UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
(Mestrado)

Grupos de Automorfismos Abelianos com um Número Finito de Órbitas

ALEX CARRAZEDO DANTAS

Orientadora: Irene Naomi Nakaoka

Maringá - PR

2012

Grupos de Automorfismos Abelianos com um Número Finito de Órbitas

ALEX CARRAZEDO DANTAS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.
Área de concentração: Álgebra

Orientadora: Profª. Drª. Irene Naomi Nakaoka

Maringá - PR

2012

Grupos de Automorfismos Abelianos com um Número Finito de Órbitas

Alex Carrazedo Dantas

Dissertação submetida ao corpo docente do Programa de Pós-Graduação em Matemática da Universidade Estadual de Maringá - UEM-PR, como parte dos requisitos necessários à obtenção do grau de Mestre.

Aprovada por:

Prof[a]. Dr[a]. Irene Naomi Nakaoka - UEM ....
(Orientadora)

Prof. Dr. Noraí Romeu Rocco - UnB ....

Prof. Dr. Ednei Aparecido Santulo Júnior - UEM ....

Maringá - PR

2012

À minha mãe Irene Carrazedo Dantas.

Agradecimentos

Primeiramente, quero agradecer à minha família, citando meus irmãos Sandro, Sérgio, o qual é um grande companheiro nessa caminhada, Márcio, Márcia e Marcos, para este último não há palavras para expressar o quanto sou grato, meu pai Manoel Macedo Dantas e em especial minha mãe Irene Carrazedo Dantas, que me pôs no caminho da pessoa que sou, que sempre acreditou em mim e que é a base dessa grande família.

Agradeço à minha namorada Camila, que está sempre comigo, que me apoia em momentos bons e ruins e que tem sido uma grande companheira. Agradeço ao professor Aldevino que me auxiliou com moradia durante um ano e cujos conselhos foram de grande valia.

Aos meus amigos de graduação e correlatos Diego, Vitor, Priscila e Lucas, que são nas palavras do Diego "sensacionais". Aos meus amigos de mestrado Jorge, Thiago (Fera), João (Pantera), Djeison, Vitor, Fausto, Guilherme, Cesar, Thales, Arthur, Cleilton, Carlos, Flávio, Ailton, Anderson, Thiago, João, Stephanie, Rafael e André e a minha amiga Carol. Aos meus amigos de Cambé e Londrina, que não vou citá-los para não esquecer de algum.

Aos meus professores de graduação, em especial ao professor Ulisses Sodré. Aos meus professores de mestrado, que além de grandes mestres foram também grandes amigos. A todos os membros do Departamento de Matemática da UEM.

À minha orientadora Professora Doutora Irene Naomi Nakaoka, cuja especial paciência, sabedoria, compreensão, dedicação e ajuda foram cruciais na elaboração deste trabalho.

À Capes, pelo apoio financeiro.

Resumo

Sejam G um grupo e A um grupo de automorfismos de G. Uma A-órbita de G é um conjunto da forma $g^A = \{g^\alpha; \alpha \in A\}$, com g um elemento de G. Um subgrupo H de G é dito ser A-invariante se $H = H^\alpha$, para todo $\alpha \in A$, e, uma seção H/K de G é dita ser A-invariante se H e K são subgrupos A-invariantes de G. Quando G é infinito, A é abeliano e A centraliza toda seção finita A-invariante de G é dito que o par (G, A) satisfaz a condição $(*)$. O objetivo desta dissertação é demonstrar um resultado, devido a Enrico Jabara, o qual estabelece que se o grupo G é uma união de um número finito de A-órbitas e o par (G, A) satisfaz a condição $(*)$, então G possui um subgrupo abeliano normal de índice finito.

Palavras Chaves: Grupo de automorfismos, grupo de automorfismos abeliano, ação de grupos de automorfismos, órbitas.

Abstract

Let G be a group and A a group of automorphisms of G. An A-orbit of G is a set of the form $g^A = \{g^\alpha;\, \alpha \in A\}$, where g is an element of G. A subgroup H of G is an A-invariant subgroup of G if $H = H^\alpha$, for all α in A and, a section H/K of G is an A-invariant section of G if H and K are A-invariant subgroups of G. When G is an infinite group, A is an abelian group and A centralizes all A-invariant finite section of G, it is said that the pair (G, A) satisfies the condition $(*)$. The main of this dissertation is to prove a result, due to Enrico Jabara, which establishes that if G is a union of a finite number of A-orbits and the pair (G, A) satisfies the condition $(*)$, then G admits a normal abelian subgroup of finite index.

Índice de Notações

$\emptyset$	conjunto vazio
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{N}$	conjunto dos números inteiros não negativos
$\mathbb{Q}$	conjunto dos números racionais
$mdc\{x,y\}$	máximo divisor comum entre x e y
$mmc\{x,y\}$	mínimo múltiplo comum entre x e y
K^+	grupo aditivo do corpo K
$K^\times$	grupo multiplicativo do corpo K
$\|X\|$	cardinalidade do conjunto X
$X\backslash Y$	$\{x \in X;\ x \notin Y\}$
$X \subseteq Y$	X é um subconjunto de Y
$X \subset Y$	X é um subconjunto próprio de Y
$H \leqslant G$	H é um subgrupo do grupo G
$H < G$	H é um subgrupo próprio do grupo G
$H \lhd G$	H é um subgrupo normal de G
$\langle X \rangle$	subgrupo gerado pelo conjunto X
$\|g\|$	$\|\langle g \rangle\|$
$\|G:H\|$	índice do subgrupo H no grupo G
G/N	grupo quociente entre o grupo G e seu subgrupo normal N
$[g,h]$	$g^{-1}h^{-1}gh$
$[G,H]$	$\langle [g,h];\ g \in G, h \in H \rangle$
G'	$[G,G]$
$Z(G)$	centro do grupo G
$\widehat{Z}(G)$	conjunto de todos os FC-elementos do grupo G
$H \times K$	produto direto dos grupos H e K
$Dr_{i\in I}H_i$	produto direto dos grupos H_i's
$H \oplus K$	soma direta dos grupos abelianos H e K
$Im(f)$	imagem da função f

$Nuc(f)$	núcleo da função f
$End(G)$	conjunto de todos os endomorfismos do grupo G
$Aut(G)$	conjunto de todos os automorfismos do grupo G
X_G	o "core" do subconjunto X no grupo G
X^G	fecho normal do subconjunto X no grupo G
$G[n]$	$\{g \in G;\ g^n = 1\}$
G_p	$\bigcup_{n\in\mathbb{N}} G[p^n]$
$N_G(H)$	normalizador do subconjunto X no grupo G
$C_G(X)$	centralizador do subconjunto X no grupo G
$(g)\alpha, g^\alpha$	função α aplicada no elemento g
X^α	$\{x^\alpha; x \in X\}$
g^x	$x^{-1}gx$
g^G	$\{g^x;\ x \in G\}$
α^*	o transfer de α
X^A	$\langle x^\alpha;\ x \in X \text{ e } \alpha \in A\}$
$[g, \alpha]$	$g^{-1}g^\alpha$
$[X, A]$	$\langle [x, \alpha];\ x \in X, \alpha \in A\rangle$
T_α	função associada a α
$\mathcal{L}_A(G)$	conjunto de todos os subgrupos A-invariantes do grupo G
$I_G^A(H)$	$\{K \in \mathcal{L}_A(G);\ K \leqslant H, \lvert H : K\rvert < \infty\}$
$S_G^A(H)$	$\{K \in \mathcal{L}_A(G);\ H \leqslant K, \lvert K : H\rvert < \infty\}$
$min_G^A(H)$	$\bigcap_{K\in I_G^A} K$
$max_G^A(H)$	$\langle K;\ K \in S_G^A\rangle$
$\overline{\mathcal{L}}_A(G)$	$\{max_G^A(H);\ H \in \mathcal{L}_A(G)\}$
$\underline{\mathcal{L}}_A(G)$	$\{min_G^A(H);\ H \in \mathcal{L}_A(G)\}$
$\ell_A(G)$	comprimento de G em realação a A
g^A	$\{g^\alpha;\ \alpha \in A, g \in G \text{ e } A \leqslant Aut(G)\}$
$C_H(A)$	$\{h \in H;\ h^\alpha = h, \forall\alpha \in A\}$
$C_A(H)$	$\{\alpha \in A; h^\alpha = h, \forall h \in H\}$
C_t^n	n-cubo sobre um conjunto com t elementos

