Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Extensões de Grupos

por

Caio Antony Gomes de Matos Andrade

sob orientação de

Prof. Dr. Antônio Pereira Brandão Júnior

Campina Grande - PB
agosto, 2018

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Caio Antony Gomes de Matos Andrade

Extensões de Grupos

Trabalho apresentado ao Curso de Graduação em Matemática da Universidade Federal de Campina Grande como requisito para a obtenção do título de Bacharel em matemática.

Orientador: Prof. Dr. Antônio Perreira Brandão Júnior

Campina Grande - PB, agosto de 2018
Curso de Matemática, modalidade Bacharelado

Dedicatória

Dedico esse trabalho a todos que me apoiaram durante minha trajetória pela matemática. Nada poderia ser conquistado sem o apoio de vocês. Dedico também ao eterno professor Bráulio Maia Junior, que certamente gostaria de ler esse trabalho, se ainda estivesse entre nós.

Agradecimentos

Minha trajetória foi marcada por várias pessoas que, com pequenos ou grandes gestos, fizeram uma diferença enorme na minha vida. Eu não seria ninguém sem o apoio de cada um deles.

Agradeço aos meus pais, José Maria e Daniela, meus irmãos Victor e Luluca, e à Mãe Lu, que sempre me apoiaram em todos os aspectos, desde que me entendo por gente. Aos meus professores de ensino fundamental em médio, em particular os de matemática Antônio e Edilma, que fizeram com que eu me apaixonasse por essa linda ciência. Às amigas Angel e Renata e meu irmão Victor, por terem apoiado minha escolha pelo curso de matemática como ninguém. Aos amigos Rhyon, Angélica, Rafaela, Amanda, Danilo e as ex-vizinhas Kadma e Brenda, por terem feito da minha estadia em Campina divertidíssima, aos amigos Neto, Epitácio, Gabriel, Luiza, Bernardo(s), Ítalo, Frost, Moana, Marina, Isabela e mais tantos, que sempre me aguardaram em João Pessoa, para ótimas farras, e aos amigos distantes, Danniel, Brenno e Lucas, cuja amizade faz a distância parecer mínima. Ao apoio emocional e amizade de Renata, Rafaela, Lilian, Angel, que me estendiam uma mão e me faziam sorrir sempre que eu precisava. Ao meu amigo e psicólogo, Luís Amaral, cujo apoio foi imprescindível em algumas das épocas mais difíceis da minha vida.

Agradeço também aos colegas do PET-MATEMÁTICA-UFCG, e ao tutor Daniel, pelos três anos e meio de muito crescimento e muitas conquistas. Ao lendário Ismael, por tantos anos de contribuições, estudos, trabalhos, artigos, pesquisas e pizzas. Aos amigos Felipe e Thiago, por terem me iniciado no mundo da álgebra e me carregado pra boas farras. Ao meu orientador, professor Brandão, por três anos de estudo, seis projetos de iniciação científica, duas disciplinas, muita aprendizagem, alegria e álgebra. Ao professor Marcelo, pelo ano e meio de estudo de análise e toda a ajuda para que eu pudesse assistir às disciplinas do mestrado. Aos companheiros de mestrado e às Baianas, que me acolheram tão bem durante essa aventura. Aos demais professores e funcionários da UAMAT, por toda a contribuição que fizeram para minha caminhada.

Agradeço ao Naruto, Deku, Hinata, Souma, e tantos outros personagens que, ao sofrerem pra vencer seus problemas, me davam forças pra que eu vencesse os meus. Ao meu time de Pokémon que me ajudou a subir ao 17º lugar no ranking da Smogon. Ao Link, Robin, Ike, Greninja, Ness, Wario, Samus e Donkey Kong, por me ajudarem a derrotar Victor e Bernardo em tantas jogatinas. Ao eterno Tritão e meus companheiros em Azeroth.

Agradeço finalmente à Matemática, por ser tão linda e apaixonante.

Obrigado!

Resumo

Sendo K e Q grupos, uma extensão de K por Q é um grupo G que possui um subgrupo normal isomorfo a K que faz quociente isomorfo a Q. Nesse trabalho, começaremos estudando os casos mais simples de extensões de grupos, os produtos semidiretos. Depois, caracterizaremos todas as extensões de K por Q em dois casos diferentes: o caso K abeliano e o caso em que K tem centro trivial. Para o estudo do primeiro caso, construiremos o segundo grupo de cohomologia, com o qual podemos construir a tábua de operação de toda extensão em que K é abeliano. Para o segundo caso, estudaremos o produto fibrado, e mostraremos que toda extensão em que K tem núcleo trivial é isomorfa a um produto fibrado. Finalmente, construiremos o produto entrelaçado, para mostrar que toda extensão de D por Q, em que D é finito, está imersa no produto entrelaçado $D \wr_r Q$.

Abstract

If K and Q are groups, an extension of K by Q is a group G having a normal subgroup isomorphic to K which makes quotient Q. In this paper, we will begin studying the simplest cases of group extensions, the semidirect products. Then, we will characterize every extension of K by Q in two cases: the case in which K is abelian, and the case in which K has trivial center. To study the first case, we will construct the second cohomology group, with which we will construct the operation table of every extension in which K is abelian. For the second case, we will study the fiber product, and we will show that every extension that K has trivial center is isomorphic to a fiber product. Lastly, we will construct the wreath product, to show that every extension of D by Q, in which D is finite, is immersed in the wreath product $D \wr_r Q$.

Sumário

Introdução

Um grupo é um conjunto G munido de uma operação binária $* : G \times G \longrightarrow G$ com hipóteses suficientes para que uma equação linear $a * x = b$ tenha uma única solução $x \in G$, independentemente de quais são $a, b \in G$. Para descobrir quais são essas hipóteses, vamos resolver passo a passo a equação $2 + x = 7$. Temos:

$$2 + x = 7$$

$$-2 + (2 + x) = -2 + 7$$

$$(-2 + 2) + x = 5$$

$$0 + x = 5$$

$$x = 5.$$

Usamos acima a associatividade, a existência de elemento neutro 0, a existência do inverso para o 2. Assim, definimos grupo como um conjunto munido de uma operação que é associativa, possui elemento neutro e todo elemento possui um inverso.

Alguns conceitos e técnicas da teoria de grupos aparecem na literatura do século XIX, no estudo das equações algébricas, na teoria dos números e na geometria. Os matemáticos Walter Von Dyck (1856-1934) e Heinrich Weber (1849-1913), em 1882, combinaram essas três raízes históricas para definir o que hoje conhecemos como grupo.

É fácil conseguir exemplos cotidianos de grupos, como o conjunto dos números inteiros munido de sua soma usual, o conjunto dos números reais (sem o zero) munido de sua multiplicação usual, o conjunto das matrizes quadradas (de tamanho fixo, com entradas reais) de determinante diferente de zero munido de sua multiplicação usual, entre inúmeros outros. Ainda assim, surge uma pergunta: como construir grupos?

Uma extensão de um grupo K por um grupo Q é um terceiro grupo G, o qual possui um subgrupo normal K_1 que é isomorfo a K e tal que o quociente $\frac{G}{K_1}$ é isomorfo a Q. À luz do teorema da correspondência, isso quer dizer que G é "metade" K e "metade" Q. É natural se fazer a pergunta: podemos conhecer todas as extensões de K por Q? Tal problema é conhecido como **problema das extensões** e tem duas possíveis vertentes:

i) Construir a tábua de operação de qualquer extensão de K por Q;

ii) Descobrir quantas extensões não isomorfas de K por Q existem.

A teoria clássica de extensões de grupos foi desenvolvida por Otto Hölder (1856-1937) e Otto Schreier (1901-1929). Em 1926, Schreier solucionou a primeira questão. Apesar disso, a solução de Schreier não responde precisamente a segunda questão, e apenas fornece uma cota superior para o número de extensões não isomorfas.

Inicialmente, estudaremos alguns conceitos preliminares para o entendimento das técnicas a serem utilizadas. Entre eles, estudaremos grupos, subgrupos, subgrupos normais, grupos quociente, homomorfismos de grupo, grupos de automorfismos e ações de grupos, dentre outros conceitos que forem relevantes.

O estudo de extensões de grupo iniciará com o produto semidireto, o qual veremos que é o caso mais simples de extensões de grupos. Mostraremos então que nem toda extensão de grupo é um produto semidireto, gerando assim a necessidade de um estudo mais aprofundado. Faremos tal estudo do problema das extensões para os casos em que K é abeliano e em que K tem centro trivial. O primeiro caso é devido a O. Schreier, e sua solução usa o segundo grupo de cohomologia para construir a tábua de operação de toda extensão de K por Q, em que K é abeliano. O segundo caso usa a construção do produto fibrado pra mostrar que toda extensão de K por Q, em que K tem centro trivial, é isomorfa a um produto fibrado. Finalizaremos nosso trabalho construindo o produto entrelaçado, que é um caso especial de produto semidireto, e mostraremos que toda extensão de D por Q está imersa no produto entrelaçado $D \wr_r Q$ no caso em que Q é finito, teorema esse atribuído a Kaloujnine e Krasner.

Um estudo mais geral de extensões de grupos pode ser feito, mas se faz necessário um conhecimento maior de cohomologia, o que foge do escopo do trabalho. Recomendamos [4], [5] para quem desejar fazer esse estudo.

Capítulo 1

Resultados preliminares

Faremos um estudo introdutório sobre grupos, onde cobriremos os conceitos e resultados necessários para o entendimento deste trabalho. Para um estudo introdutório mais detalhado sobre grupos, bem como as demonstrações dos resultados básicos apresentados nesse capítulo, recomendamos as referências [1] [2], [3], [8].

1.1 Grupos e subgrupos

1.1.1 Grupos

Definição 1.1. Sejam G um conjunto e $* : G \times G \longrightarrow G$ uma operação binária. Dizemos que o par $(G, *)$ é um grupo se são satisfeitas:

i) A associatividade da operação $*$, isto é, $x * (y * z) = (x * y) * z$, para quaisquer $x, y, z \in G$;

ii) Existe elemento neutro e para $*$, ou seja, existe $e \in G$ tal que $x * e = e * x = x$, para todo $x \in G$;

iii) Para todo $x \in G$, existe um inverso (ou simétrico) $y \in G$, ou seja, $x * y = y * x = e$.

Caso ainda seja satisfeita:

iv) Comutatividade de $*$, isto é, $x * y = y * x$, para todo $x, y \in G$; dizemos que G é um **grupo abeliano**.

Mostra-se que o elemento neutro de um grupo é único, e se $x \in G$, o inverso de x também é único.

Definição 1.2. Se G é um grupo com uma quantidade finita n de elementos, dizemos que G tem **ordem** n, e denotamos por $|G| = n$. Caso G seja infinito, dizemos que G tem **ordem infinita**, e denotamos $|G| = \infty$.

Usaremos as seguintes notações no decorrer do texto:

(I) **Notação aditiva:** usando essa notação, a operação $*$ é denotada por $+$, e elemento neutro é denotado por 0 e o inverso de x é denotado por $-x$. Tal notação é normalmente usada para grupos abelianos, mas nesse texto, a usaremos para alguns grupos não abelianos.

(II) **Notação multiplicativa:** em tal notação, a operação $*$ é denotada pela justaposição de termos (isto é, $x*y := xy$), o elemento neutro é denotado por 1 ou e, e o inverso de x é denotado por x^{-1}.

Observação 1.1. *Sendo G um grupo, valem as seguintes propriedades:*

(i) Lei do corte, isto é, se $a, x, y \in G$ são tais que $xa = ya$, então $x = y$, ou ainda, se $ax = ay$, então $x = y$.

(ii) Sendo $x, y \in G$, temos $(xy)^{-1} = y^{-1}x^{-1}$. Isto é facilmente generalizado para mostrar que se $x_1, x_2, ..., x_n \in G$, então $(x_1x_2...x_n)^{-1} = x_n^{-1}x_{n-1}^{-1}...x_1^{-1}$.

Exemplo 1.1. *O conjunto unitário $\{e\}$ é um grupo, munido da única operação binária que pode ser definida nele. Denotaremos os grupos $\{1\}$ e $\{0\}$ por 1 e 0, respectivamente.*

Exemplo 1.2. *Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são grupos munidos da operação de adição usual, mas não são grupos munidos da multiplicação usual, pois 0 não possui inverso multiplicativo. Os conjuntos $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, que são respectivamente os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ sem o zero, são grupos munidos da multiplicação usual. Todos os grupos citados nesse exemplo têm ordem infinita.*

Exemplo 1.3. *Seja $G = \{e, a, b, c\}$ munido da operação:*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

O par $(G, *)$ é um grupo, chamado ***grupo de Klein****.*

Exemplo 1.4. *Sendo X um conjunto não vazio, defina S_X como o conjunto de todas as funções $f : X \longrightarrow X$ bijetoras. Tal conjunto, munido da operação de composição, é um grupo, chamado* ***grupo das permutações de*** *X. Em tal grupo, o elemento neutro é a aplicação Id_X, tal que $Id_X(x) = x$, para todo $x \in X$. Caso $X = \{1, 2, ..., n\}$, denotamos S_X por S_n. Os grupos S_n, para $3 \leq n$, são não abelianos. Mostra-se que $|S_n| = n!$.*

Exemplo 1.5. *Sendo G_1, G_2 grupos, o conjunto $G_1 \times G_2$ munido da operação $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$, para todo $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$ é um*

grupo, chamado ***produto direto (externo)*** *de G_1 e G_2. Se $|G_1| = n$ e $|G_2| = m$, então $|G_1 \times G_2| = mn$.*

O produto direto pode ser facilmente generalizado para n grupos. Sendo $G_1, G_2, ..., G_n$ grupos, o conjunto $G_1 \times G_2 \times ... \times G_n$, munido da operação $(x_1, x_2, ..., x_n)(y_1, y_2, ..., y_n) = (x_1y_1, x_2y_2, ..., x_ny_n)$ é um grupo, chamado produto direto externo de G_1, ..., G_n.

Definição 1.3. Tomando $a, x \in G$, onde G é um grupo, definimos o **conjugado de a por x**, denotado por a^x, como sendo o elemento $xax^{-1} \in G$.

Observação 1.2. *Muitos textos definem $a^x = x^{-1}ax$, mas observaremos em capítulos futuros que, para o nosso estudo, é mais prático definirmos assim. Acreditamos que tal opção não apresenta nenhuma contra-indicação.*

Definição 1.4. Sendo G um grupo, $x \in G$ e $n \in \mathbb{Z}$, definimos

$$x^n = \begin{cases} e & , \text{se } n = 0. \\ \underbrace{xx...x}_{n \text{ vezes}} & , \text{se } n > 0. \\ (x^{-1})^{|n|} & , \text{se } n < 0. \end{cases}$$

E em notação aditiva:

$$nx = \begin{cases} 0 & , \text{se } n = 0. \\ \underbrace{x + x + ... + x}_{n \text{ vezes}} & , \text{se } n > 0. \\ |n|(-x) & , \text{se } n < 0. \end{cases}$$

Observação 1.3. *Sendo G um grupo, $x \in G$ e $n, m \in \mathbb{Z}$, algumas propriedades que decorrem da definição acima são:*

(i) $(x^n)^m = x^{nm}$;

(ii) $(x^{n+m}) = x^n x^m$;

(iii) $(x^{-1})^n = (x^n)^{-1} = x^{-n}$.

1.1.2 Subgrupos

Definição 1.5. Seja G um grupo. Um subconjunto $H \subseteq G$ não vazio é dito um **subgrupo** de G, e denotado por $H \leq G$, se valem:

(i) $xy \in H$;

(ii) $x^{-1} \in H$;

para todo $x, y \in H$.

Observação 1.4. *Podemos definir um subgrupo de G como um subconjunto $H \subset G$ não vazio tal que vale*

(i') $xy^{-1} \in H$, para todo $x, y \in H$.

Tal definição é equivalente à dada anteriormente.

Um subgrupo é, efetivamente, um subconjunto H de G que é um grupo com a operação de G restrita a H.

Exemplo 1.6. *Sendo G um grupo, os conjuntos $\{e\}$ e G são subgrupos de G, chamados subgrupos triviais.*

Exemplo 1.7. *Se G é um grupo e $x \in G$, então o conjunto $\langle x \rangle = \{x^n, n \in \mathbb{Z}\}$ (em notação aditiva, $\langle x \rangle = \{nx; n \in \mathbb{Z}\}$) é um subgrupo, chamado **subgrupo gerado por** x. Dizemos que um grupo G é **cíclico** se existe $x \in G$ tal que $G = \langle x \rangle$.*

Definição 1.6. Sejam G um grupo e $x \in G$. Se existe $n \in \mathbb{N}$ tal que $x^n = e$, dizemos que x tem **ordem finita**, e definimos a **ordem de** x, denotada por $\circ(x)$, como

$$\circ(x) = \min\{n \in \mathbb{N}; x^n = e\}.$$

Caso não exista $n \in \mathbb{N}$ tal que $x^n = e$, dizemos que x tem **ordem infinta**, e denotamos $\circ(x) = \infty$.

Proposição 1.1. *Sendo G um grupo e $x \in G$ um elemento de ordem finita e $m \in \mathbb{Z}$, temos:*

(i) $|\langle x \rangle| = \circ(x)$;

(ii) $x^m = e$ se, e somente se, $\circ(x)$ divide m.

Demonstração. (ii) Sejam $\circ(x) = n$ e $m \in \mathbb{Z}$. Pelo Algoritmo da Divisão de Euclides, existem $q, r \in \mathbb{Z}$, com $0 \leq r < n$ tais que $m = qn + r$. Assim, temos

$$x^m = x^{qn+r} = x^{qn}x^r = x^r,$$

de onde $x^m = e$ se, e somente se, $x^r = e$. Como $r < n$, pela definição de $\circ(x)$, vale $x^r = e$ se, e somente se, $r = 0$, ou seja, $m = qn$. Concluímos então que $x^m = e$ se, e somente se, $\circ(x) = n$ divide m. □

Exemplo 1.8. *Considere o grupo $\mathbb{Z}$ (o grupo aditivo dos inteiros). Fixado $n \in \mathbb{Z}$, o subgrupo $\langle n \rangle$ de $\mathbb{Z}$ é o conjunto dos múltiplos de n em $\mathbb{Z}$, que será denotado por $n\mathbb{Z}$.*

Exemplo 1.9. *Sendo $\mathbb{C}^*$ o grupo multiplicativo dos complexos, fixado $n \in \mathbb{N}$, o conjunto $C_n = \{z \in \mathbb{C}^*; z^n = 1\}$ é um subgrupo de $\mathbb{C}^*$. O subgrupo C_n é cíclico, pois sendo $z = \cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)$, temos $C_n = \langle z \rangle$.*

Exemplo 1.10. *Sendo G um grupo e $S \subseteq G$ um subconjunto, denotamos por $\langle S \rangle$ a interseção de todos os subgrupos de G que contém S. Temos que $\langle S \rangle$ é um subgrupo, chamado de* ***subgrupo gerado por*** *S. Se $G = \langle S \rangle$, dizemos que S é um conjunto gerador para G. Se existe um conjunto S finito tal que $G = \langle S \rangle$, então dizemos que G é um* ***grupo finitamente gerado****.*

Exemplo 1.11. *Dados G um grupo, $H \leq G$ e $x \in G$, o conjunto $H^x = \{xhx^{-1}, h \in H\}$ é um subgrupo, chamado* ***conjugado de*** *H* ***por*** *x.*

Exemplo 1.12. *Sendo G um grupo e H, N subgrupos de G, definimos o conjunto*

$$HN = \{hn, h \in H, n \in N\}.$$

Observe que $H \subseteq HN$ e $N \subseteq HN$. Tal conjunto não necessariamente é um subgrupo de G. Mostra-se, na verdade, que HN é subgrupo de G se, e somente se, $HN = NH$. Independentemente de HN ser subgrupo de G, temos que HN é finito se, e somente se, H e N são finitos, e vale a relação

$$|HN| = \frac{|H||N|}{|H \cap N|}.$$

Para a demonstração desse resultado, recomendamos[2], Proposição V.4.12., página 142.

