \in G \setminus < a >$. Então é claro que $| < b > | = p$. Suponha que $x \in < a > \cap < b >$, ou seja $x = a^j = b^k$ e suponha que j ou k é maior que 1. Suponha, sem perda de generalidade, que $j > 1$ de forma que $x = a^j$. Mas $| < x > | = p$, de forma que a ordem de a^j é p, absurdo, já que $j > 1$. Logo não podemos ter nem j nem k maior que 1 e as opções que temos são $x = b$, de forma que teríamos $b \in < a >$, absurdo. Se $x = a$, teríamos $a = b$ ou $a = e$, absurdo. A única possibilidade então é $x = e$. Como G é abeliano, $< a >< b >=< b >< a >$, de forma que $< a >< b >$ é subgrupo e além disso $| < a >< b > | = \frac{|<a>||<b>|}{|<a>\cap<b>|}$. Como $< a > \cap < b >= \{e\}$, temos que $| < a >< b > | = p^2$ de forma que $< a >< b >= G$, ou seja, qualquer $x \in G$ pode ser escrito como $x = a^j b^k$ para $0 \leq k \leq p$ e $0 \leq k \leq k$. Provado isso, seja $\phi\colon G \to \mathbb{Z}\times\mathbb{Z}$ dada por $\phi(a^j b^k) = (j, k)$. Como G é abeliano, segue que ϕ é homomorfismo, manipulando os expoentes. Para mostrar que é isomorfismo, basta notar que, se $\phi(a^j b^k) = \phi(a^{j_2} b^{k_2})$ então $j = j_2$ e $k = k_2$. Sendo ambos os conjuntos finitos, ϕ também é sobrejetora. □

5 O Grupo de Simetrias e Ações de Grupos

As ações de grupo vão representar a forma como os grupos agem em determinados conjuntos mudando seus elementos de lugar. Da mesma forma como uma permutação o faz. Nosso primeiro exemplo de grupo foi o das bijeções de C em C, que nós chamamos de $S(C)$. Vamos trabalhar com alguns conceitos de conjugação que vão preparar o terreno para a definição de grupos simétricos.

5.1 Conjugados

Se a e b são dois elementos de G tais que $a = gbg^{-1}$ para algum $g \in G$, então dizemos que a e b são conjugados. Tal relação é uma relação de equivalência

Demonstração. É claro que $a = gag^{-1}$, se $a = gbg^{-1}$ então $b = g^{-1}a(g^{-1})^{-1}$. Se $a = gbg^{-1}$ e $b = hch^{-1}$ então $a = (gh)c(gh)^{-1}$. □

Definição 5.1 (Conjugação)**.** *Seja G um grupo e $a \in G$, chamamos de classe de conjugação de a o conjunto*

$$a^G = \{x \in G \mid x = gag^{-1} \text{ para algum } g \in G\}$$

Da nossa demonstração anterior, as classe de conjugação são disjuntas, pois são as partições de G segundo a relação de equivalência definida anteriormente.

Definição 5.2 (Centro)**.** *O centro de um grupo G é definido como os elementos de G que comutam com todos os outros, isto é*

$$Z(G) = \{a \in G \mid ab = ba \text{ para todo } b \in G\}$$

Definição 5.3 (Centralizador)**.** *Se $a \in G$, o centralizador de a é o conjunto de todos os x que comutam com a ou*

$$C_G(a) = \{x \mid ax = xa\}$$

Agora vem nosso primeiro teorema, que motivará uma generalização posteriormente.

Teorema 5.4. *Se G for finito então o número de elementos na classe de conjugação de qualquer elemento é um divisor de G, além disso $|a^G| = [G : C_G(a)]$*

Demonstração. Para cada elemento da classe de conjugação, vamos relacionar um representante das coclasses de $C_G(a)$. Primeiro vamos mostar que $C_G(a)$ é um subgrupo: se $x, y \in C_G(a)$ então $xya = xay = axy$, de forma que $xy \in C_G(a)$. Além disso, se $ax = xa$ então $x^{-1}a = ax^{-1}$, de forma que $x^{-1} \in C_G(a)$. Seja $\{x_1, \ldots, x_n\}$ representantes das coclasses (a direita) de $C_G(a)$.

Seja $\phi \colon a^G \to \{x_1, \ldots, x_n\}$ dada por $\phi(hah^{-1}) = x_h$, sendo que $h^{-1}x_h \in C_G(a)$. Primeiros vamos mostrar que ϕ está bem definida: se $hah^{-1} = gag^{-1}$ então $g^{-1}hah^{-1}g = a$, ou seja $g^{-1}h \in C_G(a)$, de forma que se $h^{-1}x_j \in C_G(a)$ então $g^{-1}x_j \in C_G(a)$ e portanto $\phi(gag^{-1}) = \phi(hah^{-1})$.

Vamos mostrar que ϕ é injetora: Se $\phi(gag^{-1}) = \phi(hah^{-1})$ então $g^{-1}x_j \in C_G(a)$ e $h^{-1}x_j \in C_G(a)$, de forma que $g^{-1}x_j(h^{-1}x_j)^{-1} = g^{-1}h \in C_G(a)$ e assim $g^{-1}ha = ag^{-1}h$ ou seja $hah^{-1} = gag^{-1}$.

Vamos provar que ϕ é sobrejetora, $\phi(x_j a x_j^{-1}) = x_j$, já que $e \in C_G(a)$

Dessa forma ϕ é bijetora e como $[G : C_G(a)]$ é o numero de representantes distintos das coclasses: $|a^G| = [G : C_G(a)]$. Pelo Teorema de Lagrange, sabemos que $|a^G|$ divide $|G|$. □

Vamos trabalhar agora com a conjugação em relação a subgrupos agora

5.2 Ações de Grupos

Definição 5.5 (Ação de Grupo)**.** *Seja G um grupo e X um conjunto. Uma função ϕ será chamada de ação (à direita) de G em X se $\phi\colon G \times X \to X$*

$$\phi(g, hx) = \phi(gh, x) \tag{10}$$

□