Sumário

Introdução

Investigar a estrutura de um grupo G por meio de propriedades de um grupo A de automorfismos de G é comum na Teoria de Grupos. Em verdade, pesquisas nessa linha vêm sendo feitas há mais de um século. Como exemplo de tal fato, W. Burnside (1852 - 1927) demonstra em seu livro *Theory of Groups of Finite Order* (veja [1]), que *se um grupo finito G admite um automorfismo τ de ordem 2 e livre de pontos fixos, isto é, tal que $C_G(\tau) = \{g \in G; g^\tau = g\} = \{1\}$, então G é um grupo abeliano finito de ordem ímpar.* Na mesma situação, mas com τ com ordem 3, Neumann [10], em 1956, mostrou que G é nilpotente. Três anos mais tarde, Thompson [16], generaliza esses resultados mostrando que: *um grupo finito que admite um automorfismo de ordem prima e livre de pontos fixos, é nilpotente.*

Sobre ainda grupos finitos, no caso em que o grupo G é um p-grupo abeliano e o grupo A é um p'-grupo de automorfismos de G, isto é, o primo p não é um divisor da ordem de algum α em $A \backslash Id_G$, é possível escrever G como um produto direto de subgrupos A-invariantes. Em outras palavras, é possível mostrar que: *se p é um número primo e G é um p-grupo abeliano finito que admite um p'-grupo de automorfismos A de G, então $G = C_G(A) \times [G, A]$, onde $C_G(A) = \{g \in G; g^\alpha = g, \forall \alpha \in A\}$ e $[G, A] = \langle [g, \alpha] = g^{-1}g^\alpha; g \in G, \alpha \in A\rangle$.* Mais que isso, pode-se mostrar que: *se p é um número primo e G é um p-grupo finito que admite um p'-grupo de automorfismos A de G, então $G = C_G(A)[G, A]$.*

Quando o grupo G é infinito e o grupo de automorfismos A age sobre G com uma quantidade finita de órbitas, isto é, o grupo G é uma união de um número finito de A-órbitas, alguns resultados sobre a estrutura de G também podem ser obtidos. Por exemplo, em 1998, no artigo intitulado *Free Actions of Abelian Groups on Groups*, os matemáticos Peter M. Neumann e Peter J. Rowley (veja [12]), expõem e demonstram o seguinte teorema:

Teorema. (Neumann-Rowley) *Sejam G um grupo e A um grupo infinito de automorfismos de G livre de pontos fixos. Se G é uma união de um número finito de A-órbitas e A é abeliano, então G é abeliano.*

Tentando impulsionar pesquisas futuras, neste mesmo artigo, eles propõem a seguinte questão: *"O que se pode dizer sobre um grupo G que admite um grupo abeliano A de automorfismos de G tal que G é uma união de um número finito de A-órbitas?"*.

Percorrendo a mesma linha desses autores, Enrico Jabara [8] troca no teorema acima a condição *"A é um grupo abeliano"* pela condição *"A é um FC-grupo"*, isto é, a classe de conjugação de cada um de seus elementos é finita, e detalha um pouco mais a estrutura do grupo G, demonstrando o

Teorema 1. (Jabara) *Sejam G um grupo e A um grupo infinito de automorfismos de G livre de pontos fixos. Se G é uma união de um número finito de A-órbitas e A é um FC-grupo, então G é abeliano e um dos seguintes casos ocorre:*

(*a*) *G é de torção: em tal caso, G é um p-grupo abeliano elementar, para algum primo p;*

(*b*) *G é livre de torção: em tal caso, G é divisível, isto é, para todo elemento g de G e todo inteiro positivo m existe $h \in G$ tal que $g = mh$.*

Em seguida, intencionando responder a questão de Neumann e Rowley, Enrico Jabara, no artigo *Abelian automorphisms groups with a finite number of orbits* (veja [6]), introduz uma condição, chamada por ele de *condição* $(*)$, a qual diz que: *"o par (G, A) satisfaz a condição $(*)$ se G é infinito, A é abeliano e A centraliza toda seção finita A-invariante de G"*, onde uma seção A-invariante de G é um grupo quociente H/K tal que H e K são subgrupos A-invariantes de G. Com essa condição e supondo que o grupo G é abeliano, Jabara mostra que *se G é uma união de um número finito de A-órbitas e o par (G, A) satisfaz a condição $(*)$, então $G = C_G(A) \times [G, A]$*. Utilizando esse resultado e o Teorema 1 ele demonstra o

Teorema B. *Sejam G um grupo abeliano infinito e A um grupo abeliano de automorfismos de G, tal que G é uma união de um número finito de A-órbitas e A centraliza toda seção finita A-invariante de G. Então existem um inteiro positivo r, subgrupos $B_1, ..., B_r$ de A e subgrupos A-invariantes $G_1, ..., G_r$ de G tais que $B = B_1 \times ... \times B_r$ possui índice finito em*

A, $G = C_G(A) \times G_1 \times ... \times G_r$ e

(a) B_i age trivialmente sobre G_j, para todo $i \neq j$, com $i, j = 1, ..., r$;

(b) G_i é um subgrupo B_i-monolítico de G, isto é, existe um único subgrupo B_i-invariante minimal não trivial em G_i, para todo $i = 1, ..., r$.

Além disso, cada G_i ou é um p-grupo de expoente finito, para algum primo p, ou é um grupo livre de torção e divisível.

Utilizando esse último resultado, ele finaliza este artigo demonstrando seu resultado principal, o qual mostra que: *"se um grupo G é uma união de um número finito de A-órbitas, onde A é um grupo abeliano de automorfismos de G e o par (G, A) satisfaz a condição $(*)$, então G possui um subgrupo abeliano normal de índice finito"*. Em outros termos, ele mostra o

Teorema A. (Jabara) *Sejam G um grupo e A um subgrupo abeliano de $Aut(G)$ tais que G é uma união de um número finito de A-órbitas e o par (G, A) satisfaz a condição $(*)$. Então*

(a) G é abeliano-por-finito;

(b) Se G é livre de torção, então G é abeliano e divisível;

(c) Se G é infinito, então G possui expoente infinito.

Assim, é respondida de uma maneira parcial a questão levantada por Peter M. Neumann e Peter J. Rowley.

O objetivo desta dissertação é expor a teoria suficiente para apresentar a demonstração de Jabara desses dois últimos teoremas. Este trabalho foi dividido em quatro capítulos, em que o último vem em forma de apêndice, pois os conceitos abordados em tal capítulo fogem dos conceitos dados na Teoria de Grupos.