Definição 1.7. Sendo G um grupo, o **centro de** G, o qual é denotado por $Z(G)$, e definido como

$$Z(G) = \{x \in G; xy = yx, \forall y \in G\}.$$

Dizemos que G tem **centro trivial** se $Z(G) = \{e\}$.

Exemplo 1.13. *Se G é um grupo, então $Z(G)$ é um subgrupo de G.*

Exemplo 1.14. *Se X é um conjunto com mais do que 2 elementos, então o grupo S_X, conforme definido no Exemplo 1.4, tem centro trivial. Com efeito, seja $f \in S_X$ uma aplicação diferente da identidade, ou seja, existe $x \in X$ tal que $f(x) = y \neq x$. Como X tem mais que dois elementos, podemos tomar um terceiro elemento $z \in X$ diferente de x e y. Definamos a aplicação:*

$$\begin{array}{rccl} g: & X & \longrightarrow & X \\ & a & \longmapsto & g(a) = \begin{cases} z & , \text{ se } a = x. \\ x & , \text{ se } a = z. \\ a & , \text{ caso contrário.} \end{cases} \end{array}$$

Observemos que

$$(f \circ g)(x) = f(z)$$

e

$$(g \circ f)(x) = g(y) = y$$

mas $f(z) \neq y = f(x)$*, uma vez que* f *é bijetiva e* $x \neq z$*, o que mostra que* $f \circ g \neq g \circ f$*, e assim,* $f \notin Z(S_X)$*. Concluímos que* $Z(S_X) = \{Id_X\}$*.*

Definição 1.8. Sendo H um subgrupo de G e $x \in G$, definimos **classe lateral à esquerda de** H **contendo** x como sendo o conjunto $xH = \{xh, h \in H\}$. Analogamente, definimos **classe lateral à direita de** H **contendo** x como o conjunto $Hx = \{hx, h \in H\}$.

Mostra-se que duas classes laterais à esquerda são iguais ou disjuntas, e o mesmo vale para classes laterais à direita. Temos ainda que, se H é um subgrupo de G

$$G = \bigcup_{x \in G} xH = \bigcup_{x \in G} Hx.$$

A igualdade de classes laterais à esquerda é caracterizada como

$$xH = yH \iff y^{-1}x \in H,$$

e à direita como

$$Hx = Hy \iff yx^{-1} \in H.$$

Se $xH = yH$, diremos que x e y são congruentes módulo H à esquerda, e se $Hx = Hy$, dizemos que x e y são congruentes módulo H à direita. Das relações acimas, vemos que

$$Hx = H \iff x \in H \iff xH = H,$$

pois $He = H = eH$.

Considerando $E_{G:H}$ o conjunto das distintas classes laterais à esquerda de H e $D_{G:H}$ o conjunto das distintas classes laterais à direita, a aplicação

$$\begin{array}{rccc} f: & E_{G:H} & \longrightarrow & D_{G:H} \\ & xH & \longmapsto & f(xH) = Hx^{-1} \end{array}$$

está bem definida e é uma bijeção. Assim, os conjuntos $E_{G:H}$ e $D_{G:H}$ têm a mesma cardinalidade, chamada de **índice de** H **em** G, e denotada por $|G : H|$.

Observação 1.5. *Sendo* G *um grupo e* $H \leq G$*, mostra-se que* $|xH| = |H|$*, para todo* $x \in G$*. Ademais, se* G *é finito, concluí-se que* $|G : H||H| = |G|$*.*

Imediatamente da observação anterior, temos:

Teorema 1.1. ***(Teorema de Lagrange)*** *Se* G *é um grupo finito e* H *é um subgrupo de* G*, então* $|H|$ *divide* $|G|$*.*

Corolário 1.2. *Se* G *é um grupo finito e* $g \in G$*, então* $\circ(g)$ *divide* $|G|$*.*

1.2 Subgrupos normais e grupos quocientes

Definição 1.9. Sejam G um grupo e N um subgrupo de G. Dizemos que N é um **subgrupo normal**, e denotamos $N \trianglelefteq G$, se $xN = Nx$, para todo $x \in G$.

Proposição 1.2. *Sendo $N \leq G$ um subgrupo, são equivalentes:*
(i) N é normal;
(ii) $N^x = N$, para todo $x \in G$;
(iii) $N^x \subseteq N$, para todo $x \in G$.

Demonstração. Lembrando que $N^x = xNx^{-1}$, a equivalência entre *(i)* e *(ii)* é dada por

$$xN = Nx \iff xNx^{-1} = N$$

Temos que *(ii)* implica *(iii)* trivialmente. Para mostrar que *(iii)* implica *(ii)*, basta observar que a equivalência

$$N^{x^{-1}} \subseteq N \iff N \subseteq N^x$$

fornece a inclusão contrária. □

Observação 1.6. *Se H e N são subgrupos de G, com $N \trianglelefteq G$, então*

$$HN = \bigcup_{h \in H} hN = \bigcup_{h \in H} Nh = NH$$

de onde, pelo Exemplo 1.12, temos que HN é um subgrupo de G.

Exemplo 1.15. *Sendo G um grupo arbitrário, os subgrupos $\{e\}$ e G são normais em G.*

Exemplo 1.16. *Em um grupo G abeliano, todo subgrupo N é normal. Com efeito, temos*

$$N^x = \{xnx^{-1}; n \in N\} = \{nxx^{-1}; n \in N\} = \{ne; n \in N\} = N.$$

Exemplo 1.17. *Se G é um grupo e N é um subgrupo tal que $|G : N| = 2$, então N é normal em G. Com efeito, as duas classes laterais à esquerda de N em G são N e $G - N$, e essas também são as únicas classes laterais à direita. Caso $x \in N$, temos $xN = N = Nx$. Caso $x \notin N$, temos $xN = G - N = Nx$, o que mostra a normalidade de N.*

Exemplo 1.18. *Sendo G um grupo, o centro $Z(G)$ conforme a Definição 1.7 é um subgrupo normal de G.*

Exemplo 1.19. *Dados G_1 e G_2, os subgrupos $H_1 = G_1 \times \{e_2\}$ e $H_2 = \{e_1\} \times G_2$ de $G_1 \times G_2$ são normais. Com efeito, dados $(g_1, e_2) \in H_1$ e $(x_1, x_2) \in G_1 \times G_2$, temos*

$$(x_1, x_2)(g_1, e_2)(x_1, x_2)^{-1} = (x_1 g_1 x_1^{-1}, x_2 x_2^{-1}) = (g_1', e_2)$$

onde $g_1' = x_1 g_1 x_1^{-1} \in G_1$. Isto mostra que $H_1^x \subseteq H_1$, para todo $x \in G_1 \times G_2$, e portanto $H_1 \trianglelefteq G_1 \times G_2$. A demonstração para $H_2 \trianglelefteq G_1 \times G_2$ é análoga.

Sendo G um grupo e $N \trianglelefteq G$, consideremos o conjunto $G/N = \{xN, x \in G\}$ de todas as distintas classes laterais de H em G (aqui, não fazemos distinção de lado de classe lateral por causa da normalidade de N em G), e definamos em $\dfrac{G}{N}$ a operação

$$\begin{array}{rccc} \cdot : & \dfrac{G}{N} \times \dfrac{G}{N} & \longrightarrow & \dfrac{G}{N} \\ & (xN, yN) & \longmapsto & (xN) \cdot (yN) = xyN. \end{array}$$

Tal operação é bem definida pela normalidade de N em G, e munido dela, o conjunto $\dfrac{G}{N}$ é um grupo, chamado **grupo quociente de G por N**. Observe que o elemento neutro de tal grupo é $eN = N$, e $(xN)^{-1} = x^{-1}N$. Quando não houver confusão de qual é o subgrupo normal N, denotaremos xN por $\overline{x}$.

Exemplo 1.20. *Sendo $n \in \mathbb{N}$, do fato que $\mathbb{Z}$ é abeliano concluímos que $n\mathbb{Z}$ é normal, e portanto podemos falar do quociente $\mathbb{Z}/n\mathbb{Z}$, que é comumente denotado por $\mathbb{Z}_n$. Com o auxílio do Algoritmo da Divisão de Euclides, dado $m \in \mathbb{Z}$, existem $r, q \in \mathbb{Z}$, com $0 \leq r \leq n-1$ tais que $m = nq + r$, de onde $m - r = nq \in n\mathbb{Z}$, o que mostra que $\overline{m} = \overline{r}$. Assim, temos $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, $|\mathbb{Z}_n| = n$ e*

$$\overline{x} + \overline{y} = \overline{x + y} = \overline{r},$$

onde $r \in \{0, 1, ..., n-1\}$ é o resto da divisão euclidiana de $x + y$ por n. Mostra-se que $\langle \overline{1} \rangle = \mathbb{Z}_n$.

Na próxima seção, caracterizaremos os subgrupos do grupo quociente e estudaremos o Teorema Fundamental dos Homomorfismos, que nos ajudará a compreender melhor a estrutura dos grupos quociente.

1.3 Homomorfismos

Definição 1.10. Sejam G e G_1 grupos e $\varphi : G \longrightarrow G_1$ uma função. Dizemos que φ é um **homomorfismo (de grupos)** se $\varphi(xy) = \varphi(x)\varphi(y)$, para todo

$x, y \in G$. Se $\varphi : G \longrightarrow G_1$ é bijetivo, dizemos que φ é um **isomorfismo**. Se existe um isomorfismo entre $\varphi : G \longrightarrow G_1$, dizemos que G e G_1 são isomorfos, e denotamos $G \simeq G_1$.

Sendo $\varphi : G \longrightarrow G_1$ um homomorfismo, definimos ainda:

$$Ker(\varphi) = \{x \in G; \varphi(x) = e_{G_1}\} \quad e \quad Im(\varphi) = \{\varphi(x), x \in G\},$$

denominados **núcleo** e **imagem**, respectivamente.

Exemplo 1.21. *A aplicação*

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & G_1 \\ & x & \longmapsto & \varphi(x) = e_{G_1} \end{array}$$

é um homomorfismo, chamado de ***homomorfismo trivial (ou nulo)****. Temos* $Ker(\varphi) = G$ *e* $Im(\varphi) = \{e_{G_1}\}$.

Exemplo 1.22. *Se* $\varphi : G \longrightarrow G_1$ *é um isomorfismo, então* $\varphi^{-1} : G_1 \longrightarrow G$ *é também um isomorfismo, o que mostra que a relação de isomorfismo é simétrica, isto é,*

$$G \simeq G_1 \iff G_1 \simeq G.$$

Exemplo 1.23. *Sendo* $\varphi : G \longrightarrow G_1$ *e* $\psi : G_1 \longrightarrow G_2$ *homomorfismos, então a aplicação* $(\psi \circ \varphi) : G \longrightarrow G_2$ *é também um homomorfismo, isto é, a composição de homomorfismos é também um homomorfismo. Consequentemente, a relação de isomorfismo é transitiva, ou seja, se* $G \simeq G_1$ *e* $G_1 \simeq G_2$*, então* $G \simeq G_2$.

Observação 1.7. *Se* $\varphi : G \longrightarrow G_1$ *é um homomorfismo, então:*

(i) $\varphi(e_G) = e_{G_1}$ *e* $\varphi(x^{-1}) = (\varphi(x))^{-1}$*, para todo* $x \in G$*. Mais geralmente, vale* $\varphi(x^n) = (\varphi(x))^n$*, para todo* $n \in \mathbb{Z}$ *e para todo* $x \in G$.

(ii) Se H *é um subgrupo de* G*, então* $\varphi(H)$ *é um subgrupo de* G_1*. Particularmente,* $Im(\varphi)$ *é um subgrupo de* G_1.

(iii) Se K *é um subgrupo de* G_1*, então* $\varphi^{-1}(K)$ *é um subgrupo de* G*, e* $Ker(\varphi) \subseteq \varphi^{-1}(K)$*. Ademais, se* $K \trianglelefteq G_1$*, então* $\varphi^{-1}(K) \trianglelefteq G$*. Particularmente,* $Ker(\varphi) \trianglelefteq G$.

(iv) φ *é injetiva se, e somente se,* $Ker(\varphi) = e_G$.

Exemplo 1.24. *Sejam* G *um grupo e* $g \in G$*. A função*

$$\begin{array}{rccc} \varphi_g: & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & \varphi_g(n) = g^n \end{array}$$

é um homomorfismo, pois pelo item (ii) da Observação 1.3, vale

$$\varphi_g(n+m) = g^{n+m} = g^n g^m = \varphi_g(n)\varphi_g(m)$$

para todo $n, m \in \mathbb{Z}$. Concluímos que fixados um grupo G e um elemento $g \in G$ quaisquer, existe um (único) homomorfismo $\varphi_g : \mathbb{Z} \longrightarrow G$ tal que $\varphi_g(1) = g$.

Exemplo 1.25. ***(Produto Direto Interno)*** *Sejam G um grupo, H, N subgrupos normais de G tais que $H \cap N = \{e\}$ e $HN = G$. Então, $G \simeq H \times N$, onde $H \times N$ foi definido no Exemplo 1.5. Com efeito, considere a aplicação*

$$\varphi : \ H \times N \ \longrightarrow \ G$$

tal que $\varphi(h, n) = hn$. Para mostrar que tal aplicação é um homomorfismo, observemos primeiro que $h^{-1}n^{-1}hn \in H \cap N$, pois da normalidade de N, temos $h^{-1}n^{-1}hn = (n^{-1})^{h^{-1}}n \in N$, e da normalidade de H, temos $h^{-1}n^{-1}hn = h^{-1}h^{n^{-1}} \in H$. Assim, $h^{-1}n^{-1}hn = e$, ou seja, $hn = nh$, para todo $n \in N$, $h \in H$. Sendo $(h_1, n_1), (h_2, n_2) \in H \times N$, temos

$$\varphi((h_1, n_1)(h_2, n_2)) = \varphi((h_1h_2, n_1n_2)) = h_1h_2n_1n_2 =$$

$$= h_1n_1h_2n_2 = \varphi(h_1, n_1)\varphi(h_2, n_2).$$

Ademais, tal homomorfismo é sobrejetivo pelo fato de que $HN = G$, e é injetivo pelo fato de que $Ker(\varphi) = \{(x, x^{-1}), x \in H \cap N\} = \{(e, e)\}$.

*Nas condições desse exemplo, dizemos que G é o **produto direto (interno)** de H por N.*

Exemplo 1.26. *Sendo G um grupo e N um subgrupo normal de G, a aplicação*

$$\begin{array}{rccc} \pi : & G & \longrightarrow & \dfrac{G}{N} \\ & x & \longmapsto & \pi(x) = \overline{x} \end{array}$$

*é um homomorfismo, chamado **projeção canônica**. Tal aplicação é sobrejetiva e $Ker(\pi) = N$.*

Teorema 1.3. ***(Teorema da Correspondência)*** *Se G é um grupo e $N \trianglelefteq G$, então existe uma correspondência biunívoca entre os subgrupos de G que contêm N e os subgrupos de $\dfrac{G}{N}$.*

Demonstração. Considere a aplicação projeção canônica $\pi : G \longrightarrow \dfrac{G}{N}$ definida no Exemplo 1.26. Sendo X o conjunto dos subgrupos de G que contém N e Y o conjunto dos subgrupos de $\dfrac{G}{N}$, defina a aplicação

$$\begin{array}{rccc} f : & X & \longrightarrow & Y \\ & H & \longmapsto & f(H) = \pi(H) = \{hN; h \in H\} = \dfrac{H}{N}. \end{array}$$

Tal aplicação é bem definida, pois $\pi(H) = \{hN, h \in H\} = \dfrac{H}{N}$ é um subgrupo de $\dfrac{G}{N}$ pela propriedade *(ii)* da Observação 1.7.

Para a injetividade, se H, H_1 são subgrupos de G, ambos contendo N, tais que $\pi(H) = \pi(H_1)$, então dado $x \in H$, existe $x_1 \in H_1$ tal que $\overline{x} = \pi(x) = \pi(x_1) = \overline{x_1}$, e então $xx_1^{-1} \in Ker(\pi) = N \subseteq H_1$. Logo, $x = (xx_1^{-1})x_1 \in H_1$, e assim $H \subseteq H_1$. Analogamente, mostra-se que $H_1 \subseteq H$ e portanto $H = H_1$, o que mostra que a aplicação é injetiva.

Quanto à sobrejetividade, seja $K \in Y$. Então, pelo item *(iii)* da Observação 1.7, temos que $\pi^{-1}(K)$ é um subgrupo de G tal que $Ker(\pi) = N \subseteq \pi^{-1}(K)$. Pela sobrejetividade da aplicação π, temos que $\pi(\pi^{-1}(K)) = K$. □

Observação 1.8. *Na linguagem do teorema anterior, sendo $H, H_1 \in X$ ainda valem:*

$$H \leq H_1 \iff \frac{H}{N} \leq \frac{H_1}{N};$$

$$H \trianglelefteq G \iff \frac{H}{N} \trianglelefteq \frac{G}{N}.$$

Sejam G e G_1 grupos, $\varphi : G \longrightarrow G_1$ um homomorfismo e $K = Ker(\varphi)$. Sendo $x, y \in G$, temos:

$$\varphi(x) = \varphi(y) \iff \varphi(xy^{-1}) = e_{G_1} \iff xy^{-1} \in K \iff xK = yK.$$

Isso mostra que todos os elementos de uma classe lateral $xKer(\pi)$ têm necessariamente a mesma imagem por π. Com isso, enunciamos:

Teorema 1.4. ***(Teorema Fundamental dos Homomorfismos)*** *Se G e G_1 são grupos e $\varphi : G \longrightarrow G_1$ é um homomorfismo, então $\dfrac{G}{Ker(\varphi)} \simeq Im(\varphi)$.*

Demonstração. Considere $K = Ker(\varphi)$ e a aplicação

$$\overline{\varphi} : \frac{G}{K} \longrightarrow Im(\varphi),$$

tal que $\overline{\varphi}(xK) = \varphi(x)$. A aplicação $\overline{\varphi}$ está bem definida pela discussão acima, e é um homomorfismo pelo fato de que φ é um homomorfismo, e é sobrejetivo por ter como contra-domínio $Im(\varphi)$. Ademais, denotando $xK = \overline{x}$, se $\overline{x} \in Ker(\overline{\varphi})$, então $\overline{\varphi}(\overline{x}) = e$, ou seja, $\varphi(x) = e$. Assim, $x \in K$, e portanto $\overline{x} = \overline{e}$, mostrando que a aplicação é injetiva. □

Exemplo 1.27. *Se G é um grupo, a aplicação*

$$\begin{aligned} Id : \ G &\longrightarrow G \\ x &\longmapsto Id(x) = x \end{aligned}$$

é um homomorfismo, chamado ***homomorfismo identidade****, cujos núcleo e imagem são* $Ker(Id) = \{e_G\}$ *e* $Im(Id) = G$*, respectivamente. Tal homomorfismo mostra, com o auxílio do Teorema Fundamental dos Homomorfismos, que* $\dfrac{G}{\{e\}} \simeq G$*.*

Exemplo 1.28. *Se* $G = \langle x \rangle$ *é um grupo cíclico tal que* $|G| = n$*, então* $G \simeq \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$*. De fato, a aplicação*

$$\varphi : \ \mathbb{Z} \ \longrightarrow \ G$$

tal que $\varphi(n) = x^n$ *é um homomorfismo sobrejetivo, e de núcleo* $Ker(\varphi) = n\mathbb{Z}$*, conforme a Proposição 1.1. Pelo Teorema Fundamental dos Homomorfismos, temos* $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \simeq G$*. Caso* $|G| = \infty$*, a aplicação* φ *é um isomorfismo, de onde* $G \simeq \mathbb{Z}$*.*

Observação 1.9. *Denotaremos o único (a menos de isomorfismo) grupo cíclico de* n *elementos de* $\mathbb{Z}_n$*, se estivermos usando notação aditiva, ou de* C_n*, se estivermos usando notação multiplicativa.*

Teorema 1.5. ***(Segundo Teorema dos Isomorfismos)*** *Se* G *é um grupo e* H, N *são subgrupos de* G*, com* $N \trianglelefteq G$ *e* $N \subseteq H$*, então*

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}.$$

Demonstração. Considere a aplicação

$$\begin{array}{rccc} \varphi : & H & \longrightarrow & \dfrac{HN}{N} \\ & h & \longmapsto & \varphi(h) = \overline{h}, \end{array}$$

que é um homomorfismo sobrejetivo, e $Ker(\varphi) = H \cap N$. Assim, o resultado segue do Teorema Fundamental dos Homomorfismos. □

1.4 Grupos de automorfismos

Definição 1.11. Um isomorfismo $\varphi : G \longrightarrow G$ é dito um **automorfismo do grupo** G. Definimos o **grupo de automorfismos de** G como o grupo $Aut(G) = \{\varphi : G \longrightarrow G; \varphi \text{ é automorfismo}\}$, munido da operação de composição de funções.

Observação 1.10. *Observe que* $Aut(G) \leq S_G$*. Consequentemente, o elemento neutro de* $Aut(G)$ *é a aplicação identidade* Id_G*.*

Exemplo 1.29. *Seja G um grupo abeliano (com notação aditiva). A aplicação*

$$\begin{array}{rccc} f: & G & \longrightarrow & G \\ & x & \longmapsto & f(x) = -f(x) \end{array}$$

é um automorfismo de G. Tal automorfismo será chamado de ***automorfismo inversão****.*

Exemplo 1.30. *Se $G = \{e, a, b, c\}$ é o grupo de Klein definido no Exemplo 1.3, então $Aut(G) \simeq S_3$. De fato, basta ver que todo automorfismo $\varphi : G \longrightarrow G$ deve satisfazer $\varphi(e) = e$ e, além disso, φ provoca uma permutação em $\{a, b, c\}$. Mais ainda, se $f : \{a, b, c\} \longrightarrow \{a, b, c\}$ é uma permutação, então $\varphi_f : G \longrightarrow G$ tal que $\varphi_f(e) = e$ e $\varphi_f(x) = f(x)$, se $s \neq e$, é um automorfismo.*

Exemplo 1.31. *Temos $Aut(\mathbb{Z}) = \{Id_{\mathbb{Z}}, f\}$, onde f é o automorfismo inversão. De fato, sendo $\varphi \in Aut(\mathbb{Z})$, com $\varphi(1) = a$, temos $\varphi(n) = an$. Assim, $Im(\varphi) = a\mathbb{Z}$, de onde φ é sobrejetiva se, e somente se, $\varphi(1) = \pm 1$. No caso em que $\varphi(1) = 1$, temos que φ é o automorfismo identidade, e caso $\varphi(1) = -1$, temos que φ é o automorfismo inversão.*

Exemplo 1.32. *Temos $Aut(\mathbb{Z}_2) = \{Id\}$ e $Aut(\mathbb{Z}_4) = \{Id, f\}$, onde f é o automorfismo inversão. Se $G = \mathbb{Z}_{p^n}$, onde p é um número primo ímpar e $n \in \mathbb{N}$, então $Aut(G) \simeq \mathbb{Z}_{(p-1)p^{n-1}}$. Particularmente, se $n = 1$, então $Aut(G) \simeq \mathbb{Z}_{p-1}$. A demonstração desses fatos constam em [6], nas páginas 129 e 157.*

Exemplo 1.33. ***(Automorfismos internos)*** *Sejam G um grupo e $x \in G$ fixado. A aplicação*

$$\begin{array}{rccc} \psi_x: & G & \longrightarrow & G \\ & a & \longmapsto & \psi_x(a) = a^x = xax^{-1} \end{array}$$

é um automorfismo de G, chamado ***autormorfismo interno associado a*** *x* ***(ou conjugação por*** *x****)****. O conjunto de todos os automorfismos internos, que será denotado por $Inn(G)$, é um subgrupo normal de $Aut(G)$, chamado* ***grupo dos automorfismos internos de*** *G. Definimos também o* ***grupo dos automorfismos externos de*** *G, denotado por $Out(G)$, como o grupo quociente $Out(G) = \dfrac{Aut(G)}{Inn(G)}$. Ademais, a aplicação*

$$\begin{array}{rccc} \psi: & G & \longrightarrow & Aut(G) \\ & x & \longmapsto & \psi(x) = \psi_x \end{array}$$

é um homomorfismo de imagem $Inn(G)$ e núcleo $Z(G)$ (o centro de G, conforme a Definição 1.7), o que mostra, pelo Teorema Fundamental dos Homomorfismos, que $\dfrac{G}{Z(G)} \simeq Inn(G)$.

1.5 Ações de grupo

Definição 1.12. Sejam G um grupo e X um conjunto não vazio. Definimos uma **ação de G em X (à esquerda)** como sendo uma aplicação

$$\begin{array}{rccc} \rho: & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & \rho(g,x) = g \cdot x, \end{array}$$

que satisfaz:

(i) $e \cdot x = x$, para todo $x \in X$;

(ii) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$, para quaisquer $g_1, g_2 \in G$ e $x \in X$.

Se X é um conjunto e G age sobre X, dizemos que X é um **G-conjunto**.

Observação 1.11. *Podemos definir ação de G em X à direita de forma análoga à definição acima, e podemos transformar uma ação à esquerda em uma ação à direita definindo*

$$x \cdot g = g^{-1} \cdot x$$

para todo $g \in G$ e $x \in X$.

Ações de G em X são uma outra maneira de ver homomorfismos da forma $\varphi : G \longrightarrow S_X$. De fato, seja $\varphi : G \longrightarrow S_X$

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & S_X \\ & g & \longmapsto & \varphi(g) = \varphi_g(x) \end{array}$$

um homomorfismo. A aplicação

$$\begin{array}{rccc} \rho: & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & \rho(g,x) = g \cdot x = \varphi_g \end{array}$$

é uma ação de grupo. As condições *(i)* e *(ii)* da definição 1.12 decorrem do fato de que φ é um homomorfismo.

Reciprocamente, sejam X um conjunto não vazio, G um grupo, g um elemento fixado de G e $\rho : G \times X \longrightarrow X$ uma ação de G em X. Então, a aplicação $\sigma_g : X \longrightarrow X$, definida por $\sigma_g(x) = g \cdot x$, é uma permutação em X. Com efeito, a aplicação $\sigma_{g^{-1}}$ é inversa de σ_g, visto que

$$(\sigma_g \circ \sigma_{g^{-1}})(x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e_G \cdot x = x$$

para todo $x \in X$, de onde $\sigma_g \circ \sigma_{g^{-1}} = Id_X$. Analogamente, $\sigma_{g^{-1}} \circ \sigma_g = Id_X$, e assim σ_g é uma permutação. Ademais, decorre da condição *(ii)* da Definição 1.12 que a aplicação $\sigma : G \longrightarrow S_X$

$$\begin{array}{rccc} \sigma: & G & \longrightarrow & S_X \\ & g & \longmapsto & \sigma(g) = \sigma_g \end{array}$$

é um homomorfismo, mostrando assim que um homomorfismo $\varphi : G \longrightarrow S_X$ define uma ação $\rho : G \times X \longrightarrow X$, e vice-versa.

Observação 1.12. *Sendo K e Q grupos, em muitas ocasiões durante os capítulos que seguem trabalharemos com homomorfismos do tipo*

$$\theta : \quad Q \quad \longrightarrow \quad Aut(K)$$

e uma vez que $Aut(K) \leq S_K$, tal homomorfismo define uma ação de grupo, conforme o que foi exposto acima.

Capítulo 2

Produto semidireto

Neste capítulo estudaremos os produtos semidiretos, os quais veremos futuramente que são o tipo mais simples de extensões de grupos.

Definição 2.1. Seja K um subgrupo de um grupo G. Um subgrupo $Q \leq G$ é um **complemento** de K em G se $K \cap G = \{e\}$ e $KQ = G$.

Observamos aqui que um subgrupo não precisa ter um complemento, e, se tiver, o mesmo não precisa ser único, conforme os exemplos a seguir.

Exemplo 2.1. *Em S_3, qualquer subgrupo de ordem 2 é complemento do (único) de ordem 3.*

Exemplo 2.2. *Sendo $n \in \mathbb{N}$, os subgrupos não triviais de $\mathbb{Z}_{p^n}$ não possuem complemento. Isso ocorre pelo fato de que, sendo H e K dois subgrupos de $\mathbb{Z}_{p^n}$, tem-se necessariamente $H \cap K = H$ ou $H \cap K = K$*

Observação 2.1. *Um complemento Q de um subgrupo normal $K \trianglelefteq G$ é sempre isomorfo à $\dfrac{G}{K}$, pois utilizando o Teorema 1.5, vemos que*

$$Q \simeq \frac{Q}{\{e\}} = \frac{Q_1}{K \cap Q_1} \simeq \frac{KQ_1}{K} = \frac{G}{K}.$$

Ademais, se Q_1, Q_2 são dois complementos de um subgrupo normal $K \trianglelefteq G$, então $Q_1 \simeq Q_2$.

Definição 2.2. Sejam K e Q grupos. Dizemos que um grupo G é um **produto semidireto** de K por Q, e denotamos por $G = K \rtimes Q$, se existe um subgrupo normal $K_1 \trianglelefteq G$, com $K_1 \simeq K$, e K_1 tem complemento $Q_1 \simeq Q$.

Observação 2.2. *Quando trabalhamos com produto semidireto, para a simplicidade da notação, muitas vezes denotaremos o subgrupo de G que é complemento de K também pela letra Q.*

Antes de mais exemplos, mostremos a seguinte caracterização de produtos semidiretos.

Lema 2.1. *Se K é um subgrupo normal de um grupo G, então são equivalentes:*

(i) G é um produto semidireto de K por $\dfrac{G}{K}$.

(ii) Existe um subgrupo $Q \leq G$ tal que todo elemento $g \in G$ tem uma única expressão

$$g = ax$$

com $a \in K$ e $x \in Q$.

(iii) Existe um homomorfismo

$$s : \frac{G}{K} \longrightarrow G$$

tal que $\pi \circ s = Id_{\frac{G}{K}}$, onde

$$\pi : \ G \ \longrightarrow \ \frac{G}{K}$$

é o homomorfismo projeção canônica, definido no Exemplo 1.26.

(iv) Existe um homomorfismo

$$r : \ G \ \longrightarrow \ G$$

*tal que $Ker(r) = K$ e $r(x) = x$, para todo $x \in Im(r)$ (tal homomorfismo é chamado uma **retração** de G).*

Demonstração. $(i) \implies (ii)$

Seja Q um complemento de K em G. Por definição de complemento, vale $G = KQ$, de onde, para cada $g \in G$, existem $a \in K$ e $x \in Q$ tais que $g = ax$. Supondo $a_1, a_2 \in K$ e $x_1, x_2 \in Q$ tais que $a_1x_1 = a_2x_2 = g$, temos $a_1^{-1}a_2 = x_1x_2^{-1} \in K \cap Q = \{e\}$, e assim $a_1 = a_2$ e $x_1 = x_2$, mostrando a unicidade de tal expressão.

$(ii) \implies (iii)$

Defina

$$\begin{array}{rccc} s : & \dfrac{G}{K} & \longrightarrow & G \\ & \overline{g} = \overline{ax} = \overline{x} & \longmapsto & s(\overline{g}) = x \end{array}$$

com $a \in K$ e $x \in Q$. Mostremos que s está bem definida. De fato, sejam $g_1 = a_1x_1$ e $g_2 = a_2x_2$, com $a_1, a_2 \in K$, $x_1, x_2 \in Q$, tais que $\overline{g_1} = \overline{g_2}$. Daí, $\overline{x_1} = \overline{x_2}$, e assim $x_1x_2^{-1} \in K \cap Q$. Basta mostrarmos que $K \cap Q = \{e\}$ para

concluirmos que $x_1 x_2^{-1} = e$. Dado $x \in K \cap Q$, então podemos escrever e das seguintes maneiras:

$$e = xx^{-1} \quad \text{e} \quad e = ee.$$

Como a decomposição $e = ax$, com $a \in K$ e $x \in Q$, é única, segue que $x = e$, e assim, $K \cap Q = \{e\}$. Concluímos então que $x_1 x_2^{-1} = e$, e portanto $x_1 = x_2$. Assim, s está bem definida. O fato de que s é um homomorfismo segue de $\overline{x_1 x_2} = \overline{x_1}\,\overline{x_2}$. Para mostrar $\pi \circ s = Id_{\frac{G}{K}}$, tomemos $g \in G$, $a \in K$ e $x \in Q$ tais que $g = ax$. Temos

$$(\pi \circ s)(\overline{g}) = (\pi \circ s)(\overline{ax}) = \pi(x) = \overline{x} = \overline{ax} = \overline{g}$$

o que mostra o resultado.

$(iii) \implies (iv)$
Definamos

$$\begin{array}{rccc} r: & G & \longrightarrow & G \\ & g & \longmapsto & r(g) = (s \circ \pi)(g). \end{array}$$

Sendo $g \in G$ e $x = r(g)$, temos

$$r(x) = r(r(g)) = s((\pi \circ s)(\pi(g))) = s(\pi(g)) = r(g) = x$$

o que mostra que $r(x) = x$, para todo $x \in Im(r)$. Ainda, sendo $a \in K$,

$$r(a) = s(\pi(a)) = s(\overline{a}) = s(\overline{e}) = e$$

e, portanto, $K \subseteq Ker(r)$. Agora, sendo $g \in Ker(r)$, devemos ter $r(g) = s(\pi(g)) = e$, e assim $\pi(g) \in Ker(s)$. Mas como s possui inversa à esquerda (por *(iii)*), a mesma deve ser injetiva, de onde $\pi(g) \in Ker(s) = \{e\}$ e, portanto, $g \in Ker(\pi)$. Como $Ker(\pi) = K$, temos que $g \in K$.

$(iv) \implies (i)$
Seja $Q = Im(r)$. Dado $g \in Q \cap K$, temos $r(g) = g$ pelo fato de que $g \in Q$, e $e = r(g)$ pelo fato de que $g \in K$. Assim, $g = e$ e, portanto, $Im(r) \cap K = Q \cap K = \{e\}$. Ainda, sendo $g \in G$, então

$$r(gr(g^{-1})) = r(g)r^2(g^{-1}) = r(g)r(g^{-1}) = r(gg^{-1}) = e$$

de onde $gr(g^{-1}) \in K = Ker(r)$. Assim, existe $x \in K$ tal que $gr(g^{-1}) = x$, e daí $g = x(r(g^{-1}))^{-1} = xr(g)$. Mostramos assim que $G = KIm(r)$, e portanto, G é produto semidireto de K por $Im(r)$. Mas pelo Teorema Fundamental dos Homomorfismos, temos $Im(r) \simeq \dfrac{G}{Ker(r)} = \dfrac{G}{K}$, e portanto, G é produto semidireto de K por $\dfrac{G}{K}$, o que mostra o resultado. $\square$

Exemplo 2.3. *Sendo $D_\infty = \mathbb{Z} \times \{-1, 1\}$, munido da operação:*

$$(a, n) * (b, m) = (a + nb, nm)$$

então $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}_2$. De fato, considerando os subgrupos

$$K = \{(a, 1), a \in \mathbb{Z}\} \quad e \quad Q = \{(0, 1), (0, -1)\}$$

vemos que $K \cap Q = \{(0, 1)\}$. Ainda, sendo $a \in \mathbb{Z}$, podemos escrever

$$(a, 1) = (a, 1) * (0, 1) \quad e \quad (a, -1) = (a, 1) * (0, -1),$$

o que mostra que $KQ = D_\infty$, e ainda que $K * (0, 1) \cup K * (0, -1) = D_\infty$, de onde K faz índice 2 e pelo Exemplo 1.17, é um subgrupo normal de D_∞. Assim, temos $D_\infty = K \rtimes Q = \mathbb{Z} \rtimes \mathbb{Z}_2$.

Lema 2.2. *Se G é um produto semidireto de K por Q, então existe um homomorfismo*

$$\begin{array}{rccc} \theta: & Q & \longrightarrow & Aut(K) \\ & x & \longmapsto & \theta_x = \psi_x|K, \end{array}$$

onde $\psi_x|K$ é a conjugação por x restrita a K, ou seja, ,

$$\begin{array}{rccc} \theta_x: & K & \longrightarrow & K \\ & a & \longmapsto & \theta_x(a) = xax^{-1}. \end{array}$$

Consequentemente, sendo $x, y, e \in Q$ e $a \in K$,

$$\theta_e(a) = a \quad e \quad \theta_x(\theta_y(a)) = \theta_{xy}(a).$$

Demonstração. Cada função θ_x, e portanto θ, estão bem definidas pela normalidade de K em G. Ademais, θ é um homomorfismo, pois dados $x, y \in Q$ e $a \in K$:

$$\theta_{xy}(a) = xya(xy)^{-1} = xyay^{-1}x^{-1} =$$
$$= x\theta_y(a)x^{-1} = \theta_x(\theta_y(a)) = (\theta_x \circ \theta_y)(a)$$

donde $\theta_{xy} = \theta_x \circ \theta_y$, o que mostra o lema. □

Agora, recuperaremos a estrutura de G a partir de K, Q e algum homomorfismo $\theta : Q \longrightarrow Aut(K)$.

Definição 2.3. Sejam Q e K grupos e seja $\theta : Q \longrightarrow Aut(K)$ um homomorfismo. Um produto semidireto G de K por Q **realiza** θ se, para todo $x \in Q$ e $a \in K$, tem-se

$$\theta_x(a) = xax^{-1}.$$

Nessa linguagem, o Lema 2.2 diz que todo produto semidireto G de K por Q determina um homomorfismo $\theta : Q \longrightarrow Aut(K)$, o qual ele realiza.

Definição 2.4. Dados os grupos Q e K e um homomorfismo $\theta : Q \longrightarrow Aut(K)$, definimos $G = K \rtimes_\theta Q$ como sendo o conjunto $K \times Q$ munido da operação

$$(a, x) *_\theta (b, y) = (a\theta_x(b), xy),$$

para $(a, x), (b, y) \in K \times Q$.

Teorema 2.3. *Dados os grupos Q e K, e um homomorfismo $\theta : Q \longrightarrow Aut(K)$, então $G = K \rtimes_\theta Q$ é um grupo, e G é um produto semidireto de Q por K que realiza θ.*

Demonstração. Mostremos que $G = K \rtimes_\theta Q$ é um grupo.