No primeiro capítulo são abordados alguns conceitos elementares da Teoria de Grupos, como grupos abelianos e FC-grupos, no qual o resultado de maior impôrtancia é devido a B. H. Neumann e diz que: *"o subgrupo derivado de um grupo G é finito se, e somente se, G é* *um BFC-grupo"*, isto é, um FC-grupo tal que o conjunto das cardinalidades das classes de conjugação de todos os elementos desse grupo é limitado superiormente em $\mathbb{N}$.

No segundo capítulo é estudado mais a fundo a ação de um grupo A de automorfismos de um grupo G sobre G e, então, são obtidos alguns resultados sobre a estrutura do grupo G quando G é uma união de um número finito de A-órbitas.

No Apêndice, cuja função é obter um resultado que é usado somente no Teorema A, é apresentado e demonstrado um teorema de combinatória chamado de *Teorema de Hales-Jewet* e, em seguida, alguns fatos sobre corpos infinitos.

Por fim, o Capítulo 3 é dividido em três seções. A primeira aborda vários fatos sobre um grupo G e um grupo A de automorfismos de G tais que o par (G, A) satisfaz a condição $(*)$ e um de seus resultados principais é um teorema devido a Enrico Jabara que mostra que: *"se um grupo G é uma união de uma quantidade finita de A-órbitas, com $A \leqslant Aut(G)$, e o par (G, A) satisfaz a condição $(*)$, então $[G, A]$ é um BFC-grupo"*. Assim, as duas últimas seções são deixadas exclusivamente para as demonstrações dos Teoremas B e A, respectivamente.

Capítulo 1

Preliminares

Este capítulo tem por objetivo estabelecer os conceitos preliminares para os dois próximos que o seguem. Desta forma, aparecerão aqui, alguns resultados de cursos básicos e avançados em Teoria de Grupos. Foi feito o possível para que esses resultados não lançassem mão de outros que não foram enunciados nessas notas, a não ser, quando o fato faz parte de um curso elementar em Teoria de Grupos. Resultados que não foram demonstrados vêm com a indicação bibliográfica e sua página, onde será possível encontrar sua demonstração.

A Seção 1.1 estabelece os conceitos que serão usados quase que na totalidade dessas notas e enuncia um fato devido ao matemático *B. H. Neumman*, cuja demonstração usa apenas conceitos simples para ser demonstrado. Alguns fatos sobre grupos abelianos livres são tratados na Seção 1.2, os quais não são demonstrados. Esses fatos serão de grande importância na Seção 1.3, a qual trata de grupos abelianos. Na Seção 1.4 é demonstrado o Teorema de Schur, o qual estabelece que se o índice do centro de um grupo é finito, o subgrupo derivado desse grupo é finito. Por fim, a Seção 1.5 estabelece uma grande quantidade de fatos relevantes sobre os grupos com classes de conjugação finitas.

1.1 Alguns Conceitos Básicos da Teoria de Grupos

As seguintes convenções serão usadas no decorrer dessa seção: Letras maiúsculas do alfabeto, como $A, B, C, ..., G, H, K, ...$, serão usadas para designar grupos quaisquer, letras minúsculas do alfabeto, como $a, b, c, ..., g, h, k, ...$, para elementos de grupos. Para conjuntos quaisquer, serão usadas letras maiúsculas do final do alfabeto, como $X, Y, Z, ...$. A cardinalidade de um conjunto X será indicada por $|X|$. A expressão $H \leqslant G$ será usada para dizer que H é um subgrupo de G, a expressão $H < G$, para dizer que H é um subgrupo próprio de G e, a expressão $H \lhd G$, para dizer que H é um subgrupo normal de G.

Dados G um grupo, $g \in G$ e $H \leqslant G$, o conjunto $gH = \{gh;\ h \in H\}$ é a classe lateral à esquerda de H em G que contém g. Analogamente, Hg é a classe lateral à direita de H em G que contém g. É um fato bem conhecido que dado $H \leqslant G$, então G se escreve como uma união disjunta de classes laterais à esquerda de H em G, ou seja, existem um conjunto de índices I e elementos g_i de G, para todo $i \in I$, tais que $G = \biguplus_{i\in I} g_iH$. Analogamente, existe um conjunto de índices J e elementos $h_j \in G$, para todo $j \in J$, tais que $G = \biguplus_{j\in J} Hh_i$. Escolha, para cada $i \in I$, um representate t_i da classe g_iH (isso é possível pelo Axioma da Escolha). Então, o conjunto $T = \{t_i;\ i \in I\}$ é chamado de um *transversal à esquerda* de H em G. Analogamente, define-se um *transversal* U *à direita* de H em G. É bem conhecido que se T e U são transversais à direita e à esquerda de H em G, respectivamente, então $|T| = |U|$. A cardinalidade de um transversal qualquer de H em G, denotado pelo símbolo $|G : H|$, é chamado *índice de* H *em* G. A seguinte proposição será muito usada.

Proposição 1.1. *([14], página 14) Sejam H e K subgrupos de G. Então*

(i) $|HK||H \cap K| = |H||K|$;

(ii) $|G : H \cap K| \leqslant |G : H||G : K|$.

Segue, desta proposição, que a interseção, em uma quantidade finita, de subgrupos de índices finitos é um subgrupo de índice finito.

Seja X um subconjunto não vazio de um grupo G. O *fecho normal* de X em G é a interseção de todos os subgrupos normais de G que contém X. Esse subconjunto de G é um subgrupo normal de G e é denotado por X^G. É fácil mostrar que $X^G = \langle g^{-1}Xg;\ g \in G\rangle$. Dualmente, o *interior normal* ou *"core"* de X em G, denotado por X_G, é o subgrupo gerado por todos os subgrupos normais de G que estão contidos em X, se não existe um tal subgrupo normal contido em X, usa-se a convenção $X_G = \{1\}$.

Proposição 1.2. *([14], página 36) Sejam G um grupo e H um subgrupo de índice finito em G. Então H_G, o "core" de H em G, possui índice finito em G.*

Uma condição suficiente para que um subgrupo de um grupo finitamente gerado seja finitamente gerado é que esse subgrupo tenha índice finito, como é dado pela

Proposição 1.3. *([14], página 36) Se H é um subgrupo de índice finito em um grupo finitamente gerado G, então H é finitamente gerado.*

O matemático B. H. Neumann, no artigo *Groups Covered by Permutable Subsets*, demonstra que se um grupo G é uma união de uma quantidade finita de classes laterais de alguns de seus subgrupos, então pelo menos um desses subgrupos possui índice finito (veja [9]). Nesse mesmo artigo, Neumann diz que, possivelmente, tal resultado já era conhecido, mas que não havia encontrado referências na literatura da época.

Teorema 1.4. (B. H. Neumann) *Sejam G um grupo, $H_1, ..., H_n \leqslant G$ e elementos $g_1, ..., g_n$ de G, tais que $G = \bigcup_{i=1}^{n} g_i H_i$. Então existe $i \in \{1, ..., n\}$, tal que $|G : H_i| \leqslant n$.*

Demonstração. A demonstração será feita em alguns passos.

Afirmação 1: Existe $i \in \{1, ..., n\}$, tal que $|G : H_i| < \infty$.