1) Associatividade:

Sejam $(a_1, x_1), (a_2, x_2), (a_3, x_3) \in K \rtimes_\theta Q$. Temos

$$[(a_1, x_1) *_\theta (a_2, x_2)] *_\theta (a_3, x_3) = (a_1\theta_{x_1}(a_2), x_1x_2) *_\theta (a_3, x_3) =$$

$$= (a_1\theta_{x_1}(a_2)\theta_{x_1x_2}(a_3), x_1x_2x_3).$$

Como θ é um homomorfismo, vale $\theta_{x_1x_2}(a_3) = \theta_{x_1}(\theta_{x_2}(a_3))$, e assim

$$(a_1\theta_{x_1}(a_2)\theta_{x_1x_2}(a_3), x_1x_2x_3) = (a_1\theta_{x_1}(a_2)\theta_{x_1}(\theta_{x_2}(a_3)), x_1x_2x_3) =$$

$$= (a_1\theta_{x_1}(a_2\theta_{x_2}(a_3)), x_1x_2x_3) = (a_1, x_1) *_\theta (a_2\theta_{x_2}(a_3), x_2x_3) =$$

$$= (a_1, x_1) *_\theta [(a_2, x_2) *_\theta (a_3, x_3)],$$

o que mostra a associatividade.

2) Existência de elemento neutro:

Sejam e_K e e_Q os elementos neutros de K e Q, respectivamente. Temos, para todo $(a, x) \in K \rtimes_\theta Q$,

$$(e_K, e_Q) *_\theta (a, x) = (e_K\theta_{e_Q}(a), e_Qx) = (e_Ka, e_Qx) = (a, x).$$

E por outro lado

$$(a, x) *_\theta (e_K, e_Q) = (a\theta_x(e_K), xe_Q) = (ae_K, xe_Q) = (a, x).$$

3) Existência de simétricos:

Seja $(a, x) \in K \rtimes_\theta Q$. Temos:

$$(a, x) *_\theta (\theta_{x^{-1}}(a^{-1}), x^{-1}) = (a\theta_{xx^{-1}}(a^{-1}), xx^{-1}) = (e_K, e_Q)$$

e

$$(\theta_{x^{-1}}(a^{-1}), x^{-1}) *_\theta (a, x) = (\theta_{x^{-1}}(a^{-1})\theta_{x^{-1}}(a), x^{-1}x) =$$
$$= (\theta_{x^{-1}}(e_K), e_Q) = (e_K, e_Q).$$

Assim, $K \rtimes_\theta Q$ é um grupo, cujo elemento neutro é (e_K, e_Q), o qual denotaremos por (e, e) e cujo simétrico de um elemento (a, x) é $(\theta_{x^{-1}}(a^{-1}), x^{-1})$.

Mostremos agora que G é um produto semidireto de Q por K que realiza θ. Para tal, defina as aplicações

$$\varphi_K : K \longrightarrow G \quad \text{e} \quad \varphi_Q : Q \longrightarrow G$$

tais que $\varphi_K(a) = (a, e)$ e $\varphi_Q(x) = (e, x)$. Tais aplicações são homomorfismos, cujas imagens são respectivamente os subgrupos

$$K_1 = \{(a, e) \in G; a \in K\} \quad \text{e} \quad Q_1 = \{(e, x), x \in Q\}.$$

Pelo Teorema Fundamental dos Homomorfismos, observando que tais homomorfismos são injetivos, concluímos que $K_1 \simeq K$ e $Q_1 \simeq Q$. Ainda, o homomorfismo

$$\begin{array}{rccc} \pi : & G & \longrightarrow & Q \\ & (a, x) & \longmapsto & \pi(a, x) = x \end{array}$$

tem núcleo $Ker(\pi) = \{(a, e), a \in K\} = K_1$, e pelo item *(iv)* da Observação 1.7, temos $K_1 \trianglelefteq G$. Denotaremos então, por abuso de notação, os conjuntos K_1 e Q_1 por K e Q, respectivamente. Como $K \cap Q = \{(e, e)\}$, e

$$(a, e) *_\theta (e, x) = (a\theta_e(e), x) = (a, x),$$

segue que G é o produto semidireto de K por Q. Ainda

$$(e, x) *_\theta (a, e) *_\theta (e, x)^{-1} = (\theta_x(a), x) *_\theta (e, x^{-1}) = (\theta_x(a), e)$$

o que mostra o resultado. □

Uma vez que $K \rtimes_\theta Q$ realiza θ, isto é, $\theta_x(b) = xbx^{-1}$, podemos usar a notação mais simplificada:

$$(a, x)(b, y) := (ab^x, xy), \text{ para todo } a, b \in K \text{ e } x, y \in Q.$$

Exemplo 2.4. *Considere K e Q grupos, e $\theta : Q \longrightarrow Aut(K)$ o homomorfismo trivial, isto é, $\theta(x) = Id_K$, para todo $x \in Q$. O produto semidireto $K \rtimes_\theta Q$ tem a operação*

$$(a, x)(b, y) := (ab, xy), \text{ para todo } a, b \in K \text{ e } x, y \in Q.$$

sendo assim o produto direto, definido no Exemplo 1.5. Vemos então que o produto direto é um caso particular de produto semidireto, a saber, o produto semidireto com homomorfismo θ trivial.

Exemplo 2.5. *Sendo $k \in \mathbb{N}$ e C_2 o grupo cíclico de dois elementos com notação multiplicativa, conforme o Exemplo 1.9, o* ***grupo diedral*** *D_{2k} é definido como o produto semidireto $\mathbb{Z}_k \rtimes_\theta C_2$, em que o homomorfismo $\theta : C_2 \longrightarrow Aut(\mathbb{Z}_k)$ é dado por*

$$\theta_n(\overline{x}) = \overline{nx}.$$

Assim, a operação de D_{2k} é dada por

$$(\overline{a}, n)(\overline{b}, m) = (\overline{a + nb}, nm).$$

Observação 2.3. *O grupo diedral D_{2n}, construído no exemplo anterior, pode ser visto como o grupo das simetrias de um polígono regular de n lados. Assim, muitos textos o denotam por D_n.*

Mostraremos agora que todo produto semidireto G de K por Q é isomorfo a $K \rtimes_\theta Q$, onde θ é o homomorfismo que G realiza.

Teorema 2.4. *Se G é um produto semidireto de K por Q, então existe $\theta : Q \longrightarrow Aut(K)$ tal que $G \simeq K \rtimes_\theta Q$.*

Demonstração. Consideremos o homomorfismo $\theta : Q \longrightarrow Aut(K)$ definido no Lema 2.2, ou seja, $\theta_x(a) = xax^{-1}$, para $a \in K$ e $x \in Q$. Como (pelo Lema 2.1) $g \in G$ tem uma expressão única como $g = ax$, com $a \in K$ e $x \in Q$, e como

$$(ax)(by) = a(xbx^{-1})xy = ab^x xy,$$

vemos que a aplicação

$$\begin{array}{rccc} \varphi : & K \rtimes_\theta Q & \longrightarrow & G \\ & (a, x) & \longmapsto & \varphi(a, x) = ax \end{array}$$

é um isomorfismo. □

Exemplo 2.6. *Para caracterizar os produtos semidiretos de $\mathbb{Z}_3$ por $\mathbb{Z}_4$, observemos que $Aut(\mathbb{Z}_3) = \{Id_{\mathbb{Z}_3}, f\}$, onde f é o automorfismo inversão definido no exemplo 1.29. Assim, os únicos produtos semidiretos de $\mathbb{Z}_3$ por $\mathbb{Z}_4$ são o produto direto e $\mathbb{Z}_3 \rtimes_f \mathbb{Z}_4$. Na bibliografia [2], seções V.9 e VI.5, é feita a caracterização dos grupos de ordem 12, que consiste dos dois grupos citados acima, além dos grupos $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, D_{12} e o subgrupo A_4 das permutações pares de S_4, o qual optamos por não definir nesse trabalho.*

Capítulo 3

Extensões de grupos

3.1 O problema das extensões

Definição 3.1. Sejam K e Q grupos. Uma **extensão** de K por Q é um grupo G que possui um subgrupo normal $K_1 \simeq K$ tal que $\dfrac{G}{K_1} \simeq Q$.

Observação 3.1. *Denotaremos K e Q com tais letras como recurso mnemônico, visto que tais letras lembram "Kernel" e "Quociente". Assim, nos referiremos ao K como **núcleo da extensão**. Ainda, usaremos as letras a, b, c para denotar elementos de K e x, y, z para denotar elementos de Q.*

Exemplo 3.1. *Para quaisquer grupos K e Q, são extensões de K por Q os produtos semidiretos*

$$K \rtimes_\theta Q$$

para qualquer $\theta : Q \longrightarrow Aut(K)$. Em particular, tomando $\theta : Q \longrightarrow Aut(K)$ como o homomorfismo trivial, concluímos que o produto direto $K \times Q$ é uma extensão de K por Q.

Exemplo 3.2. *Tanto $\mathbb{Z}_6$ quanto S_3 são extensões de $\mathbb{Z}_3$ por $\mathbb{Z}_2$. Por outro lado, $\mathbb{Z}_6$ é uma extensão de $\mathbb{Z}_2$ por $\mathbb{Z}_3$, mas S_3 não é.*

Com os exemplos anteriores, verificamos que, dados Q e K grupos, em geral não há unicidade de extensões de K por Q. Conforme dito na introdução do trabalho, isso motiva o seguinte problema: podemos conhecer todas as extensões de K por Q? Tal problema é conhecido como **problema das extensões** e tem duas possíveis vertentes:

i) Construir a tábua de operação de qualquer extensão de K por Q;

ii) Descobrir quantas extensões não isomorfas de K por Q existem.

A teoria clássica de extensões de grupos foi desenvolvida por O. Holder e O. Schreier. Em 1926, Schreier solucionou a primeira questão. Apesar disso,

a solução de Schreier não responde precisamente a segunda questão, apenas dá uma cota superior para o número de extensões não isomorfas.

Neste capítulo, faremos primeiramente o estudo das extensões de núcleo abeliano, que foi a abordagem inicial de Schreier. Após isso, estudaremos extensões cujo núcleo tem centro trivial, que tem uma forte relação com o que chamaremos de produto fibrado.

Um estudo mais geral de extensões de grupos pode ser feito, mas para isso se faz necessário um conhecimento maior de cohomologia, o que foge do escopo desse trabalho. Recomendamos as referências [4] e [5] para quem desejar fazer esse estudo.

Observação 3.2. *A primeira diferença que vemos entre produtos semidiretos e extensões é que uma extensão não precisa ter um subgrupo isomorfo a Q, enquanto um produto semidireto precisa.*

Exemplo 3.3. *$\mathbb{Z}$ é uma extensão de $\mathbb{Z}$ por $\mathbb{Z}_2$. Com efeito, $\mathbb{Z}$ possui o subgrupo $2\mathbb{Z}$, e $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \simeq \mathbb{Z}_2$. Observe ainda que $\mathbb{Z}$ não é um produto semidireto de $\mathbb{Z}$ por $\mathbb{Z}_2$, visto que $\mathbb{Z}$ não tem subgrupo isomorfo a $\mathbb{Z}_2$. Assim, existem extensões de grupos que não são produtos semidiretos.*

3.2 Sequências exatas curtas

Introduziremos nessa seção a linguagem de sequências exatas curtas, que é intrínseca à ideia de extensão de grupo. Por simplicidade, optamos por só usar essa linguagem a partir da discussão de equivalências de extensões, onde ela se mostra crucial.

Seja G uma extensão de K por Q. Isto significa que

(i) G possui um subgrupo normal $K_1 \simeq K$. Assim, existe um homomorfismo injetivo $i : K \longrightarrow G$ tal que $Im(i) = K_1$. Iremos escrever, por um aceitável abuso de notação, $K = K_1$ e suporemos que i é o homomorfismo inclusão.

(ii) De $\dfrac{G}{K} \simeq Q$, existe um homomorfismo sobrejetivo $\pi' : G \longrightarrow Q$ tal que $Ker(\pi') = K$. Com efeito, sendo $\varphi : \dfrac{G}{K} \longrightarrow Q$ um isomorfismo, a aplicação $\pi' = \varphi \circ \pi$, onde π é o homomorfismo projeção canônica definido, no Exemplo 1.26, é sobrejetivo e tem-se $Ker(\pi') = Ker(\pi) = K$. Usaremos o abuso de notação $\pi' = \pi$ para tal homomorfismo, apesar de que esta notação já estava sendo usada para o homomorfismo projeção canônica, pois se tomarmos $Q = \dfrac{G}{K}$, a projeção canônica é um exemplo de homomorfismo sobrejetivo e de núcleo $Ker(\pi) = K$. Deixaremos claro quando uma aplicação π for, de

fato, a projeção canônica.

Podemos então escrever a sequência de grupos e homomorfismos:

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

onde 1 é o grupo unitário. Na sequência acima, a imagem de cada homomorfismo é o núcleo do homomorfismo seguinte. Uma sequência que satisfaz tais propriedades é dita uma **sequência exata**. Esta, em particular, é chamada de **sequência exata curta**. A "exatidão" da sequência exata curta acima acontece exatamente quando i é injetivo, π é sobrejetivo e $Im(i) = Ker(\pi)$. Assim, é compatível a seguinte definição:

Definição 3.2. Sendo K, G e Q grupos, dizemos que uma sequência de grupos e homomorfismos

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

onde 1 é o grupo unitário, é uma **sequência exata curta** se i é injetiva, π é sobrejetiva, e $Im(i) = Ker(\pi)$.

Exemplo 3.4. *Se G é um grupo e $K \trianglelefteq G$, então a sequência*

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} \frac{G}{K} \longrightarrow 1$$

onde i e π são respectivamente a inclusão e a projeção canônica, é exata.

Vimos na discussão anterior que cada extensão de grupo, fixado um homomorfismo sobrejetivo $\pi : G \longrightarrow Q$ com $Ker(\pi) = K$, define uma sequência exata curta. Ademais, é fácil ver que uma sequência exata curta define uma extensão G de K por Q. Portanto, extensões de grupos e sequências exatas curtas são conceitos intrínsecos um ao outro.

Entre as vantagens da linguagem de sequências exatas curtas, vemos que a mesma explicita o homomorfismo π, que de certa forma mostra a relação entre G e Q. Além disso, tal conceito faz mais sentido com a linguagem de diagramas comutativos, que será muito explorada nas seções futuras.

3.3 Transversais e levantamentos

Definição 3.3. Se G é um grupo e $H \leq G$, um **transversal (à direita)** de H em G é um subconjunto $T \subseteq G$ tal que $Hg \cap T$ é unitário, para todo $g \in G$, onde Hg é a classe lateral à direita de H contendo g.

Observação 3.3. *Sendo K um subgrupo de G, então T é um transversal à direita de K em G, se, e somente se, valem*

$$G = \bigcup_{t \in T} Kt \quad e \quad Kt \neq Kt', \text{ para } t, t' \in T, \text{ com } t \neq t'.$$

Nas condições acima, cada elemento $g \in G$ tem uma única fatoração

$$g = kt, \text{ com } k \in K \text{ e } t \in T.$$

Exemplo 3.5. *Se G é um produto semidireto de K por Q, então Q é um transversal de K em G. Com efeito, pelo Lema 2.1, cada elemento $g \in G$ pode ser escrito de maneira única como $g = ax$, com $a \in K$ e $x \in Q$. Dessa forma, sendo $g = ax \in G$, temos $Kg = Kax = Kx$. Dado $y \in Kx \cap Q$, temos $y = bx$, para algum $b \in K$. Mas $y = ey$, e pela unicidade da expressão, temos $y = x$, de onde $Kg \cap Q = Kx \cap Q = \{x\}$.*

Definição 3.4. Se $\pi : G \longrightarrow Q$ é um homomorfismo sobrejetivo, um **levantamento** de $x \in Q$ é um elemento $l(x) \in G$ tal que $\pi(l(x)) = x$, isto é, um elemento do conjunto $\pi^{-1}(\{x\}])$.

Proposição 3.1. *Seja $\pi : G \longrightarrow Q$ um homomorfismo sobrejetivo. Um conjunto*

$$\{l(x); x \in Q\},$$

onde cada $l(x)$ é um levantamento escolhido de x, é um transversal (à direita) de $K = Ker(\pi)$ em G.

Demonstração. Tomando $K = Ker(\pi)$, se $x, y \in Q$ são tais que

$$Kl(x) = Kl(y)$$

então existe $k \in K$ tal que $l(x)l(y)^{-1} = k$, de onde $\pi(l(x)l(y)^{-1}) = 1$, ou ainda $\pi(l(x)) = \pi(l(y))$, e pelo fato de que $l(x)$ e $l(y)$ são levantamentos, temos $x = y$, e portanto $l(x) = l(y)$. Assim, dois elementos de $\{l(x); x \in Q\}$ determinam a mesma classe lateral de K se, e somente se, são iguais.

Sendo Kg uma classe lateral de K arbitrária, tome $q = \pi(g) \in Q$. Temos $\pi(g) = \pi(l(q))$, de onde $Kg = Kl(q)$. Mostramos assim que cada classe lateral tem um único representante no conjunto $\{l(x); x \in Q\}$, e assim tal conjunto é um transversal à direita. □

Definição 3.5. Seja $\pi : G \longrightarrow Q$ um homomorfismo sobrejetivo. Uma função

$$\begin{array}{rccc} l: & Q & \longrightarrow & G \\ & q & \longmapsto & l(q) \end{array}$$

tal que $\pi(l(q)) = q$ para todo $q \in Q$, é chamada de **(função) transversal à direita de** $Ker(\pi)$.

A proposição anterior garante que a definição de função transversal à direita faz sentido com a noção já estabelecida de transversal à direita. Portanto, chamaremos ambas de transversal à direita.

3.4 Extensões de núcleo abeliano

3.4.1 Datas

Sendo K e Q grupos, com K abeliano, mostraremos aqui que uma extensão G de K por Q determina um homomorfismo $\theta : Q \longrightarrow Aut(K)$ que, de certa forma, nos mostra "como K é normal em G". Veremos na subseção seguinte que, de posse de tal homomorfismo, é possível reconstruir a estrutura de toda extensão G que o induz.

Na discussão que segue, fixaremos para uma extensão G de K por Q um homomorfismo sobrejetivo $\pi : G \longrightarrow Q$ de núcleo $Ker(\pi) = K$, e $l : Q \longrightarrow G$ será um transversal à direita de $Ker(\pi) = K$, ou seja, $\pi \circ l = Id_Q$. Nesse contexto, diremos simplesmente que $l : Q \longrightarrow G$ é um transversal de K.