Essa afirmação será provada por indução sobre o número dos distintos subgrupos entre os subgrupos $H_1, ..., H_n$ de G. Se $H_1 = ... = H_n = H$, tem-se que G é uma união de n classes laterais à esquerda de um único subgrupo H, logo H possui índice finito. Suponha, como hipótese de indução, que a afirmação seja verdadeira quando há no máximo $r - 1$ subgrupos distintos K_i's entre os subgrupos $K_1, ..., K_{n'}$, com n' um inteiro positivo maior ou igual a $r - 1$. Seja, então, r a quantidade máxima de subgrupos distintos entre os subgrupos $H_1, ..., H_n$. Suponha que, rearranjando se necessário, $H_1, ..., H_m$, com $m \leqslant n$, são todos os subgrupos, entre os subgrupos $H_1, ..., H_n$, distintos de H_n, assim $H_{m+1} = H_{m+2} = ... = H_n$. Agora, ou $G = \bigcup_{i=m+1}^{n} g_i H_n$ e, neste caso, H_n possui índice finito em G ou, existe $h \in G$ tal que $h \notin \bigcup_{i=m+1}^{n} g_i H_n$, neste caso, $hH_n \cap \bigcup_{i=m+1}^{n} g_i H_n = \emptyset$. Daí, $hH_n \subseteq \bigcup_{i=1}^{m} g_i H_i$, assim $gH_n \subseteq \bigcup_{i=1}^{m} gh^{-1} g_i H_i$, isto é, cada classe lateral à esquerda de H_n em G está contida em uma união de uma quantidade finita de classes laterais à esquerda de outros $r - 1$ subgrupos H_i's. Com isso, G pode ser escrito na forma

$$G = \bigcup_{i=1}^{m} g_i H_i \cup \bigcup_{j=m+1}^{n} \bigcup_{i=1}^{m} g_j h^{-1} g_i H_i,$$

ou seja, G é uma união de classes laterais à esquerda de no máximo $r-1$ subgrupos distintos entre os subgrupos $H_1, ..., H_m$. Aplicando a hipótese de indução, a afirmação segue.

Afirmação 2: Se $H_1, ..., H_m$ posuem índices infinitos em G e $H_{m+1} = H_{m+2} = ... = H_n$, então vale a igualdade $G = \bigcup_{i=1}^{n} g_i H_i = \bigcup_{i=m+1}^{n} g_i H_n$.

Suponha, por contradição, que $G \neq \bigcup_{i=m+1}^{n} g_i H_n$. Pelo mesmo processo aplicado na afirmação anterior, tem-se que G é uma união de uma quantidade finita de classes laterais dos subgrupos $H_1, ..., H_m$. Logo, pela afirmação *(1)*, algum subgrupo, entre os subgrupos $H_1, ..., H_m$, possui índice finito em G, absurdo.

Afirmação 3: Se $H_1, ..., H_m$ possuem índices infinitos em G, então $G = \bigcup_{i=m+1}^{n} g_i H_i$.

Pela afirmação *(1)*, algum dos subgrupos $H_{m+1}, ..., H_n$ possui índice finito em G. Pode-se assumir, sem perda de generalidade, que todos os subgrupos $H_{m+1}, ..., H_n$ possuem índices finitos em G. Colocando $D = \bigcap_{i=m+1}^{n} H_i$, segue, pela Proposição 1.1, que D possui índice finito em G. Assim, cada H_i, com $i \in \{m+1, m+2, ..., n\}$, pode ser posto na forma $H_i = \bigcup_{j=1}^{n_i} d_{ij} D$, com $d_{ij} \in H_i$, para todos i e j. Logo, $G = \bigcup_{i=1}^{m} g_i H_i \cup \bigcup_{i=m+1}^{n} \bigcup_{j=1}^{n_i} g_i d_{ij} D$. Pela afirmação anterior, as classes laterais dos $H_1, ..., H_m$, na cobertura de G, podem ser omitidas e, com isso, $G = \bigcup_{i=m+1}^{n} \bigcup_{j=1}^{n_i} g_i d_{ij} D = \bigcup_{i=m+1}^{n} g_i H_i$.

Afirmação 4: Existe $i \in \{1, ..., n\}$, tal que $|G : H_i| \leqslant n$.

Pela afirmação *(3)*, pode-se omitir as classes dos subgrupos H_i's de índices infinito na cobertura de G. Assim, rearranjando, se necessário, os índices, pode-se escrever $G = \bigcup_{i=m+1}^{n} g_i H_i$, para algum $m \leqslant n$, com cada H_i de índice finito em G. Denote $D = \bigcap_{i=m+1}^{n} H_i$. Para cada $i \in \{m+1, ..., n\}$, existem $n_i \in \mathbb{N}$ e $d_{ij} \in H_i$, $j = 1, ..., n_i$, tais que $g_i H_i = \bigcup_{j=1}^{n_i} g_i d_{ij} D$, daí, G está contido em uma união de $\sum_{i=m+1}^{n} |H_i : D|$ classes laterais à esquerda de D. Então, $\sum_{i=m+1}^{n} |H_i : D| \geqslant |G : D|$. Isto junto com a identidade $|G : D| = |G : H_i||H_i : D|$, para todo $i \in \{m+1, ..., n\}$, resulta em

$$\sum_{i=m+1}^{n} \frac{1}{|G : H_i|} \geqslant 1,$$

ou seja, pelo menos uma das parcelas $1/|G : H_i|$'s é maior do que ou igual a $1/n$. Portanto, o resultado segue. $\square$

Segue agora um resultado técnico que será somente usado no capítulo 3.

Proposição 1.5. *Sejam G um grupo, $H_1, ..., H_r$ subgrupos normais de índices infinitos em G e $Y = \bigcup_{i=1}^{r} H_i$. Então, existem um número natural $t \leqslant 2^r$ e elementos $g_1, ..., g_t \in G$, com $g_1 = 1$, tais que $\bigcap_{i=1}^{t} g_i Y = \emptyset$ ou, em outros termos, $\bigcup_{i=1}^{t} g_i(G \backslash Y) = G$.*

Demonstração. A demonstração será feita por indução sobre r. Se $r = 1$, tome $t = 2$, $g_1 = 1$ e $g_2 \notin H_1$, assim

$$g_1 Y \cap g_2 Y = H_1 \cap g_2 H_1 = \emptyset$$

e a base da indução fica demonstrada. Agora, se $r > 1$, seja $Y_0 = \bigcup_{i=1}^{r-1} H_i$. Observe que $Y_0 \subseteq Y \neq G$, em virtude do Teorema 1.4. Por hipótese de indução, existe $s \leqslant 2^{r-1}$ e elementos $h_1, ..., h_s \in G$, com $h_1 = 1$, tais que $\bigcap_{i=1}^{s} h_i Y_0 = \emptyset$. Escolha $g \in G$ de tal forma que $g h_i H_r \neq h_j H_r$, com $i, j \in \{1, ..., s\}$ Isso é possível, pois existe uma quantidade finita de classes da forma $h_j h_i^{-1} H_r$, com $i, j \in \{1, ..., s\}$, e H_r possui índice infinito em G. Assim,

$$\bigcap_{i=1}^{s} h_i Y \cap \bigcap_{i=1}^{s} g h_i Y = \bigcap_{i=1}^{s} h_i (Y_0 \cup H_r) \cap \bigcap_{i=1}^{s} g h_i (Y_0 \cup H_r) =$$

$$= \bigcap_{i=1}^{s} (h_i Y_0 \cup h_i H_r) \cap (g h_i Y_0 \cup g h_i H_r) =$$

$$= \bigcap_{i=1}^{s} ((h_i Y_0 \cap g h_i Y_0) \cup (h_i Y_0 \cap g h_i H_r) \cup (h_i H_r \cap g h_i Y_0) \cup (h_i H_r \cap g h_i H_r)) =$$

$$= \bigcap_{i=1}^{s} ((h_i Y_0 \cap g h_i Y_0) \cup (h_i Y_0 \cap g h_i H_r) \cup (h_i H_r \cap g h_i Y_0)).$$