Teorema 3.1. *Seja G uma extensão de K por Q e seja $l : Q \longrightarrow G$ um transversal de K. Então, existe um homomorfismo*

$$\begin{array}{rccc} \theta : & Q & \longrightarrow & Out(K) = \dfrac{Aut(K)}{Inn(K)} \\ & x & \longmapsto & \theta_x = \psi_{l(x)} Inn(K) \end{array}$$

onde

$$\begin{array}{rccc} \psi_{l(x)} : & K & \longrightarrow & K \\ & a & \longmapsto & \psi_{l(x)}(a) = l(x)al(x)^{-1}. \end{array}$$

Além disso, se $l_1 : Q \longrightarrow G$ é outro transversal de K, então

$$\psi_{l(x)} Inn(K) = \psi_{l_1(x)} Inn(K)$$

para todo $x \in Q$, isto é, a aplicação θ independe do transversal escolhido. Ademais, se K é abeliano, o homomorfismo θ é da forma

$$\begin{array}{rccc} \theta : & Q & \longrightarrow & Aut(K) \\ & x & \longmapsto & \theta_x = \psi_{l(x)}. \end{array}$$

Demonstração. Seja

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

uma extensão G de K por Q, onde i é a inclusão, e escolha um transversal $l : Q \longrightarrow G$ para $K = Ker(\pi)$, isto é, $\pi(l(x)) = x$, para todo $x \in Q$. Definimos então a aplicação

$$\begin{array}{rccc} \psi_l : & Q & \longrightarrow & Aut(K) \\ & x & \longmapsto & \psi_l(x) = \psi_{l(x)} \end{array}$$

onde

$$\begin{array}{rccc} \psi_{l(x)} : & K & \longrightarrow & K \\ & a & \longmapsto & \psi_{l(x)}(a) = l(x)al(x)^{-1}. \end{array}$$

A aplicação ψ_l em geral não é um homomorfismo, e depende da escolha do transversal l. Sendo $l' : Q \longrightarrow G$ outro transversal de K, então

$$\pi(l'(x)l(x)^{-1}) = \pi(l'(x))\pi(l(x))^{-1} = xx^{-1} = 1$$

Ou seja, $l'(x)l(x)^{-1} \in Ker(\pi) = K$, de onde existe um $k(x) \in K = Ker(\pi)$ tal que $l'(x) = k(x)l(x)$, para cada $x \in Q$. Consequentemente, sendo $\psi_{l'} : Q \longrightarrow Aut(K)$ a aplicação induzida por l', conforme a construção de ψ_l, temos

$$\begin{gathered} \psi_{l'(x)}(a) = l'(x)al'(x)^{-1} = k(x)l(x)al(x)^{-1}k(x)^{-1} = \\ = (l(x)al(x)^{-1})^{k(x)} = (\psi_{l(x)}(a))^{k(x)} \end{gathered}$$

e portanto $\psi_{l(x)}$ e $\psi_{l'(x)}$ diferem por um automorfismo interno de K. Assim,

$$\psi_{l(x)}Inn(K) = \psi_{l'(x)}Inn(K)$$

o que nos leva a definir a função

$$\begin{array}{rccc} \theta : & Q & \longrightarrow & Out(K) \\ & x & \longmapsto & \theta(x) = \psi_{l(x)}Inn(K) \end{array}$$

que independe da escolha do transversal. Ademais,

$$\pi(l(xy)l(y)^{-1}l(x)^{-1}) = xyy^{-1}x^{-1} = 1$$

e portanto existe um $k' \in K$ tal que $l(xy) = k'l(x)l(y)$. Logo,

$$\begin{gathered} \psi_l(xy)(a) = l(xy)al(xy)^{-1} = k'l(x)l(y)al(y)^{-1}l(x)^{-1}(k')^{-1} = \\ = k'l(x)(\psi_{l(y)}(a))l(x)^{-1}(k')^{-1} = k'(\psi_{l(x)}(\psi_{l(y)}(a)))(k')^{-1} = \\ = ((\psi_{l(x)} \circ \psi_{l(y)})(a))^{k'}, \end{gathered}$$

de onde $\psi_{l(xy)}Inn(K) = (\psi_{l(x)} \circ \psi_{l(y)})Inn(K)$, e portanto θ é um homomorfismo.

Observe que, caso K seja abeliano, temos $Inn(K) = 1$, e assim $Out(K) = Aut(K)/1 \simeq Aut(K)$, e a aplicação θ toma a forma descrita no enunciado do Teorema. □

Observação 3.4. *Vimos na demonstração do Teorema 3.1 que toda extensão*

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

induz uma única aplicação $\theta : Q \longrightarrow Out(K)$, que nasce da conjugação por elementos de um transversal $l(x)$ qualquer. É natural fazer a pergunta: dado um homomorfismo $\theta : Q \longrightarrow Out(K)$ qualquer, existe uma extensão de K por Q cujo homomorfismo induzido seja θ? A resposta é negativa para o caso geral, e o estudo dessa pergunta leva à construção de uma função de nome obstrução, que está intimamente ligada ao terceiro grupo de cohomologia. Para um estudo detalhado de obstruções, recomendamos [4]. Veremos nesse trabalho que, para o caso K abeliano, a resposta para tal pergunta é afirmativa.

Observação 3.5. *Nas condições do Teorema 3.1 e supondo K abeliano, um homomorfismo $\theta : Q \longrightarrow Aut(K)$, conforme o construído, induz uma ação de Q em K, dada por*

$$x \cdot a = \theta_x(a) = l(x) + a - l(x), \text{ para } x \in Q \text{ e } a \in K$$

ou em notação multiplicativa (para K)

$$x \cdot a := a^x = l(x)al(x)^{-1}, \text{ para } x \in Q \text{ e } a \in K.$$

Usaremos notação multiplicativa principalmente quando G for um produto semidireto.

Note ainda que, além das propriedades usuais de ações, a ação descrita satisfaz

$$x \cdot (a + b) = \theta_x(a + b) = \theta_x(a) + \theta_x(b) = x \cdot a + x \cdot b \tag{3.4.1}$$

e

$$x \cdot (-a) = -(x \cdot a). \tag{3.4.2}$$

Destacamos que tais propriedades não valem para toda ação, sendo uma propriedade especial da ação aqui definida. Caso estejamos usando a notação multiplicativa em K, as equações acima se escrevem como

$$(ab)^x = \theta_x(ab) = \theta_x(a)\theta_x(b) = a^x b^x$$

e

$$(a^{-1})^x = (a^x)^{-1}.$$

No restante da seção, K sempre será um grupo abeliano. A notação aditiva será usada para as operações de K e G, apesar de que G não necessariamente é abeliano. Evitaremos usar a notação de sequências exatas curtas até a discussão sobre equivalências de extensões, seguindo a escolha de [6], visando simplicidade e acessibilidade ao texto. Para cada extensão G de K por Q, estará fixado $\pi : G \longrightarrow Q$ um homomorfismo sobrejetivo e de núcleo $Ker(\pi) = K$.

Definição 3.6. Uma tripla ordenada

$$(Q, K, \theta)$$

é dita uma **data** se K é um grupo abeliano, Q é um grupo e $\theta : Q \longrightarrow Aut(K)$ é um homomorfismo. Dizemos que um grupo G **realiza** a data (Q, K, θ) se G é uma extensão de K por Q e existe um homomorfismo $\pi : G \longrightarrow Q$ sobrejetivo de núcleo $Ker(\pi) = K$ tal que, para cada transversal $l : Q \longrightarrow G$ de K, vale

$$x \cdot a = \theta_x(a) = l(x) + a - l(x), \text{ para quaisquer } x \in Q \text{ e } a \in K.$$

Usando esses termos, o Teorema 3.1 diz que, quando K é abeliano, toda extensão G de K por Q determina um homomorfismo $\theta : Q \longrightarrow Aut(K)$, de forma que G realiza a data (Q, K, θ).

Assim, toda extensão realiza uma data e, portanto, o problema das extensões pode ser reformulado da seguinte forma: encontre todas as extensões G que realizam a data (Q, K, θ).

3.4.2 Construindo uma extensão

Mostraremos como construir uma tábua de operação de uma extensão G que realiza a data (Q, K, θ). Destacamos que, na discussão de extensões de núcleo abeliano, usaremos notação aditiva para K e para G, e notação multiplicativa para Q. Assim, denotaremos o elemento neutro de K (que é o mesmo de G) por 0 e o elemento neutro de Q por 1.

Seja $\pi : G \longrightarrow Q$ um homomorfismo sobrejetivo de núcleo K e escolha um transversal $l : Q \longrightarrow G$ com $l(1) = 0$. Dados $x, y \in Q$, temos

$$\pi(l(xy)) = xy \quad \text{e} \quad \pi(l(x) + l(y)) = \pi(l(x))\pi(l(y)) = xy$$

de onde $(l(x) + l(y) - l(xy)) \in Ker(\pi) = K$. Assim, está bem definida a função

$$\begin{array}{rccl} f: & Q \times Q & \longrightarrow & K \\ & (x, y) & \longmapsto & f(x, y) = l(x) + l(y) - l(xy) \end{array}$$

ou ainda, f é caracterizada pela relação

$$l(x) + l(y) = f(x, y) + l(xy).$$

Definição 3.7. Se $\pi : G \longrightarrow Q$ é um homomorfismo sobrejetivo de núcleo K e $l : Q \longrightarrow G$ é um transversal com $l(1) = 0$, então a função $f : Q \times Q \longrightarrow K$ tal que

$$l(x) + l(y) = f(x, y) + l(xy)$$

é chamada **2-cociclo (ou factor set)**.

Observação 3.6. *O termo 2-cociclo vem do estudo de grupos de cohomologia, pois, como veremos, estamos trabalhando com o segundo grupo de cohomologia. Uma vez que não trabalharemos com outros grupos de cohomologia, chamaremos um 2-cociclo simplesmente de cociclo.*

Observação 3.7. *Note que um cociclo f depende fortemente do transversal l escolhido.*

Exemplo 3.6. *Considere o caso especial de um produto semidireto G. Como já vimos, existe $\theta : Q \longrightarrow Aut(K)$ tal que $G \simeq K \rtimes_\theta Q$. Podemos então considerar G o conjunto dos elementos $(a, x) \in K \times Q$, com a operação*

$$(a, x)(b, y) = (ab^x, xy)$$

Considerando o homomorfismo sobrejetivo

$$\begin{array}{rccc} \pi : & G & \longrightarrow & Q \\ & (a, x) & \longmapsto & \pi(a, x) = x \end{array}$$

e $l : Q \longrightarrow G$ o transversal definido por

$$l(x) = (0, x)$$

então l é um homomorfismo, de onde o cociclo f definido por tal transversal é identicamente nulo. Assim, podemos pensar no cociclo como uma "medida" do quanto G se distancia de um produto semidireto, pois ele descreve uma "obstrução" que impede l de ser um homomorfismo.

Teorema 3.2. *Sejam $\pi : G \longrightarrow Q$ um homomorfismo sobrejetivo cujo núcleo é K, com K abeliano, $l : Q \longrightarrow G$ um transversal, com $l(1) = 0$, e $f : Q \times Q \longrightarrow K$ o cociclo correspondente. Então:*

(i) Para todo $x, y \in Q$, vale

$$f(1, y) = 0 = f(x, 1)$$

(ii) f satisfaz

$$f(x,y) + f(xy,z) = x \cdot f(y,z) + f(x,yz)$$

para todo $x, y, z \in Q$*, onde* $x \cdot f(y,z) = l(x) + f(y,z) - l(x)$*. Tal equação é chamada de* ***identidade dos cociclos****.*

Demonstração. (i) A definição de f nos dá

$$f(1,y) = l(1) + l(y) - l(1y) = 0 + l(y) - l(y) = 0,$$

$$f(x,1) = l(x) + l(1) - l(x1) = l(x) + 0 - l(x) = 0.$$

(ii) Temos

$$(l(x) + l(y)) + l(z) = (f(x,y) + l(xy)) + l(z) =$$

$$= f(x,y) + (l(xy) + l(z)) = f(x,y) + f(xy,z) + l(xyz)$$

e

$$l(x) + (l(y) + l(z)) = l(x) + (f(y,z) + l(yz)) =$$

$$= (l(x) + f(y,z) - l(x)) + (l(x) + l(yz)) = x \cdot f(y,z) + f(x,yz) + l(xyz).$$

Igualando as equações acima, obtemos a identidade dos cociclos. □

Mostraremos agora a recíproca do Teorema 3.2, que nos dará uma maneira de construir extensões de núcleo abeliano.

Teorema 3.3. *Dada a data* (Q, K, θ)*, se uma função* $f : Q \times Q \longrightarrow K$ *satisfaz a* ***identidade dos cociclos***

$$f(x,y) + f(xy,z) = x \cdot f(y,z) + f(x,yz)$$

e ainda $f(1,y) = 0 = f(x,1)$*, para quaisquer* $x, y, z \in Q$*, então* f *é um cociclo. Mais precisamente, existe uma extensão* G *realizando a data* (Q, K, θ)*, um homomorfismo* $\pi : G \longrightarrow Q$ *sobrejetivo e de núcleo* K*, e um transversal* $l : Q \longrightarrow G$ *tal que* f *é o cociclo correspondente.*

Demonstração. Seja G o conjunto dos pares ordenados $(a,x) \in K \times Q$, munido da operação

$$(a,x) + (b,y) = (a + x \cdot b + f(x,y), xy).$$

A demonstração de que G é um grupo é um tanto maçante, e portanto seguirá no fim da demonstração do teorema. Aceitemos temporariamente que G é de fato um grupo e que

$$0_G = (0,1) \quad \text{e} \quad -(a,x) = (-x^{-1} \cdot a - x^{-1} \cdot f(x, x^{-1}), x^{-1}).$$

Defina $\pi : G \longrightarrow Q$ por $(a, x) \longmapsto x$. Temos que π é um homomorfismo, pois sendo $(a, x), (b, y) \in G$, temos

$$\pi((a, x) + (b, y)) = \pi(a + x \cdot b + f(x, y), xy) = xy = \pi((a, x))\pi((b, y)).$$

Ainda, π é sobrejetivo, e tem núcleo $Ker(\pi) = \{(a, 1); a \in K\}$.

Afirmação: $K \simeq Ker(\pi)$

De fato, a aplicação

$$\begin{array}{rccc} \varphi: & K & \longrightarrow & Ker(\pi) \\ & a & \longmapsto & \varphi(a) = (a, 1) \end{array}$$

é bijetiva, e ainda, para quaisquer $a, b \in K$,

$$\varphi(a + b) = (a + b, 1) = (a + 1 \cdot b + f(1, 1), 1) = (a, 1) + (b, 1) = \varphi(a) + \varphi(b).$$

Assim, G é uma extensão de $K \simeq Ker(\pi)$ por Q. Usaremos, pelo resto dessa demonstração, o abuso de notação em que diremos que $x = \varphi(x)$, apesar de x e $\varphi(x)$ serem objetos de naturezas diferentes. Tal abuso de notação pode ser evitado usando linguagem de equivalência de sequências exatas, que será introduzida mais adiante. Aqui, optamos pela simplicidade.

Mostremos agora que G realiza (Q, K, θ), isto é, que dado um transversal $l : Q \longrightarrow G$ arbitrário, devemos ter

$$x \cdot a = \theta_x(a) = l(x) + a - l(x), \text{ para quaisquer } x \in Q \text{ e } a \in K.$$

Pela forma como π foi definida, para cada $x \in Q$, devemos ter $l(x) = (b_x, x)$, para algum $b_x \in K$. Assim,

$$l(x) + a - l(x) = (b_x, x) + (a, 1) - (b_x, x) =$$

$$= (b_x + x \cdot a, x) + (-x^{-1} \cdot b_x - x^{-1} \cdot f(x, x^{-1}), x^{-1}) =$$

$$= (b_x + x \cdot a + x \cdot (-x^{-1} \cdot b_x - x^{-1} \cdot f(x, x^{-1})) + f(x, x^{-1}), xx^{-1}) =$$

$$(b_x + x \cdot a - b_x - f(x, x^{-1}) + f(x, x^{-1}), 1) = (b_x + x \cdot a - b_x, 1) = (x \cdot a, 1).$$

Como identificamos a como $\varphi(a)$, temos $x \cdot a = \varphi(x \cdot a) = (x \cdot a, 1)$, segue que G realiza a data (Q, K, θ).

Nos resta mostrar que f é um cociclo para algum transversal de G. Defina o transversal

$$\begin{array}{rccc} l: & Q & \longrightarrow & G \\ & x & \longmapsto & l(x) = (0, x). \end{array}$$

Temos

$$f(x,y) = l(x) + l(y) - l(xy) = (0,x) + (0,y) - (0,xy) =$$

$$= (0 + x \cdot 0 + f(x,y), xy) + (-(xy)^{-1} \cdot 0 - (xy)^{-1} \cdot f(xy,(xy)^{-1}),(xy)^{-1}) =$$

$$= (f(x,y),xy) + (-(xy)^{-1} \cdot f(xy,(xy)^{-1}),(xy)^{-1}) =$$

$$= (f(x,y) + (xy) \cdot (-(xy)^{-1} \cdot f(xy,(xy)^{-1})) + f(xy,(xy)^{-1},1) =$$

$$= (f(x,y) - f(xy,(xy)^{-1}) + f(xy,(xy)^{-1}),1) = (f(x,y),1),$$

de onde f, que pelo abuso de notação adotado é vista como $(f,1)$, é um cociclo. Basta então mostrarmos que G é, de fato, um grupo.
Afirmação: G é um grupo.
(i) Associatividade:
Sejam $(a,x),(b,y),(c,z) \in G$. Temos

$$[(a,x) + (b,y)] + (c,z) = (a + x \cdot b + f(x,y), xy) + (c,z) =$$

$$(a + x \cdot b + f(x,y) + (xy) \cdot c + f(xy,z), xyz) \tag{3.4.3}$$

e

$$(a,x) + [(b,y) + (c,z)] = (a,x) + (b + y \cdot c + f(y,z), yz) =$$

$$= (a + x \cdot (b + y \cdot c + f(y,z)) + f(x,yz), xyz) =$$

$$(a + x \cdot b + x \cdot (y \cdot c) + x \cdot f(y,z) + f(x,yz), xyz). \tag{3.4.4}$$

Observe que, para demonstrar a Equação 3.4.4, usamos a Propriedade 3.4.1. Usando que

$$x \cdot (y \cdot c) = (xy) \cdot c$$

(do fato de que $\cdot$ é uma ação), que f satisfaz a identidade dos cociclos e que K é abeliano, temos que o elemento (3.4.3) é igual ao elemento (3.4.4), o que mostra a associatividade.
(ii) Existência de elemento neutro:
Sendo $(a,x) \in G$, temos

$$(a,x) + (0,1) = (a + x \cdot 0 + f(x,1), x) = (a,x)$$

e

$$(0,1) + (a,x) = (0 + 1 \cdot a + f(1,x), x) = (a,x),$$

e portanto $(0,1)$ é elemento neutro de G.
(iii) Existência de simétrico aditivo:
Sendo $(a,x) \in G$, temos

$$(a,x) + (-x^{-1} \cdot a - x^{-1} \cdot f(x,x^{-1}), x^{-1}) =$$

$$(a + x \cdot (-x^{-1} \cdot a - x^{-1} \cdot f(x, x^{-1})) + f(x, x^{-1}), 1) =$$
$$= (a + x \cdot (x^{-1} \cdot (-a)) + x \cdot (x^{-1} \cdot (-f(x, x^{-1}))) + f(x, x^{-1}), 1) =$$
$$(a + 1 \cdot (-a) + 1 \cdot (-f(x, x^{-1}) + f(x, x^{-1}, 1) = (0, 1)$$

e

$$(-x^{-1} \cdot a - x^{-1} \cdot f(x, x^{-1}), x^{-1}) + (a, x) =$$
$$(-x^{-1} \cdot a - x^{-1} \cdot f(x, x^{-1}) + x^{-1} \cdot a + f(x^{-1}, x), x^{-1}x) =$$
$$= (-x^{-1} \cdot f(x, x^{-1}) + f(x^{-1}, x), 1) = (*)$$

Mas, pela identidade dos cociclos,

$$(*) = (f(x^{-1}, xx^{-1}) - f(x^{-1}x, x^{-1}), 1) = (f(x^{-1}, 1) - f(1, x^{-1}), 1) = (0, 1)$$

Concluímos então que G é um grupo. □

Denotaremos a extensão G construída na demonstração do teorema anterior por G_f. Note que G_f realiza (Q, K, θ) e tem um cociclo f, que é induzido pelo transversal

$$l(x) = (0, x).$$

Concluímos essa discussão com o seguinte resultado:

Teorema 3.4. *Sejam G uma extensão satisfazendo a data (Q, K, θ), $\pi : G \longrightarrow Q$ um homomorfismo sobrejetivo de núcleo K, $l : Q \longrightarrow G$ um transversal de K e f o cociclo de G correspondente à l. Então $G \simeq G_f$.*

Demonstração. Considere a aplicação

$$\begin{array}{rccl} \varphi : & G_f & \longrightarrow & G \\ & (a, x) & \longmapsto & \varphi(a, x) = a + l(x). \end{array}$$

Pela Observação 3.3, todo elemento $g \in G$ pode ser escrito de maneira única como $g = a + l(x)$, com $a \in K$ e $x \in Q$, o que mostra que φ é bijetora. Ademais, temos

$$\varphi((a, x) + (b, y)) = \varphi(a + x \cdot b + f(x, y), xy) = a + x \cdot b + f(x, y) + l(xy) =$$
$$= a + (l(x) + b - l(x)) + l(x) + l(y) = a + l(x) + b + l(y) = \varphi(a, x) + \varphi(b, y)$$

o que mostra que φ é um isomorfismo, e portanto $G \simeq G_f$. □

Mostramos nessa subseção que, a partir de uma extensão, podemos construir cociclos, e que de posse de um cociclo f, podemos construir uma extensão G_f que o induz e, finalmente, que toda extensão é isomorfa a uma construída dessa forma. Assim, a questão de como encontrar todas as extensões de G que realizam a data (Q, K, θ) foi respondida: basta construirmos todas as aplicações $f : Q \times Q \longrightarrow K$ que satisfazem as propriedades *(i)* e *(ii)* descritas no Teorema 3.2, isto é, construir todos os cociclos.