Desenvolvendo a interseção $\bigcap_{i=1}^{s} ((h_i Y_0 \cap g h_i Y_0) \cup (h_i Y_0 \cap g h_i H_r) \cup (h_i H_r \cap g h_i Y_0))$, obtem-se uma união de um número finito de conjuntos e, todos esses conjuntos são interseções de outros conjuntos, onde pelo menos um desses tem uma das formas $\bigcap_{i=1}^{s} h_i Y_0$, $\bigcap_{i=1}^{s} g h_i Y_0$ ou $h_i H_r \cap g h_j H_r$, com $i \neq j$. Logo,

$$\bigcap_{i=1}^{s} ((h_i Y_0 \cap g h_i Y_0) \cup (h_i Y_0 \cap g h_i H_r) \cup (h_i H_r \cap g h_i Y_0)) = \emptyset.$$

Tomando, assim, $g_1 = h_1, g_2 = h_2, ..., g_s = h_s, g_{s+1} = g h_1, ..., g_{2s} = g h_s$, tem-se $\bigcap_{i=1}^{2s} g_i Y = \emptyset$ e $t = 2s \leqslant 2.2^{r-1} = 2^r$. O resultado segue. $\square$

1.2 Grupos Abelianos Livres

Como dito na introdução deste capítulo, o conceito de grupos abelianos livres nesta dissertação será apenas para ser utilizado na demonstração de algumas propriedades da seção de grupos abelianos.

Definição 1.6. Sejam F um grupo, X um conjunto não vazio e $\sigma : X \to F$. Então F, ou mais geralmente (F, σ), é dito ser *abeliano livre* sobre X, se para cada função α de X em um grupo abeliano G, existe um único homomorfismo $\beta : F \to G$, tal que $\alpha = \sigma\beta$.

A função σ, da definição anterior, é injetiva. De fato, suponha que $x_1\sigma = x_2\sigma$ e $x_1 \neq x_2$. Seja G um grupo abeliano com pelo menos dois elementos distintos g_1 e g_2 e defina uma função $\alpha : X \to G$, tal que $x_1\alpha = g_1$ e $x_2\alpha = g_2$. Como $x_1\sigma = x_2\sigma$, aplicando β em ambos os lados, tem-se $x_1\sigma\beta = x_2\sigma\beta$, ou seja, $g_1 = x_1\alpha = x_2\alpha = g_2$, absurdo. Portanto, σ é injetiva. Assim, claramente, F também é abeliano livre sobre seu subconjunto $Im(\sigma)$.

O primeiro resultado a ser considerado sobre grupos abeliano livres é o

Teorema 1.7. *([14], página 49) Sejam G um grupo abeliano gerado por um subconjunto X e F um grupo abeliano livre sobre um conjunto Y. Se existe uma função $\alpha : Y \to X$ sobrejetora, então α pode ser estendida a um epimorfismo $\bar{\alpha} : F \to G$. Em particular, cada grupo abeliano é uma imagem homomórfica de um grupo abeliano livre.*

É fato relevante para essas notas, que se F é um grupo abeliano livre, então existem um subconjunto X de F tal que para cada $f \in F$, existe uma única expressão $f = x_1^{k_1}...x_n^{k_n}$, com $x_1, ..., x_n \in X$ e $k_1, ..., k_n \in \mathbb{Z}$. É que mostra o

Teorema 1.8. *([14], página 60) Sejam F um grupo não trivial e X um subconjunto de F. Então, F é abeliano livre sobre X se, e somente se, $F = Dr_{x \in X} \langle x \rangle$, onde $\langle x \rangle$ é um grupo cíclico infinito para cada $x \in X$.*

Segue desse teorema o

Teorema 1.9. *([14], página 100) Sejam X um conjunto, F um grupo e H um subgrupo de F. Se F é abeliano livre sobre X, então H é abeliano livre sobre um conjunto Y, com $|Y| \leqslant |X|$.*

1.3 Grupos Abelianos

A teoria dos grupos abelianos tem suas particularidades e grandeza. Dar essa teoria completa não é o objetivo desta seção (para mais detalhes, consulte [14]), mas, apresentar alguns resultados que serão de suma importância nesta dissertação. Como os grupos desta seção são grupos abelianos, esses grupos serão escritos aditivamente.

Sejam G um grupo abeliano, g e h elementos de G com ordens iguais a n e m, respectivamente. Agora, se $l = mmc\{m, n\}$, então $l(g \pm h) = lg \pm lh = 0$, ou seja, $g \pm h$ também possui ordem finita. É imediato que o conjunto $G[n]$ formado por todos os elementos g de G tais que $ng = 0$ é um subgrupo de G. Fica também claro, que o conjunto $T = \bigcup_{n\in\mathbb{N}} G[n]$, também é um subgrupo de G, chamado *subgrupo de torção de G*. Além disso, o conjunto $G_p = \bigcup_{n\in\mathbb{N}} G[p^n]$ é um subgrupo de G, para todo primo p, denominado *p-componente primária de G*.

Teorema 1.10. *([14]) Em um grupo abeliano G o subgrupo de torção T é a soma direta das componentes primárias de G, ou seja, $T = Dr_{p\in P}\, G_p$, onde P é o conjunto de todos os números primos.*

Demonstração. Seja $x \in T$, com ordem n. Escreva n como um produto de potências de primos, isto é, $n = p_1^{k_1}...p_r^{k_r}$, com $p_1, ..., p_n$ primos dois a dois distintos. Seja $n_i = n/p_i^{k_i}$, para cada $i \in \{1, ..., r\}$. Observe que $mdc\{n_1, ..., n_r\} = 1$, assim, existem $l_1, ..., l_r \in \mathbb{Z}$ tais que $l_1n_1 + ... + l_rn_r = 1$. Logo, $x = (l_1n_1 + ... + l_rn_r)x = l_1n_1x + ... + l_rn_rx$. Colocando, $x_i = n_ix$, para cada $i \in \{1, ..., r\}$, tem-se que $|x_i| = p_i^{k_i}$, ou seja, $x_i \in G_{p_i}$. Assim, T está contido na soma das componentes primárias de G. Que essa soma é direta, segue do fato que $G_p \cap G_q = \{1\}$ se $p \neq q$ e que G é abeliano. Como, claramente, $Dr_{p\in P}\, G_p \leqslant T$, o resultado segue. □

Sejam G um grupo, g um elemento de G e m um inteiro positivo. Diz-se que g é *divisível* por m se existe $h \in G$ tal que $g = mh$.

Definição 1.11. Um grupo abeliano G é dito ser divisível se todo elemento de G é divisível por qualquer inteiro positivo.

Um exemplo de grupo divisível é o conjunto dos números racionais munido com a operação de adição.

Uma outra classe importante de grupos abelianos é a classe dos grupos que possuem a propriedade injetiva, cuja definição vem a seguir.

Definição 1.12. Um grupo abeliano G é dito ser injetivo se dados $\mu : H \to K$, um monomorfismo de grupos abelianos, e $\alpha : H \to G$, um homomorfismo de grupos, então existe um homomorfismo $\beta : K \to G$ tal que $\alpha = \mu\beta$, ou seja, tal que o diagrama

$$\begin{tikzcd} H \arrow[r, "\alpha"] \arrow[d, tail, "\mu"'] & G \\ K \arrow[ur, dashed, "\beta"'] & \end{tikzcd}$$

comuta.