3.4.3 Extensões de núcleo abeliano e o segundo grupo de cohomologia

Mostraremos aqui que o conjunto de todos os cociclos com relação a uma data (Q, K, θ), isto é, todas as aplicações $f : Q \times Q \longrightarrow K$ que satisfazem as propriedades *(i)* e *(ii)* do Teorema 3.2, tem a organização de um grupo abeliano. Isso induz uma organização de grupo abeliano no conjunto de todas as extensões que realizam (Q, K, θ). Comecemos introduzindo a seguinte uma notação para o tal conjunto.

Notação: Denotaremos por $Z^2(Q, K, \theta)$ o conjunto de todos os cociclos $f : Q \times Q \longrightarrow K$, onde K é abeliano, com relação ao homomorfismo $\theta : Q \longrightarrow Aut(K)$.

Podemos munir $Z^2(Q, K, \theta)$ da operação:

$$(f + g)(x, y) = f(x, y) + g(x, y), \text{ para } f, g \in Z^2(Q, K, \theta)$$

Essa operação está bem definida, pois sendo $f, g \in Z^2(Q, K, \theta)$, então

$$(f + g)(1, y) = f(1, y) + g(1, y) = 0 = f(x, 1) + g(x, 1) = (f + g)(x, 1)$$

e

$$x \cdot (f + g)(y, z) - (f + g)(xy, z) + (f + g)(x, yz) - (f + g)(x, y) =$$

$$= x \cdot f(y, z) + x \cdot g(y, z) - f(xy, z) - g(xy, z) + f(x, yz) +$$

$$+ g(x, yz) - f(x, y) - g(x, y)$$

$$= (x \cdot f(y, z) - f(xy, z) + f(x, yz) - f(x, y)) +$$

$$(x \cdot g(y, z) - g(xy, z) + g(x, yz) - g(x, y)) = 0 + 0 = 0.$$

Isso mostra que $(f + g)$ é um cociclo, de onde segue a boa definição da operação.

Ainda, a função $0(x, y) = 0$, para quaisquer $x, y \in Q$, é um cociclo, e se f é um cociclo, então $-f$ também é um cociclo, pois tanto as propriedades *(i)* e *(ii)*, descritas no Teorema 3.2, de $-f$ seguem das de f, apenas tomando inversos. Concluímos assim que $Z^2(Q, K, \theta)$, munido da soma usual de funções, é um grupo. Podemos ainda observar que $Z^2(Q, K, \theta)$ é abeliano, o que vem da comutatividade da operação de K.

Considere agora os grupos G_f e G_g que realizam (Q, K, θ) e têm f e g como cociclos, respectivamente. A operação de $Z^2(Q, K, \theta)$ nos induz:

$$G_f + G_g := G_{f+g}$$

o que mostra que o conjunto das extensões G_f, onde f é um cociclo com respeito a uma homomorfismos sobrejetivo $\pi : G \longrightarrow Q$ de núcleo $Ker(\pi) = K$ fixada, realizando (Q, K, θ) tem uma organização de grupo abeliano, onde o elemento neutro é o produto semidireto $K \rtimes_\theta Q$.

Apesar disso, ainda temos um problema: considere G uma extensão que realiza (Q, K, θ), $\pi : G \longrightarrow Q$ homomorfismo sobrejetivo e de núcleo K, e $l, l' : Q \longrightarrow G$ transversais de K, com f e f' os cociclos induzidos por l e l', respectivamente. Os grupos G_f e $G_{f'}$ são isomorfos, visto que pelo Teorema 3.4, ambos são isomorfos a G, mas não estamos fazendo distinção entre eles. Isso mostra que o grupo das extensões da forma G_f é enorme e impreciso, visto que a mesma extensão aparece nele várias vezes.

Exemplo 3.7. *Considere $K = \mathbb{Z}$ e $Q = C_2 = \{-1, 1\}$. Como $C_2 \simeq Aut(\mathbb{Z}) = \{Id, \varphi\}$, onde φ é o automorfismo inversão, só existem duas possibilidades para um homomorfismo $\theta : C_2 \longrightarrow Aut(\mathbb{Z})$:*

$$\theta_0 : C_2 \longrightarrow Aut(\mathbb{Z}) \quad e \quad \theta_1 : C_2 \longrightarrow Aut(\mathbb{Z})$$

$$-1 \longmapsto Id. \qquad\qquad -1 \longmapsto \varphi.$$

Construamos então cociclos para as datas $(C_2, \mathbb{Z}, \theta_0)$ e $(C_2, \mathbb{Z}, \theta_1)$. Para que $f : C_2 \times C_2 \longrightarrow \mathbb{Z}$ seja um cociclo devemos ter necessariamente

$$0 = f(1,1) = f(1,-1) = f(-1,1)$$

de onde, tanto para θ_0 quanto pra θ_1, nosso problema se resume a escolher $f(-1,-1)$. Escrevendo a identidade dos cociclos como

$$f(x,y) = x \cdot f(y,z) + f(x,yz) - f(xy,z)$$

que vale imediatamente para $x = 1$ e para $y = 1$, para que f seja um cociclo, só precisamos ter que

$$f(-1,-1) = (-1) \cdot f(-1,z) + f(-1,-z)$$

para todo $z \in C_2$. Observando que tal igualdade sempre é satisfeita quando $z = 1$, concluímos que f é um cociclo se, e somente se,

$$f(-1,-1) = (-1) \cdot f(-1,-1).$$

Dividamos então nosso problema nos dois casos:

(i) Para a data $(C_2, \mathbb{Z}, \theta_1)$, temos

$$f(-1,-1) = (-1) \cdot f(-1,-1) = -f(-1,-1),$$

de onde $f(-1,-1)=0$. *Assim, a única extensão possível satisfazendo a data* $(C_2,\mathbb{Z},\theta_1)$ *é o produto semidireto* $\mathbb{Z}\rtimes_{\theta_1} C_2\simeq D_\infty$ *(veja o Exemplo 2.3).*

(ii) Já para a data $(C_2,\mathbb{Z},\theta_0)$, f *é um cociclo se, e somente se, vale*

$$f(-1,-1)=(-1)\cdot f(-1,-1)=f(-1,-1)$$

o que é satisfeito sempre. Assim, seja qual for o valor escolhido para $f(-1,-1)$, *obteremos um cociclo. Observe que qualquer extensão satisfazendo essa data é um grupo abeliano. Obtemos assim mais dois casos:*

(iia) Quando $f(-1,-1)$ *for ímpar, devemos ter* G_f *isomorfo a* $\mathbb{Z}$. *Com efeito, definindo aplicação* $\psi:\mathbb{Z}\longrightarrow G_f$ *tal que:*

$$\psi(n)=n\left(\frac{-f(-1,-1)+1}{2},-1\right)=$$

$$=\begin{cases}(k,1) & ,\ se\ n=2k.\\ \left(\dfrac{-f(-1,-1)+1}{2}+k,-1\right) & ,\ se\ n=2k+1.\end{cases}$$

Temos que ψ *é um homomorfismo, pois foi obtida conforme o Exemplo 1.24, tomando*

$$\varphi(1)=\left(\frac{-f(-1,-1)+1}{2},-1\right).$$

Mostremos que ψ *é bijetiva. Quanto à injetividade, seja* $n\in Ker(\psi)$, *isto é,* $\psi(n)=(0,1)$. *Pela definição da* ψ, *temos* n *par, de onde* $k=0$, *e portanto a aplicação é injetiva. Para a sobrejetividade, sendo* $(x,y)\in G_f$, *se* $y=1$, *então* $(x,y)=\psi(2x)$. *Caso* $y=-1$, *temos* $(x,y)=\psi(2x+f(-1,-1))$, *o que mostra a sobrejetividade. Assim,* ψ *é um isomorfismo, e concluímos que* G_f *é isomorfo a* $\mathbb{Z}$.

(iib) Caso $f(-1,-1)$ *seja par, temos* $G_f\simeq\mathbb{Z}\times C_2$. *De fato, note que* $K_1:=\{(a,1),a\in\mathbb{Z}\}:=K_1\simeq\mathbb{Z}$, *pois a aplicação*

$$\begin{array}{rccl}\varphi: & \mathbb{Z} & \longrightarrow & K_1\\ & a & \longmapsto & \varphi(a)=(a,1)\end{array}$$

é um isomorfismo. Ademais, temos

$$H=\left\langle\left(\frac{-f(-1,-1)}{2},-1\right)\right\rangle\simeq C_2,$$

pois

$$2\left(\frac{-f(-1,-1)}{2},-1\right)=$$

$$= \left(\frac{-f(-1,-1)}{2} + \frac{-f(-1,-1)}{2} + f(-1,-1), (-1)(-1) \right) = (0,1) = 0_{G_f}.$$

Ainda, temos $K_1, H \trianglelefteq G_f$*, pois* G_f *é abeliano, e* $K_1 \cap H = \{0_{G_f}\}$*. Como*

$$(a,-1) = \left(a + \frac{f(-1,-1)}{2}, 1 \right) + \left(\frac{-f(-1,-1)}{2}, -1 \right),$$

segue que $(a,x) \in K_1 + H$*, quaisquer que sejam* $a \in \mathbb{Z}$ *e* $x \in C_2$*. Assim, pelo Exemplo 1.25, temos* $G_f \simeq K \times H \simeq \mathbb{Z} \times C_2$*.*

Concluímos então a classificação de todas as extensões de $\mathbb{Z}$ *por* C_2*, isto é, só existem três extensões de* $\mathbb{Z}$ *por* C_2*: uma realizando* $(C_2, \mathbb{Z}, \theta_1)$*, a saber, o produto semidireto* D_∞*, e duas realizando* $(C_2, \mathbb{Z}, \theta)$*, sendo elas o produto (semi)direto* $\mathbb{Z} \times C_2$ *e* $\mathbb{Z}$*, que* ***não*** *é um produto semidireto.*

O exemplo anterior nos passa a impressão de que as extensões satisfazendo (Q, K, θ) se organizam em classes de equivalência. Mostraremos que isso é, de fato, verdade.

Lema 3.5. *Sejam* G *uma extensão que realiza* (Q, K, θ)*,* l *e* l' *transversais com* $l(1) = 0 = l'(1)$*, induzindo cociclos* f *e* f'*, respectivamente. Então, existe uma função* $h : Q \longrightarrow K$*, com* $h(1) = 0$*, tal que*

$$f'(x,y) - f(x,y) = x \cdot h(y) - h(xy) + h(x), \text{ para quaisquer } x, y \in Q.$$

Demonstração. Para cada $x \in Q$, como $l(x)$ e $l'(x)$ são representantes da mesma classe lateral de K em G, existe um elemento $h(x) \in K$ tal que

$$l'(x) = h(x) + l(x).$$

Note que, como $l'(1) = l(1) = 0$, então $h(1) = 0$. A equação enunciada vem de

$$l'(x) + l'(y) = [h(x) + l(x)] + [h(y) + l(y)] =$$
$$= h(x) + x \cdot h(y) + l(x) + l(y) = h(x) + x \cdot h(y) + f(x,y) + l(xy) =$$
$$= h(x) + x \cdot h(y) + f(x,y) - h(xy) + l'(xy)$$

Como $l'(x) + l'(y) = f'(x,y) + l'(xy)$, temos que

$$f'(x,y) - f(x,y) = x \cdot h(y) - h(xy) + h(x)$$

o que mostra o lema. □

Definição 3.8. Dada a data (Q, K, θ), um **cobordo** é uma função $g : Q \times Q \longrightarrow K$ para a qual existe $h : Q \longrightarrow K$, com $h(1) = 0$ e

$$g(x,y) = x \cdot h(y) - h(xy) + h(x), \text{ para quaisquer } x, y \in Q.$$

O conjunto de todos os cobordos é denotado por $B^2(Q,K,\theta)$.

Observação 3.8. *O conjunto $B^2(Q,K,\theta)$ é fechado à soma e à inversão, pois se $g_1, g_2 \in B^2(Q,K,\theta)$, então existem $h_1, h_2 : Q \longrightarrow K$, com $h_1(1) = h_2(1) = 0$, tais que*

$$g_1(x,y) = x \cdot h_1(y) - h_1(xy) + h_1(x) \quad e \quad g_2(x,y) = x \cdot h_2(y) - h_2(xy) + h_2(x)$$

de onde $(h_1 + h_2)(1) = 0$ e $(-h_1)(1) = 0$, e ainda

$$(g_1 + g_2)(x,y) = x \cdot (h_1 + h_2)(y) - (h_1 + h_2)(xy) + (h_1 + h_2)(x)$$

e

$$(-g_1)(x,y) = x \cdot (-h_1)(y) - (-h_1)(xy) + h_1(x).$$

Basta verificarmos que cada cobordo é um cociclo para concluir que $B^2(Q,K,\theta) \leq Z^2(Q,K,\theta)$. Temos

$$g(1,y) = 1 \cdot h(y) - h(y) + h(1) = 0 = x \cdot h(1) - h(x) + h(x) = g(x,1)$$

e

$$\begin{gathered} x \cdot g(y,z) - g(xy,z) + g(x,yz) - g(x,y) = \\ = x \cdot (y \cdot h(z) - h(yz) + h(y)) - (xy \cdot h(z) - h(xyz) + h(xy)) + \\ + (x \cdot h(yz) - h(xyz) + h(x)) - (x \cdot h(y) - h(xy) + h(x)) = 0 \end{gathered}$$

isto é, $g(1,y) = 0 = g(x,1)$, para quaisquer $x, y \in Q$ e g satisfaz a identidade dos cociclos. Mostramos então que todo cobordo é um cociclo, e assim $B^2(Q,K,\theta) \leq Z^2(Q,K,\theta)$. Ademais, como $Z^2(Q,K,\theta)$ é abeliano, temos $B^2(Q,K,\theta) \trianglelefteq Z^2(Q,K,\theta)$.

Definição 3.9. Duas extensões G e G' realizando uma data (Q,K,θ) são ditas **equivalentes** se existem cociclos f de G e f' de G' tais que

$$f' - f \in B^2(Q,K,\theta).$$

Observação 3.9. *Nas condições da definição 3.9, a relação $G \cong G' \iff$ G é equivalente a G' define uma relação de equivalência no conjunto das extensões que realizam a data (Q,K,θ), no contexto da definição 0.2.17, apresentada na bibliografia [1], página 13.*

Definição 3.10. Dada a data (Q,K,θ), o grupo

$$H^2(Q,K,\theta) = \frac{Z^2(Q,K,\theta)}{B^2(Q,K,\theta)}$$

é chamado **segundo grupo de cohomologia**.

Em termos da Definição 3.10, podemos dizer que dois cociclos f e f' são equivalentes quando determinam o mesmo elemento de $H^2(Q, K, \theta)$, isto é, $f + B^2(Q, K, \theta) = f' + B^2(Q, K, \theta)$.

O Exemplo 3.7 nos desperta, à luz das novas definições, o seguinte questionamento: o número de extensões, a menos de isomorfismo que, que realizam (Q, K, θ) é $|H^2(Q, K, \theta)|$?

A resposta é negativa, como mostra o próximo exemplo.

Exemplo 3.8. *Seja p um número primo. Uma extensão de $\mathbb{Z}_p$ por $\mathbb{Z}_p$ deve ter ordem p^2. Pelo Teorema 4.3.7, página 226 de [1], um grupo de ordem p^2 é necessariamente abeliano. Ademais, pelo Teorema Fundamental dos Grupos Abelianos Finitamente Gerados (que em [1] é o Teorema 2.4.12 da página 133), só existem dois grupos abelianos de ordem p^2, a menos de isomorfismo, sendo eles $\mathbb{Z}_{p^2}$ e $\mathbb{Z}_p \times \mathbb{Z}_p$. Assim, como todo grupo de ordem p^2 é abeliano, só existem dois grupos de ordem p^2, e portanto só existem duas extensões de $\mathbb{Z}_p$ por $\mathbb{Z}_p$.*

Note agora que, como $Aut(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$, só existe um homomorfismo

$$\theta : \ \mathbb{Z}_p \ \longrightarrow \ Aut(\mathbb{Z}_p)$$

isto é, θ é o homomorfismo nulo. Com efeito, pelo Teorema Fundamental dos Homomorfismos (Teorema 1.4), temos $\dfrac{\mathbb{Z}_p}{Ker(\theta)} \simeq Im(\theta)$, e assim, $|\mathbb{Z}_p| = |Ker(\theta)||Im(\theta)|$, e daí $|Im(\theta)|$ divide $|\mathbb{Z}_p| = p$. Mas, pelo Teorema de Lagrange (Teorema 1.1), temos também que $|Im(\theta)|$ divide $|Aut(\mathbb{Z}_p)| = p-1$, o que mostra que $|Im(\theta)|$ divide $mdc(p, p-1) = 1$ e, portanto, $|Im(\theta)| = 1$. Assim, todas as extensões de $\mathbb{Z}_p$ por $\mathbb{Z}_p$ realizam $(\mathbb{Z}_p, \mathbb{Z}_p, \theta)$.