Note que, na definição anterior, por ser μ um monomorfismo tem-se $H \simeq Im(\mu) \leqslant K$. Assim, é fácil ver que um grupo abeliano G é injetivo se para qualquer grupo abeliano K, todo homomorfismo $\alpha : H \to G$, com $H \leqslant K$, pode ser estendido a um homomorfismo $\beta : K \to G$. Existe uma relação entre grupos divisíveis e grupos injetivos, como mostra o

Teorema 1.13. (Baer) *Um grupo abeliano G é injetivo se, e somente se, é divisível.*

Demonstração. Suponha que o grupo G é injetivo. Sejam $g \in G$ e m um inteiro positivo. Defina $\alpha : m\mathbb{Z} \to G$, por $(mn)\alpha = ng$. Claramente, α é um homomorfismo de grupos. Se $\mu : m\mathbb{Z} \to \mathbb{Z}$ é a função inclusão, então existe um homomorfismo $\beta : \mathbb{Z} \to G$ tal que $\alpha = \mu\beta$. Assim, $g = (m)\alpha = (m)\mu\beta = (m)\beta = m((1)\beta)$. Tomando $h = (1)\beta$, a implicação direta segue.

Suponha, agora, que G é divisível e que são dados $\mu : H \to K$ e $\alpha : H \to G$, um monomorfismo de grupos abelianos e um homomorfismo de grupos, respectivamente. Não há perda de generalidade, em supor que $H \leqslant K$ e μ é a função inclusão, pois o grupo H pode ser replicado, pelo monomorfismo μ, em K. Assim, o resultado fica demonstrado se for possível estender α para K.

Considere o conjunto S de todos os homomorfismos $\gamma : L \to G$, em que $H \leqslant L \leqslant K$ e $h\gamma = h\alpha$, para todo $h \in H$. O conjunto S é não vazio, pois $\alpha \in S$. Defina em S a relação de ordem parcial $\gamma \preccurlyeq \gamma'$ se, e somente se, $\gamma : L \to G$ e $\gamma' : L' \to G$ são tais que $L \leqslant L'$ e γ' estende γ. Considere um subconjunto $\{\gamma_i : L_i \to G; i \in I\}$ totalmente ordenado em S. Tome $L = \bigcup_{i\in I} L_i$ e $\gamma : L \to G$ definida por $x\gamma = x\gamma_i$ se $x \in L_i$. Claramente γ está bem definida e $\gamma \in S$. Pelo Lema de Zorn, existe um elemento maximal $\beta : L \to G$ em S. Se $L = K$ a demonstração acabou. Suponha, por absurdo, que existe $x \in K\backslash L$ e considere o grupo $M = L + \langle x\rangle$. Se $L \cap \langle x\rangle = \{0\}$, então $M = L \oplus \langle x\rangle$ e, assim, o homomorfismo β pode ser estendido pelo homomorfismo $\beta' : M \to G$, dado por $(y)\beta' = (y)\beta$, se $y \in L$ e $(y)\beta' = 0$, se $y \in \langle x\rangle$, absurdo. Se $L \cap \langle x\rangle \neq \{0\}$, então existe um menor inteiro positivo m tal que $mx \in L$. Suponha que $(mx)\beta = g \in G$. Como G é divisível, existe $g_1 \in G$ tal que $g = mg_1$. Pela minimalidade de m, cada elemento de M pode ser escrito de maneira única na forma $l + tx$, com $0 \leqslant t < m$. Assim, fica bem definido um homomorfismo $\beta' : M \to G$, dado por $(l + tx)\beta' = (l)\beta + tg_1$, absurdo. Portanto, o resultado segue. □

Uma consequência importante deste teorema é o

Teorema 1.14. (Baer) *Se D é um subgrupo divisível de um grupo abeliano G, então $G = D \oplus E$, para algum subgrupo E de G.*

Demonstração. Sejam $\mu : D \to G$ a inclusão e $\alpha : D \to D$ a função identidade. Como D é divisível, pelo Teorema 1.13, D é injetivo, assim existe $\beta : G \to D$ tal que $\alpha = \mu\beta$. Logo, para cada $d \in D$ tem-se $(d)\beta = d$, mas $(g)\beta \in D$, para todo $g \in G$, então $(g)\beta = (g)\beta^2$. Logo, $g - (g)\beta \in Nuc(\beta)$. Colocando $E = Nuc(\beta)$, segue que $G = D + E$. Agora, se $x \in D \cap E$, então $x = (x)\beta = 0$, daí $G = D \oplus E$, como desejado. □

Enquanto o Teorema 1.13 relaciona grupos abelianos divisíveis e grupos abelianos injetivos, existe uma propriedade parecida que relaciona duas classes de grupos abelianos importantes.

Definição 1.15. Um grupo abeliano G é dito ser projetivo se, dados $\varepsilon : K \to H$ e $\alpha : G \to H$, um epimorfismo de grupos abelianos e um homomorfismo de grupos abelianos, existe um homomorfismo $\beta : G \to K$, tal que $\beta\varepsilon = \alpha$, ou seja, tal que o diagrama

$$\begin{tikzcd} & G \arrow[dl, dashed, "\beta"'] \arrow[d, "\alpha"] \\ K \arrow[r, "\varepsilon"'] & H \end{tikzcd}$$

comuta.

Assim, tem-se o

Teorema 1.16. (MacLane) *Um grupo abeliano G é projetivo se, e somente se, é abeliano livre.*

Demonstração. Primeiramente, suponha que o grupo G é abeliano livre sobre um subconjunto X. Sejam $\varepsilon : K \to H$ e $\alpha : G \to H$, um epimorfismo e um homomorfismo de grupos abelianos, respectivamente. Dado $x \in X$, existe $k_x \in K$ tal que $(k_x)\varepsilon = (x)\alpha$. Seja $\beta : G \to K$, o homomorismo tal que $(x)\beta = k_x$, para todo $x \in X$. Como $(x)\beta\varepsilon = (k_x)\varepsilon = (x)\alpha$, para todo $x \in X$ e $G = \langle X \rangle$ tem-se $\beta\varepsilon = \alpha$. Portanto, G é projetivo.

Suponha, agora, que o grupo G é projetivo. Pelo Teorema 1.7, existe um grupo F abeliano livre e um epimorfismo $\varepsilon : F \to G$, pois G é abeliano. Colocando $\alpha = Id_G$, existe $\beta : G \to F$, tal que $\beta\varepsilon = Id_G$, pois G é projetivo. Assim, $Nuc(\beta) = \{0\}$, ou seja, β é injetivo, logo $G \simeq Im(\beta) \leqslant F$. Pelo Teorema 1.9, G é abeliano livre. $\square$

Parecido com o Teorema 1.14 para grupos abelianos divisíveis, existe o seguinte resultado para grupos abelianos.