Agora, sendo $f \in Z^2(\mathbb{Z}_p, \mathbb{Z}_p, \theta)$, temos

$$pf(x, y) = 0, \ \text{para quaisquer } x, y \in \mathbb{Z}_p,$$

pois $f(x, y) \in \mathbb{Z}_p$. Assim,

$$p\overline{f} = \overline{0}, \ \text{para todo } \overline{f} \in H^2(\mathbb{Z}_P, \mathbb{Z}_P, \theta),$$

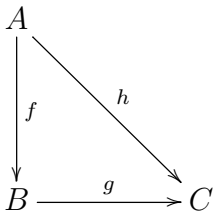
de onde $H^2(\mathbb{Z}_p, \mathbb{Z}_p, \theta)$ é trivial ou p divide $|H^2(\mathbb{Z}_p, \mathbb{Z}_p, \theta)|$, pois pelo Corolário 1.2 (observe que $Z^2(\mathbb{Z}_p, \mathbb{Z}_p, \theta)$ é um grupo finito) e Proposição 1.1, temos que $\circ(\overline{f})$ divide $|H^2(\mathbb{Z}_p, \mathbb{Z}_p, \theta)|$. Em ambos os casos, tomando $p \neq 2$, obtemos $|H^2(\mathbb{Z}_p, \mathbb{Z}_p, \theta)| \neq 2$, que portanto difere do número de extensões, a menos de isomorfismo, que realizam $(\mathbb{Z}_p, \mathbb{Z}_p, \theta)$.

3.4.4 Equivalência de Extensões

Nessa subseção, trabalharemos com o conceito de diagramas comutativos para caracterizar equivalência de extensões de núcleo abeliano (Definição 3.9).

Definição 3.11. Um diagrama de grupos e homomorfismos comuta (ou é **comutativo**) se, para cada par de grupos G e H no diagrama, todas as composições de homomorfismos de G a H são iguais.

Exemplo 3.9. *O diagrama*



comuta se, e somente se, tem-se

$$h = g \circ f.$$

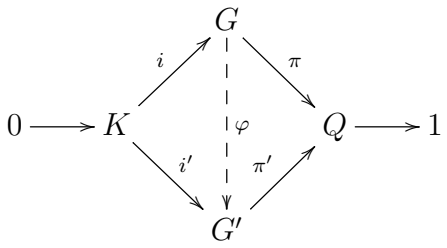
Teorema 3.6. *Duas extensões*

$$0 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

e

$$0 \longrightarrow K \xrightarrow{i'} G' \xrightarrow{\pi'} Q \longrightarrow 1$$

realizando a data (Q, K, θ) são equivalentes se, e somente se, existe um homomorfismo $\varphi : G \longrightarrow G'$ fazendo o seguinte diagrama comutar:



(3.4.5)

Observação 3.10. *No teorema acima, suporemos por simplicidade de notação que i e i' são, respectivamente, as inclusões de K em G e em G'.*

Demonstração. Primeiramente, suponhamos que G e G' são equivalentes. Existem portanto cociclos $f, f' : Q \times Q \longrightarrow K$ induzidos respectivamente por transversais l e l', com $l(1) = l'(1) = 0$, e uma função $h : Q \longrightarrow K$, com $h(1) = 0$, tal que

$$f(x, y) - f'(x, y) = x \cdot h(y) - h(xy) + h(x), \text{ para quaisquer } x, y \in Q. \qquad (*)$$

Cada elemento de G tem uma única expressão da forma $g = a + l(x)$, onde $a \in K$ e $x \in Q$ (pela Observação 3.3). Note que a adição em G é dada por

$$[a + l(x)] + [b + l(y)] = a + (l(x) + b - l(x)) + (l(x) + l(y)) =$$

$$= a + x \cdot b + f(x, y) + l(xy)$$

onde $a, b \in K$ e $x, y \in Q$. Uma descrição análoga pode ser feita para a adição de G'. Defina então a aplicação

$$\begin{array}{rccl} \varphi: & G & \longrightarrow & G' \\ & a + l(x) & \longmapsto & \varphi(a + l(x)) = a + h(x) + l'(x). \end{array}$$

Note que, como $l(1) = l'(1) = h(1) = 0$, temos

$$\varphi(a) = \varphi(a + l(1)) = a + h(1) + l'(1) = a, \text{ para todo } a \in K \qquad (3.4.6)$$

de onde φ fixa todo elemento de K. Ainda, para todo $g = a + l(x) \in G$, tem-se

$$x = 1x = 1\pi(l(x)) = \pi(a)\pi(l(x)) = \pi(a + l(x)) \qquad (3.4.7)$$

e

$$\pi'(\varphi(a + l(x))) = \pi'(a + h(x) + l'(x)) = \pi'(l'(x)) = x. \qquad (3.4.8)$$

As observações (3.4.6), (3.4.7) e (3.4.8) mostram que o diagrama comuta, pois:

- De (3.4.7), concluímos que

$$i'(a) = a = \varphi(a) = (\varphi \circ i)(a)$$

e portanto $i' = \varphi \circ i$;

- De (3.4.7) e (3.4.8), temos

$$\pi(g) = \pi(a + l(x)) = x = \pi'(\varphi(a + l(x)) = (\pi' \circ \varphi)(g)$$

e assim $\pi = \pi' \circ \varphi$.

Basta agora mostrar que φ é um homomorfismo. Temos

$$\varphi([a + l(x)] + [b + l(y)]) = \varphi([a + x \cdot b + f(x, y)] + l(xy)) =$$

$$= a + x \cdot b + f(x, y) + h(xy) + l'(xy)$$

enquanto

$$\varphi(a + l(x)) + \varphi(b + l(y)) = a + h(x) + l'(x) + b + h(y) + l'(y) =$$

$$= a + h(x) + x \cdot b + x \cdot h(y) + f'(x, y) + l'(xy) =$$

$$= a + h(x) + x \cdot b + x \cdot h(y) + f(x,y) - x \cdot h(y) + h(xy) - h(x) + l'(xy) =$$
$$= a + x \cdot b + f(x,y) + h(xy) + l'(xy)$$

e portanto φ é um homomorfismo.

Reciprocamente, suponhamos que existe um homomorfismo φ que faz o diagrama (3.4.5) comutar. A comutatividade do diagrama nos dá

$$\varphi(a) = a, \text{ para todo } a \in K \tag{3.4.9}$$

e

$$x = \pi(l(x)) = \pi'(\varphi(l(x))), \text{ para todo } x \in Q. \tag{3.4.10}$$

Pela equação (3.4.10), sendo l um transversal para π, temos que $\varphi \circ l$ é um transversal para π'. Ademais, sendo f o cociclo determinado por l, como

$$l(x) + l(y) = f(x,y) + l(xy)$$

temos

$$(\varphi \circ l)(x) + (\varphi \circ l)(y) = (\varphi \circ f)(x,y) + (\varphi \circ l)(xy)$$

de onde $\varphi \circ f$ é o cociclo de G' determinado pelo transversal $\varphi \circ l$. Mas, como $f(x,y) \in K$, temos, pela equação (3.4.9),

$$f(x,y) = (\varphi \circ f)(x,y), \text{ para quaisquer } x, y \in Q$$

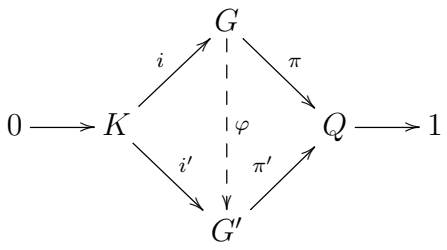
e portanto

$$f - (\varphi \circ f) = 0 \in B^2(Q, K, \theta).$$

Concluímos então que G e G' são equivalentes, o conclui a demonstração do teorema. □

Mostraremos, usando o resultado anterior, que duas extensões equivalentes são, necessariamente, isomorfas.

Proposição 3.2. *Um homomorfismo φ fazendo comutar o diagrama*



é necessariamente um isomorfismo.

Demonstração. Seja $g \in Ker(\varphi)$. Temos

$$\pi(g) = \pi'(\varphi(g)) = \pi'(0) = 1$$

e portanto g pertence a $ker(\pi) = K$. Conforme argumentado em (3.4.9), durante a demonstração do Teorema 3.6, uma função φ nessas condições deve fixar todo ponto de K. Logo,

$$g = \varphi(g) = 0$$

e assim $Ker(\varphi) = 0$, de onde φ é uma função injetiva.

Para argumentar a sobrejetividade, tomemos $g' \in G'$. Pela sobrejetividade de π, existe $g \in G$ tal que

$$\pi(g) = \pi'(g').$$

Mas, pela comutatividade do diagrama, temos $\pi(g) = \pi'(\varphi(g))$, e assim $\pi'(\varphi(g)) = \pi'(g')$, o que nos dá $(g' - \varphi(g)) \in ker(\pi') = K$. Como φ fixa todo elemento de K, temos $\varphi(g' - \varphi(g)) = g' - \varphi(g)$, e daí $\varphi(g' - \varphi(g) + g) = g'$. Concluímos então que φ é sobrejetiva e, portanto, é um isomorfismo. □

Observação 3.11. *Em momento algum da demonstração da proposição anterior foi usado o fato de que K é abeliano.*

Corolário 3.7. *Duas extensões equivalentes são isomorfas.*

Corolário 3.8. *Se G é uma extensão realizando a data (Q, K, θ) e G possui um cociclo f tal que $f \in B^2(Q, K, \theta)$, então G é um produto semidireto.*

Demonstração. Nessas condições, $f - 0$ é um cobordo, e como $0 : Q \times Q \longrightarrow K$ é um cociclo do produto semidireto $K \rtimes_\theta Q$, então G é equivalente ao produto semidireto $K \rtimes_\theta Q$. Pelo corolário anterior, G é isomorfo a $K \rtimes_\theta Q$. □

3.4.5 O Teorema de Schreier

O teorema a seguir resume os resultados sobre extensões de núcleo abeliano.

Teorema 3.9. ***(Teorema de Schreier)*** *Existe uma bijeção de $H^2(Q, K, \theta)$ no conjunto E de todas as classes de equivalência de extensões (conforme a Definição 3.9) realizando a data (Q, K, θ) que leva o elemento neutro na classe dos produtos semidiretos.*

Demonstração. Denote a classe de equivalência de uma extensão G realizando a data (Q, K, θ) por $[G]$, e defina a aplicação

$$\begin{array}{rccl} \varphi : & H^2(Q,K,\theta) & \longrightarrow & E \\ & f + B^2(Q,K,\theta) & \longmapsto & \varphi(f + B^2(Q,K,\theta)) = [G_f] \end{array}$$

onde G_f é a extensão construída no Teorema 3.3.

Primeiramente, φ é bem definida, pois se f e g são cociclos com $f + B^2(Q, K, \theta) = g + B^2(Q, K, \theta)$, então $(f - g) \in B^2(Q, K, \theta)$ e, portanto, G_f e G_g são equivalentes.

Ainda, φ é injetiva, pois se $\varphi(f + B^2(Q, K, \theta)) = \varphi(g + B^2(Q, K, \theta))$, isto é, $[G_f] = [G_g]$, então $(f - g) \in B^2(Q, K, \theta)$, e assim $f + B^2(Q, K, \theta) = g + B^2(Q, K, \theta)$.

Finalmente, se $[G] \in E$, basta tomar um cociclo f de G para termos $[G] = [G_f] = \varphi(f + B^2(Q, K, \theta))$. Assim, φ é sobrejetiva, e portanto uma bijeção. É imediato que $\varphi(0 + B^2(Q, K, \theta))$ é a classe dos produtos semidiretos. □

Observação 3.12. *É possível usar a aplicação φ construída na demonstração anterior para induzir uma estrutura de grupo em E, fazendo de φ um isomorfismo.*

3.5 Produto fibrado e extensões com núcleo de centro trivial

Nessa seção, caracterizaremos as extensões G de K por Q cujo núcleo K tem centro trivial. Para tal caracterização, usaremos a construção do produto fibrado.

3.5.1 Produto fibrado

Definição 3.12. Sejam H, K, L três grupos e $f : H \longrightarrow L$, $g : K \longrightarrow L$ dois homomorfismos de grupos. Definimos o **produto fibrado** de H por K como sendo o subgrupo $H \times_L K$ do produto direto $H \times K$ tal que

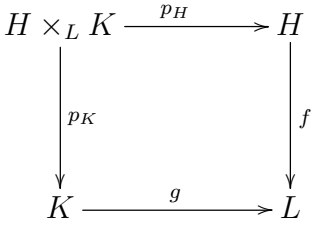
$$H \times_L K = \{(h, k) \in H \times K; f(h) = g(k)\}.$$

Na discussão que segue, H, K, L são três grupos e $f : H \longrightarrow L$, $g : K \longrightarrow L$ dois homomorfismos de grupos.

Primeiramente, mostraremos que $H \times_L K$ é de fato um subgrupo do produto direto $H \times K$. Uma vez que f e g são homomorfismos, temos $(e_H, e_K) \in H \times_L K$. Ainda, sendo $(h_1, k_1), (h_2, k_2) \in H \times_L K$, temos $f(h_1) = g(k_1)$ e $f(h_2) = g(k_2)$, e daí $f(h_1)f(h_2)^{-1} = g(k_1)g(k_2)^{-1}$, ou seja, $f(h_1h_2^{-1}) = g(k_1k_2^{-1})$, de onde $(h_1h_2^{-1}, k_1k_2^{-1}) = (h_1, k_1)(h_2, k_2)^{-1} \in H \times_L K$, e assim $H \times_L K$ é, de fato, um subgrupo de $H \times K$.

Proposição 3.3. *As projeções $p_H : H \times_L K \longrightarrow H$ e $p_K : H \times_L K \longrightarrow K$, ou seja, $p_H(h, k) = h$ e $p_K(h, k) = k$, para qualquer $(h, k) \in H \times_L K$, fazem*

comutar o diagrama:

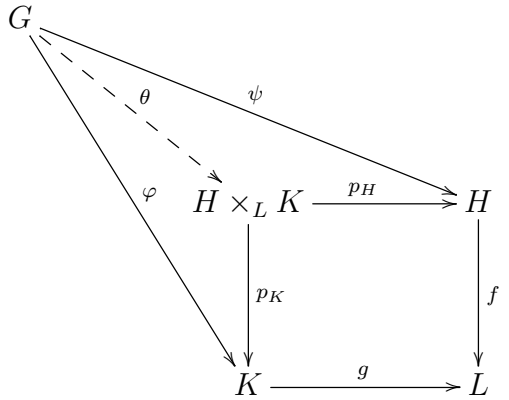


Demonstração. Basta observar que, para todo $(h, k) \in H \times_L K$,

$$g(p_K(h, k)) = g(k) = f(h) = f(p_H(h, k)).$$

□

Proposição 3.4. *O produto fibrado $H \times_L K$ é o único grupo satisfazendo a seguinte propriedade universal: se G é um grupo e $\psi : G \longrightarrow H$, $\varphi : G \longrightarrow K$ são homomorfismos tais que $f \circ \psi = g \circ \varphi$, então existe um único homomorfismo $\theta : G \longrightarrow H \times_L K$ tal que $p_H \circ \theta = \psi$ e $p_K \circ \theta = \varphi$, isto é, faz comutar o diagrama:*



Demonstração. **Demonstração de que o produto fibrado satisfaz a propriedade universal:** dados G um grupo e $\psi : G \longrightarrow H$, $\varphi : G \longrightarrow K$ homomorfismos tais que $f \circ \psi = g \circ \varphi$, definamos $\theta : G \longrightarrow H \times_L K$ como $\theta(x) = (\psi(x), \varphi(x))$. Tal aplicação está bem definida pelo fato de $(f \circ \psi)(x) = (g \circ \varphi)(x)$. Observe que $p_H \circ \theta = \psi$ e $p_K \circ \theta = \varphi$. Caso

$$\begin{array}{rccl} \gamma : & G & \longrightarrow & H \times_L K \\ & x & \longmapsto & \gamma(x) = (\gamma_1(x), \gamma_2(x)) \end{array}$$

seja um homomorfismo tal que $p_H \circ \gamma = \psi$ e $p_K \circ \gamma = \varphi$, temos

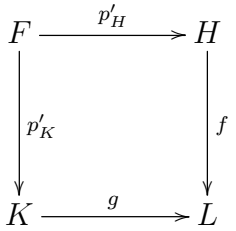
$$\psi(x) = (p_H \circ \gamma)(x) = p_H(\gamma(x)) = p_H(\gamma_1(x), \gamma_2(x)) = \gamma_1(x),$$

e

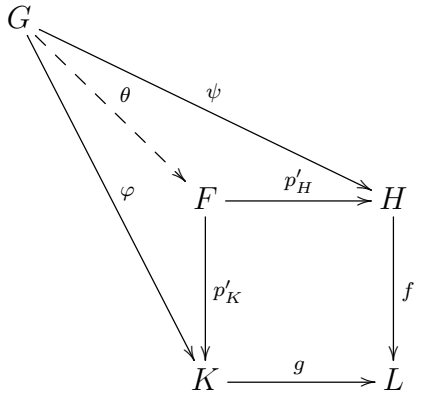
$$\varphi(x) = (p_K \circ \gamma)(x) = p_K(\gamma(x)) = p_K(\gamma_1(x), \gamma_2(x)) = \gamma_2(x)$$

de onde $\gamma(x) = (\psi(x), \varphi(x)) = \theta(x)$, mostrando a unicidade de θ.

Demonstração da unicidade do grupo e dos homomorfismos que satisfazem a propriedade universal: Suponha F um grupo e $p'_H : F \longrightarrow H$, $p'_K : F \longrightarrow K$ homomorfismos tais que $f \circ p'_H = g \circ p'_K$, isto é, tais que o seguinte digrama é comutativo



Suponha ainda que F, p'_H, p'_K satisfazem a seguinte propriedade universal: dados G um grupo e $\psi : G \longrightarrow H$, $\varphi : G \longrightarrow K$ homomorfismos tais que $f \circ \psi = g \circ \varphi$, então existe um único homomorfismo $\theta : G \longrightarrow F$ tal que $p'_H \circ \theta = \psi$ e $p'_K \circ \theta = \varphi$, isto é, que faz comutar o diagrama:



Como $H \times_L K$, p_H e p_K satisfazem as hipóteses da propriedade universal, existe um único homomorfismo $\theta_1 : H \times_L K \longrightarrow F$ tal que

$$p'_H \circ \theta_1 = p_H \quad e \quad p'_K \circ \theta_1 = p_K$$

Ainda, como $H \times_L K$ satisfaz a propriedade universal, existe um único homomorfismo $\theta_2 : F \longrightarrow H \times_L K$ tal que

$$p_H \circ \theta_2 = p'_H \quad \text{e} \quad p_K \circ \theta_2 = p'_K.$$

Compondo as relações convenientemente, obtemos:

$$p'_H \circ (\theta_1 \circ \theta_2) = p'_H \quad \text{e} \quad p'_K \circ (\theta_1 \circ \theta_2) = p'_K \qquad (I)$$

$$p_H \circ (\theta_2 \circ \theta_1) = p_H \quad \text{e} \quad p_K \circ (\theta_2 \circ \theta_1) = p_K \qquad (II)$$

Mas como as funções Id_F e $Id_{H \times_L K}$ também satisfazem (I) e (II), respectivamente, pela unicidade de θ descrita na propriedade universal, temos

$$\theta_1 \circ \theta_2 = Id_F \quad \text{e} \quad \theta_2 \circ \theta_1 = Id_{H \times_L K}$$

de onde $F \simeq H \times_L K$. □

3.5.2 Extensões com núcleo de centro trivial

Dada a sequência exata

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi'} Q \longrightarrow 1$$

onde i é a aplicação inclusão, e cujo homomorfismo associado é $\theta : Q \longrightarrow Out(K)$, onde $\theta(x) = \psi_{l(x)} Inn(K)$, conforme o Teorema 3.1, com $l : Q \longrightarrow G$ uma função transversal arbitrária de π', temos que é comutativo o diagrama

$$\begin{array}{ccc} G & \xrightarrow{\psi} & Aut(K) \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ Q & \xrightarrow{\theta} & Out(K) \end{array}$$

onde $\psi(g) = \psi_g \in Aut(K)$ é tal que $\psi_g(a) = gag^{-1}$, e $\pi : Aut(K) \longrightarrow Out(K)$ é a projeção canônica $\pi(\phi) = \phi Inn(K)$. Com efeito,

$$\theta(\pi'(g)) = \psi_{l(\pi'(g))} Inn(K)$$

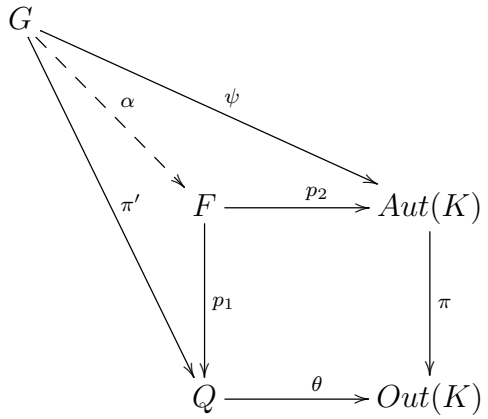
e

$$\pi(\psi(g)) = \psi_g Inn(K)$$

Mas uma vez que $\pi'(l(\pi'(g))g^{-1}) = \pi'(l(\pi'(g)))\pi'(g^{-1}) = \pi'(g)\pi'(g^{-1})$, temos $l(\pi'(g))g^{-1} \in Ker(\pi') = K$, e assim, $\psi_g Inn(K) = \psi_{l(\pi'(g))} Inn(K)$, o que mostra que o diagrama comuta. Considerando agora o produto fibrado

$$F = Q \times_{Out(K)} Aut(K) = \{(x, \varphi) \in Q \times Aut(K); \theta(x) = \pi(\varphi)\}$$

conforme visto na subseção anterior, existe um único homomorfismo $\alpha : G \longrightarrow F$ fazendo comutar o diagrama:



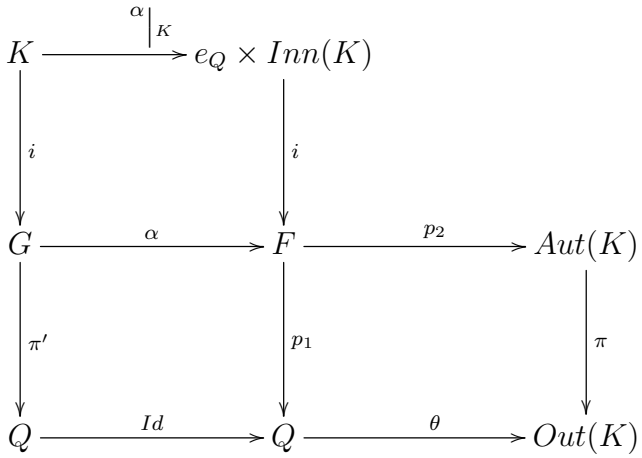
onde $p_1(x, \varphi) = x$ e $p_2(x, \varphi) = \varphi$, para todo $(x, \varphi) \in F$. O homomorfismo α é definido como

$$\alpha(g) = (\pi'(g), \psi(g)) = (\pi'(g), \psi_g). \tag{3.5.1}$$

Note ainda que

$$\begin{aligned} Ker(p_1) &= \{(x, \varphi) \in F; x = e_Q\} = \\ &= \{(e_Q, \varphi) \in Q \times Aut(K); \varphi Inn(K) = \theta(e_Q) = Inn(K)\} = \\ &= \{(e_Q, \varphi) \in Q \times Aut(K); \varphi \in Inn(K)\} = e_Q \times Inn(K). \end{aligned} \tag{3.5.2}$$

Podemos então construir o diagrama:



Tal diagrama é comutativo. Com efeito, do diagrama anterior:

$$\pi \circ p_2 = \theta \circ p_1 \quad \text{e} \quad p_1 \circ \alpha = \pi'. \tag{3.5.3}$$

Basta agora observar que $\alpha \circ i$ e $\alpha\big|_K$ são duas maneiras diferentes de se escrever o mesmo objeto.

Suponhamos agora que $Z(K) = 1$. Nesse caso, o homomorfismo $\psi : K \longrightarrow Aut(K)$ tal que $\psi(a) = \psi_a$ mostra que $K \simeq \dfrac{K}{Z(K)} \simeq Inn(K)$. Assim, $e_Q \times Inn(K) \simeq K$, e portanto podemos escrever o diagrama anterior como

$$\begin{array}{ccccc}
K & \xrightarrow{Id} & K & & \\
\downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \alpha\big|_K} & & \\
G & \xrightarrow{\alpha} & F & \xrightarrow{p_2} & Aut(K) \\
\downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle \pi} \\
Q & \xrightarrow{Id} & Q & \xrightarrow{\theta} & Out(K)
\end{array}$$

Com tais considerações, demonstraremos:

Teorema 3.10. *Considere a sequência exata*

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

com o homomorfismo associado $\theta : Q \longrightarrow Out(K)$, e suponha $Z(K) = 1$. Então, G é isomorfo a $F = Q \times_{Out(K)} Aut(K)$.

Demonstração. Conforme a discussão anterior, $l : Q \longrightarrow G$ é um transversal de π', $\pi : Aut(K) \longrightarrow Out(K)$ é a projeção canônica e $\alpha : G \longrightarrow F$ é a função definida em (3.5.1). Mostremos primeiramente que a sequência

$$1 \longrightarrow K \xrightarrow{\alpha\big|_K} F \xrightarrow{p_1} Q \longrightarrow 1$$

é exata. Temos:

$$a \in Ker(\alpha) \cap K \implies (\pi'(a), \psi_a) = \alpha(k) = (e_Q, Id) \implies$$

$$\implies Id = \psi_a \implies a \in Z(K) = 1.$$

de onde $\alpha\big|_K$ é injetiva. Ainda, conforme discutido em (3.5.2), temos $Ker(p_1) = e_K \times Inn(K)$, e por sua vez

$$Im(\alpha\big|_K) = \{(\pi'(a), \psi_a) \in F; a \in K\} =$$

$$= \{(e_K, \psi_a) \in F; a \in K\} = e_K \times Inn(K)$$

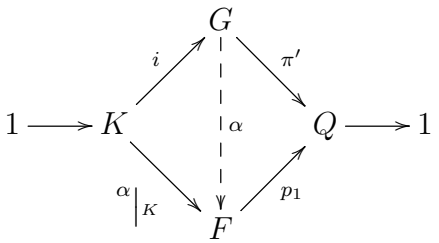
o que mostra que $Ker(p_1) = Im(\alpha_{\big|_K})$. Ademais, sendo $x \in Q$, temos que $x = \pi'(g)$, para algum $g \in G$. Uma vez que

$$\theta(\pi'(g)) = \psi_{l(\pi'(g))} Inn(K) = \pi(\psi_{l(\pi'(g))})$$

isto é, $\pi'(g)$ e $\psi_{l(\pi'(g))}$ têm a mesma imagem por θ e π, respectivamente, temos que $(\pi'(g), \psi_{l(\pi'(g))}) \in F$. Concluímos que

$$x = \pi'(g) = p_1(\pi'(g), \psi_{l(\pi'(g))}) \in Im(p_1)$$

e portanto p_1 é sobrejetiva, mostrando que a sequência descrita é exata. Obtemos então o diagrama



que, por virtude das equações (3.5.3), é comutativo. Conforme visto na Proposição 3.2, um homomorfismo fazendo tal diagrama comutar é necessariamente um isomorfismo, o que conclui a discussão. □

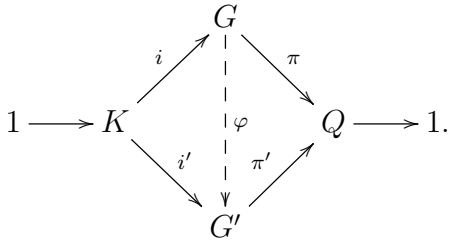
Observação 3.13. *Define-se equivalência entre extensões de núcleo qualquer da seguinte forma: duas extensões*

$$1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

e

$$1 \longrightarrow K \xrightarrow{i'} G' \xrightarrow{\pi'} Q \longrightarrow 1$$

são ditas equivalentes se existe um homomorfismo φ fazendo o seguinte diagrama comutar:



Tal definição faz sentido com a definição de equivalência de extensões de núcleo abeliano. Com essa linguagem, o teorema anterior diz que toda extensão de núcleo com centro trivial e homomorfismo associado $\theta : Q \longrightarrow Out(K)$ é equivalente a $F = Q \times_{Out(K)} Aut(K)$

3.6 Produto Entrelaçado e o Teorema de Kaloujnine-Krasner

Na discussão que segue, D e Q são grupos, Ω é um conjunto e

$$\begin{array}{rccc} \rho: & Q\times\Omega & \longrightarrow & \Omega \\ & (q,\omega) & \longmapsto & q\cdot\omega \end{array}$$

é uma ação de Q em Ω. Definimos o grupo K como sendo o conjunto $K = \{\sigma : \Omega \longrightarrow D\}$ de todas as funções de Ω em D munido da operação de D, ponto a ponto, isto é, para $\sigma, \tau \in K$, temos

$$\sigma\tau(\omega) = \sigma(\omega)\tau(\omega), \text{ para todo } \omega \in \Omega. \tag{3.6.1}$$

Proposição 3.5. *A ação de Q em Ω define um homomorfismo*

$$\begin{array}{rccc} \theta: & Q & \longrightarrow & Aut(K) \\ & q & \longmapsto & \theta(q) = \theta_q \end{array}$$

onde

$$\theta_q(\tau)(\omega) = \tau(q^{-1}\cdot\omega), \text{ para } q \in Q\, \tau \in K \text{ e } \omega \in \Omega. \tag{3.6.2}$$

Demonstração. Mostremos primeiramente que θ está bem definida, isto é, θ_q é um automorfismo de K. Para tal, sejam $\sigma, \tau \in K$. Temos

$$\theta_q(\sigma\tau)(\omega) = (\sigma\tau)(q^{-1}\cdot\omega) = \sigma(q^{-1}\cdot\omega)\tau(q^{-1}\cdot\omega) =$$

$$= \theta_q(\sigma)(\omega)\theta_q(\tau)(\omega) = (\theta_q(\sigma)\theta_q(\tau))(\omega)$$

para todo $\omega \in \Omega$. Assim, temos $\theta_q(\sigma\tau) = \theta_q(\sigma), \theta_q(\tau)$, de onde θ_q é um homomorfismo. Quanto à injetividade, sendo $\sigma, \tau \in K$ tais que $\theta_q(\sigma) = \theta_q(\tau)$, segue que $\theta_q(\sigma)(q\cdot\omega) = \theta_q(\tau)(q\cdot\omega)$, e assim $\sigma(q^{-1}\cdot(q\cdot\omega)) = \tau(q^{-1}\cdot(q\cdot\omega))$, de onde $\sigma((q^{-1}q)\cdot\omega)) = \tau((q^{-1}q)\cdot\omega)$, e portanto $\sigma(1\cdot\omega) = \tau(1\cdot\omega)$, para todo $\omega \in \Omega$, o que mostra que $\sigma = \tau$. Assim, θ_q é injetiva. Sendo então $\sigma \in K$, observe que $\theta_{q^{-1}}(\sigma) \in K$ e

$$\theta_q(\theta_{q^{-1}}(\sigma))(\omega) = \theta_{q^{-1}}(\sigma)(q^{-1}\cdot\omega) = \sigma(q\cdot(q^{-1}\cdot\omega)) = \sigma(\omega),$$

para qualquer $\omega \in \Omega$, o que mostra a sobrejetividade de θ_q, e portanto a boa definição da função θ.

Mostremos agora que θ é um homomorfismo. Para isso, sendo $q_1, q_2 \in Q$, temos

$$\theta_{q_1q_2}(\sigma)(\omega) = \sigma((q_1q_2)^{-1}\cdot\omega) = \sigma((q_2^{-1}q_1^{-1})\cdot\omega) = \sigma(q_2^{-1}\cdot(q_1^{-1}\cdot\omega))) =$$

$$= \theta_{q_2}(\sigma)(q_1^{-1} \cdot \omega) = (\theta_{q_1} \circ \theta_{q_2})(\sigma)(\omega)$$

para quaisquer $\sigma \in K$ e $\omega \in \Omega$, e portanto $\theta_{q_1 q_2} = \theta_{q_1} \circ \theta_{q_2}$. Assim, θ é um homomorfismo.

□

Nas condições da Proposição 3.5, denotamos $\theta_q(\tau) := \tau^q$.

Definição 3.13. Sejam D e Q grupos, Ω um conjunto finito, $\rho : Q \times \Omega \longrightarrow \Omega$ uma ação de Q em Ω e $K = \{\sigma : \Omega \longrightarrow D\}$ munido da operação de D, ponto a ponto, conforme definido na Equação (3.6.1). Definimos o **produto entrelaçado** de D por Q, denotado por $D \wr_\Omega Q$, como sendo o produto semidireto de K por Q realizando o homomorfismo

$$\begin{array}{rccc} \theta : & Q & \longrightarrow & Aut(K) \\ & q & \longmapsto & \theta(q) = \theta_q, \end{array}$$

conforme definido na Equação (3.6.2). A operação de $D \wr_\Omega Q$ é, então, da forma

$$(\sigma, q)(\tau, q') = (\sigma\tau^q, qq').$$

No caso em que $\Omega = Q$ e Q age em $\Omega = Q$ pela multiplicação à esquerda, dizemos que $D \wr_\Omega Q$ é o **produto entrelaçado regular**, denotado por $D \wr_r Q$.

Observação 3.14. *Supondo $|\Omega| = n$, o grupo K pode ser visto como o conjunto das n-uplas $(d_\omega)_{\omega \in \Omega}$, de entradas em D e operação coordenada a coordenada. Nesse caso, o homomorfismo θ é visto como*

$$q \cdot (d_\omega)_{\omega \in \Omega} := \theta_q((d_\omega)_{\omega \in \Omega}) = (d_{q^{-1} \cdot \omega})_{\omega \in \Omega}$$

O exemplo a seguir segue essa notação, que muitas vezes pode ser mais simples de se trabalhar.

Exemplo 3.10. *Temos $G = \mathbb{Z}_2 \wr_r \mathbb{Z}_2 \simeq D_8$. Usando a notação descrita na observação acima, podemos ver K como $\mathbb{Z}_2 \times \mathbb{Z}_2$, e assim*

$$G = \mathbb{Z}_2 \wr_r \mathbb{Z}_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\varphi \mathbb{Z}_2$$

onde $\varphi : \mathbb{Z}_2 \longrightarrow Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ é o homomorfismo tal que $\varphi(\overline{1}) = f$, onde f é dado por $f(x, y) = (y, x)$. Sendo $a = ((\overline{1}, \overline{0}), \overline{1})$ e $b = ((\overline{0}, \overline{0}), \overline{1})$, temos que as ordens de a e b são $\circ(a) = 4$ e $\circ(b) = 2$. Além disso, $\langle a \rangle \trianglelefteq G$, uma vez que tal subgrupo que tem índice 2 (ver Exemplo 1.17), e $\langle a \rangle \cap \langle b \rangle = ((\overline{0}, \overline{0}), \overline{0})$, e pelas ordens dos subgrupos (ver Exemplo 1.12), temos $\langle a \rangle \langle b \rangle = G$. Concluímos então que $G = \langle a \rangle \rtimes \langle b \rangle$. Ainda,

$$b^{-1}ab = bab = ((\overline{0}, \overline{0}), \overline{1})((\overline{1}, \overline{0}), \overline{1})((\overline{0}, \overline{0}), \overline{1}) =$$

$$((\overline{0},\overline{1}),\overline{0})((\overline{1},\overline{0}),\overline{1}) = ((\overline{0},\overline{1}),\overline{1}) = a^{-1}$$

de onde $\langle a\rangle \rtimes \langle b\rangle$ *realiza* $\theta : \langle b\rangle \longrightarrow Aut\langle a\rangle$ *tal que* $\theta_b(a) = a^{-1}$. *Portanto, pelo Exemplo 2.5,* G *é o grupo diedral de* $|\langle a\rangle||\langle b\rangle| = 8$ *elementos.*

Teorema 3.11. ***(Kaloujnine-Krasner, 1951)*** *Se* D *e* Q *são grupos e* Q *é finito, então o produto entrelaçado regular* $D \wr_r Q$ *contém uma cópia isomórfica de cada extensão de* D *por* Q.

Demonstração. Considerando a extensão

$$1 \longrightarrow D \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

e tome $l : Q \longrightarrow G$ um transversal de π. Para cada $a \in G$, defina $\sigma_a : Q \longrightarrow D$ da seguinte forma

$$\sigma_a(x) = l(x)^{-1}al(\pi(a^{-1})x), \text{ para } x \in Q$$

A boa definição de tal aplicação resulta do fato de que

$$\pi(\sigma_a(x)) = \pi(l(x)^{-1})\pi(a)\pi(l(\pi(a^{-1})x)) = x^{-1}\pi(a)\pi(a)^{-1}x = 1$$

isto é, $\sigma_a(x) \in Ker(\pi) = D$, para todo $x \in Q$. Sendo $a, b \in G$, temos

$$\sigma_a(x)\sigma_b^{\pi(a)}(x) = \sigma_a(x)\sigma_b(\pi(a^{-1})x) =$$

$$= l(x)^{-1}al(\pi(a^{-1})x)l(\pi(a^{-1})x)^{-1}bl(\pi(b^{-1})\pi(a^{-1})x) =$$

$$= l(x)^{-1}abl(\pi((ab)^{-1})x) = \sigma_{ab}(x).$$

Defina então $\varphi : G \longrightarrow D \wr_r Q$ por $\varphi(a) = (\sigma_a, \pi(a))$, para $a \in G$. Temos que φ é um homomorfismo, pois

$$\varphi(a)\varphi(b) = (\sigma_a, \pi(a))(\sigma_b, \pi(b)) = (\sigma_a\sigma_b^{\pi(a)}, \pi(a)\pi(b)) = (\sigma_{ab}, \pi(ab)).$$

Ademais, φ é injetiva, pois se $a \in Ker(\varphi)$, então $\pi(a) = 1$ e $\sigma_a(x) = 1$, para todo $x \in Q$. Logo,

$$1 = \sigma_a(x) = l(x)^{-1}al(\pi(a^{-1})x) = l(x)^{-1}al(x)$$

e daí, $a = 1$, o que mostra o resultado. □

Referências Bibliográficas

[1] FRALEIGH, J. B. *A First Course in Abstract Algebra*. 6ª Edição. New York: Addison-Wesley, 2000.

[2] GARCIA, A, LEQUAIN, Y. *Elementos de Álgebra*. 4ª Edição. Rio de Janeiro: Projeto Euclides, IMPA, 1999.

[3] GONÇALVES, A. *Introdução à Álgebra*. 2ª Edição. Rio de Janeiro: Projeto Euclides, IMPA, 2003.

[4] MARTIN, P. A. *Grupos, Corpos e Teoria de Galois*. São Paulo: Editora Livraria da Física, 2010.

[5] ROBINSON, D. J. S. *A Course in the Theory of Groups*. New York: Springer-Verlag, 1995.

[6] ROTMAN, J. J. *An Introduction to the Theory of Groups*. 4ª Edição. New York: Springer-Verlag, 1994.

[7] ROTMAN, J. J. *An Introduction to the Homological Algebra*. 2ª Edição. New York: Springer-Verlag, 2009.

[8] VIEIRA, V. L. *Álgebra Abstrata para Licenciatura*. Campina Grande: EDUEPB, 2013.