Teorema 1.17. *([14]) Se G é um grupo abeliano e H um subgrupo de G tal que G/H é abeliano livre, então $G = H \oplus K$, para algum subgrupo K de G.*

Demonstração. Pelo Teorema 1.16, $F = G/H$ é projetivo. Considere $\varepsilon : G \to F$ o epimorfismo canônico e $\alpha : F \to F$ a função identidade. Assim, existe $\beta : F \to G$, tal que $\beta\varepsilon = Id_F$. Logo, se $g \in G$, então $(g - (g)\varepsilon\beta)\varepsilon = (g)\varepsilon - (g)\varepsilon = 0$, ou seja, $g \in Nuc(\varepsilon) + Im(\beta)$, daí, $G = Nuc(\varepsilon) + Im(\beta)$. Agora, $\beta\varepsilon = Id_G$ implica $Nuc(\varepsilon) \cap Im(\beta) = \{0\}$. Portanto, $G = Nuc(\varepsilon) \oplus Im(\beta)$, como $Nuc(\varepsilon) = H$, o resultado segue. $\square$

A partir desses resultados, é possível estudar a estrutura de alguns grupos abelianos. Para o próximo resultado é necessário o conceito de grupo *limitado*. Um grupo G é dito ser *limitado* se cada elemento de G possui ordem finita e o subconjunto $\{|g|;\, g \in G\}$ de $\mathbb{N}$ é limitado superiormente.

Lema 1.18. *([14]) Sejam G um p-grupo abeliano limitado e g um elemento de G de ordem máxima. Então, $\langle g \rangle$ é um somando direto de G.*

Demonstração. Pelo Lema de Zorn, existe um subgrupo M de G o qual é maximal com relação a propriedade $M \cap \langle g \rangle = \{0\}$. Se $G = M + \langle g \rangle$, então $G = M \oplus \langle g \rangle$ e o resultado segue. Caso contrário, seja x um elemento de $G \setminus (M + \langle g \rangle)$ de ordem mínima. Pela escolha de x, segue que $px \in M + \langle g \rangle$ e, assim, existem um inteiro positivo l e $y \in M$ tais que $px = y + lg$. Seja p^n a ordem de g, como essa ordem é máxima, segue que $0 = p^n x = p^{n-1} y + p^{n-1} lg$, daí, $p^{n-1} lg \in M \cap \langle g \rangle = \{0\}$. Consequentemente, p^n divide $p^{n-1} l$, isto é, p divide l. Então, $l = pj$, para algum inteiro j e obtém-se, assim, $p(x - jg) = y \in M$. Mas $x - jg \notin M$, pois $x \notin M + \langle g \rangle$. Pela maximalidade de M, $\langle x - jg, M \rangle \cap \langle g \rangle \neq \{0\}$, o que implica que existem inteiros k e u e $y' \in M$ tais que $0 \neq kg = u(x - jg) + y'$. Então, $ux \in M + \langle g \rangle$. Agora, se $p|u$, então $u(x - jg) \in M$ e, daí, $kg = 0$, absurdo. Logo, $mdc\{u, p\} = 1$, ou seja, existem inteiros v e w tais que $vu + wp = 1$ e, assim, $v(ux) + w(px) = x \in M + \langle g \rangle$, absurdo. O resultado segue. □

Utilizando esse lema, será provado o

Teorema 1.19. (Frobenius-Stickelbergerf) *Um grupo abeliano G é finito se, e somente se, G é uma soma direta de um número finito de subgrupos cíclicos de ordens potências de primos.*

Demonstração. Suponha que o grupo abeliano G é finito. A demonstração será feita por indução sobre a ordem de G. Se $|G| = 1$, nada há para fazer. Suponha que o resultado vale para todo grupo cuja ordem é inferior a $|G|$, com $|G| > 1$. Como G é um grupo de torção, G é a soma direta de suas componentes primárias, em virtude do Teorema 1.10. Assim, pode-se supor que G é um p-grupo abeliano. Seja $g \in G$, com ordem máxima. Pelo Lema 1.18,

$G = G_1 \oplus \langle g \rangle$, para algum subgrupo G_1 de G. Agora, aplicando a hipótese de indução sobre G_1, o resultado segue. A outra implicação é imediata. $\square$

O próximo resultado diz respeito a um grupo abeliano de torção finitamente gerado.

Proposição 1.20. *([14]) Um grupo abeliano de torção finitamente gerado é finito.*

Demonstração. Seja G um grupo abeliano de torção finitamente gerado. Assim, existem um inteiro positivo n e $g_1, ..., g_n \in G$, tais que $G = \langle g_1, ..., g_n \rangle$. Logo, G é uma soma dos grupos finitos $G_i = \langle g_i \rangle$, com $i \in \{1, ..., n\}$ e, assim, G é finito. $\square$

É dito que um grupo G satisfaz a *condição maximal* se qualquer cadeia ascendente

$$H_0 \leqslant H_1 \leqslant ... \leqslant H_n \leqslant ...$$

de subgrupos de G estaciona, isto é, existe $k \in \mathbb{N}$ tal que $H_j = H_k$, para todo $j \geqslant k$. Por exemplo: Se G é um grupo cíclico, então todo subgrupo não trivial de G é também cíclico e de índice finito em G, logo toda cadeia ascendente de G é estacionária. Seguem dois resultados sobre um grupo que satisfaz a condição, os quais não serão demonstrados. Para mais detalhes consulte [14].

Teorema 1.21. *([14], página 68) Um grupo G satisfaz a condição maximal se, e somente se, cada subgrupo de G é finitamente gerado.*

Teorema 1.22. *([14], página 68) Sejam G um grupo, H um subgrupo normal de G. Se os grupos H e G/H satisfazem a condição maximal, então G satisfaz a condição maximal.*

Pelo Teorema 1.21, todo grupo que satisfaz a condição maximal é finitamente gerado. O próximo resultado diz que vale a recíproca se G é abeliano.

Proposição 1.23. *([14]) Se o grupo abeliano G é finitamente gerado, então G satisfaz a condição maximal.*

Demonstração. Suponha que G é finitamente gerado, ou seja, que existam um n inteiro positivo e $g_1, ..., g_n \in G$ tais que $G = \langle g_1, ..., g_n \rangle$. A demonstração será feita por indução sobre o número n. Se $n = 1$, então $G = \langle g_1 \rangle$, isto é, G é cíclico, assim o grupo G satisfaz a condição maximal. Suponha que $n > 1$, logo, por hipótese de indução, os grupos $\langle g_1, ..., g_{n-1}\rangle$ e $G/\langle g_1, ..., g_{n-1}\rangle$, satisfazem a condição maximal. Pelo Teorema 1.22, G satisfaz a condição maximal. O resultado segue. $\square$

Utilizando a maioria dos fatos desta seção, segue o último resultado.

Teorema 1.24. *([14]) Um grupo abeliano G é finitamente gerado se, e somente se, G é uma soma direta de um número finito de subgrupos cíclicos com ordens infinitas ou ordens potências de números primos.*

Demonstração. Seja G um grupo finitamente gerado, desta forma, existem um inteiro positivo n e elementos $g_1, ..., g_n$ de G tais que $G = \langle g_1, ..., g_n\rangle$. Suponha inicialmente que G é livre de torção. A demonstração será feita por indução sobre n. Se $n = 1$ o resultado é imediato. Suponha que o resultado vale para todo todo subgrupo finitamente gerado por m elementos, com $1 \leqslant m < n$. Seja H o subconjunto de todos os elementos x de G tais que $rx \in \langle g_1\rangle$, para algum inteiro positivo r. É fácil verificar que H é um subgrupo de G. Agora, se $sx \in H$, para algum inteiro positivo s, então $rsx \in \langle g_1\rangle$, para algum inteiro positivo r, assim $x \in H$ e, isso mostra que G/H é livre de torção. Como G/H é gerado pelos elementos $g_2 + H, ..., g_n + H$, segue, por hipótese de indução, que G/H é uma soma direta de um número finito de subgrupos ciclicos infinitos. Assim, G/H é abeliano livre. Aplicando o Teorema 1.17, tem-se que $G = H \oplus K$, com $K \simeq G/H$. Certamente, o grupo $H/\langle g_1\rangle$ é de torção. Pela Proposição 1.23, o grupo G satisfaz a condição maximal, logo, pelo Teorema 1.21, H é finitamente gerado e, assim, $H/\langle g_1\rangle$ também o é. Daí, pelo Teorema 1.20, $H/\langle g_1\rangle$ é finito. Consequentemente, existe um inteiro positivo t tal que $tH \leqslant \langle g_1\rangle$. Logo, a função $\alpha : H \to \langle g_1\rangle$ dada por $(h)\alpha = th$, para todo $h \in H$, é um monomorfismo de grupos. Portanto, H é um grupo cíclico infinito e $G = H \oplus K$ é abeliano livre. Portanto, pelo Teorema 1.8, G é uma soma direta de uma quantidade finita de subgrupos cíclicos infinitos.

Para o caso geral, seja T o subgrupo de torção de G. Assim, o grupo G/T é finitamente gerado e livre de torção. Pela primeira parte da demonstração, G/T é abeliano livre. Desta forma, pelo Teorema 1.17, $G = F \oplus T$, com F abeliano livre e finitamente gerado. Agora, T é finitamente gerado e de torção e, então, pelo Teorema 1.20, T é finito. Daí, pelos Teoremas 1.8 e 1.19, o resultado segue. $\square$

1.4 O Teorema de Schur

Quando o índice do centro de um grupo G é finito, o subgrupo derivado G' de G também é finito; isso é o que afirma o *Teorema de Schur*. O objetivo dessa seção é demonstrar esse teorema, mas, antes é necessário definir e apresentar algumas propriedades do homomorfismo *transfer*.

Para tanto, considere um grupo G e $H \leqslant G$, com índice finito n em G. Escolha uma transversal $T = \{t_1, ..., t_n\}$ à direita de H em G. Assim, para cada $g \in G$ e $i \in \{1, .., n\}$, existe $(i)\sigma_g \in \{1, ..., n\}$ tal que $Ht_i g = Ht_{(i)\sigma_g}$. Note que σ_g é uma permutação do conjunto $\{1, ..., n\}$, para cada $g \in G$. Além disso, $t_i g t^{-1}_{(i)\sigma_g} \in H$, para todo $g \in G$. Agora, se $g, h \in G$ e $i \in \{1, ..., n\}$, tem-se que $Ht_i g = Ht_{(i)\sigma_g}$, assim $Ht_i gh = Ht_{(i)\sigma_g} h$. Mas $Ht_{(i)\sigma_g} h = Ht_{((i)\sigma_g)\sigma_h}$, ou seja, $Ht_{(i)\sigma_{gh}} = Ht_i gh = Ht_{((i)\sigma_g)\sigma_h}$. Desta forma, $(i)\sigma_{gh} = ((i)\sigma_g)\sigma_h$.

Definição 1.25. Sejam G um grupo, H um subgrupo de índice finito n em G, $T = \{t_1, ..., t_n\}$ à direita de H em G e $\theta : H \to A$ um homomorfismo de H em um grupo abeliano A. O *trensfer de* θ com relação a A é a aplicação

$$\theta^* : G \to A,$$

dada por

$$g^{\theta^*} = \prod_{i=1}^{n} (t_i g t^{-1}_{(i)\sigma_g})^{\theta},$$

em que σ_g é a permutação do conjunto $\{1, ..., n\}$ tal que $Ht_i g = Ht_{(i)\sigma_g}$, $i = 1, ..., n$.

Em verdade, o *transfer* é um homomorfismo de grupos, como mostra o

Teorema 1.26. *([14]) A aplicação $\theta^* : G \to A$, como na Definição 1.25, é um homomorfismo de grupos que não depende da transversal escolhida.*

Demonstração. Inicialmente, observe que o *transfer* independe da escolha da transversal. De fato, seja $\{t'_1, ..., t'_n\}$ uma outra transversal à direita de H em G. Reordenando os índices se necessário, pode-se supor que $Ht'_i = Ht_i$, $i = 1, ..., n$. Assim, $t'_i = t_i h_i$, para algum $h_i \in H$. Se $g \in G$, tem-se que $t_i g t'^{-1}_{(i)\sigma_g} = h_i (t_i g t_{(i)\sigma_g}) h^{-1}_{(i)\sigma_g}$. Do fato de A ser abeliano, segue que

$$\prod_{i=1}^{n} (t'_i g (t'_{(i)\sigma_g})^{-1})^{\theta} = \prod_{i=1}^{n} (t_i g (t_{(i)\sigma_g})^{-1})^{\theta} \prod_{i=1}^{n} h_i^{\theta} h^{-\theta}_{(i)\sigma_g}.$$

Mas, i percorre o conjunto $\{1, ..., n\}$, como $(i)\sigma_g$ é uma permutação do conjunto $\{1, ..., n\}$ e, cada vez que h_i aparece no produto $\prod_{i=1}^{n} h_i^{\theta} h_{(i)\sigma_g}^{-\theta}$, também aparece h_i^{-1}, ou seja, $\prod_{i=1}^{n} h_i^{\theta} h_{(i)\sigma_g}^{-\theta} = 1$. Então, $\prod_{i=1}^{n}(t_i' g (t_{(i)\sigma_g}')^{-1})^{\theta} = \prod_{i=1}^{n}(t_i g t_{(i)\sigma_g}^{-1})^{\theta}$. Agora sejam $g, h \in G$, então

$$(gh)^{\theta^*} = \prod_{i=1}^{n}(t_i g h t_{(i)\sigma_{gh}}^{-1})^{\theta} = \prod_{i=1}^{n}(t_i g t_{(i)\sigma_g}^{-1} t_{(i)\sigma_g} h t_{\sigma_{gh}}^{-1})^{\theta} =$$

$$= \prod_{i=1}^{n}(t_i g t_{(i)\sigma_g}^{-1})^{\theta} \prod_{i=1}^{n}(t_{(i)\sigma_g} h t_{((i)\sigma_g)\sigma_h}^{-1})^{\theta} = \prod_{i=1}^{n}(t_i g t_{(i)\sigma_g}^{-1})^{\theta} \prod_{j=1}^{n}(t_j h t_{(j)\sigma_h}^{-1})^{\theta} = g^{\theta^*} h^{\theta^*}.$$

Como desejado. □

O próximo lema é um resultado técnico que será usado na demonstração do teorema que o segue.

Lema 1.27. *([14]) Sejam G um grupo, H um subgrupo de índice finito em G, $\theta : H \to A$ um homomorfismo de H em um grupo abeliano A e $g \in G$. Então, existe um transversal*

$$S = \{s_1, s_1 g, ..., s_1 g^{l_1 - 1}\} \uplus ... \uplus \{s_k, s_k g, ..., s_k g^{l_k - 1}\}$$

à direita de H em G, com $l_j = min\{l;\ H s_j g^l = H s_i, l \in \mathbb{N}\}$, para todo $j \in \{1, ..., k\}$, tal que

$$g^{\theta^*} = \prod_{j=1}^{k}(s_j g^{l_j} s_j^{-1})^{\theta},$$

onde θ^* é o transfer de θ.

Demonstração. Seja $T = \{t_1, ..., t_n\}$ um transversal à direita de H em G. Observe que o conjunto $\{H t_i g^l;\ l \in \mathbb{N}\}$ é finito para cada $i \in \{1, ..., n\}$. Seja $l_i' = min\{l;\ H t_i g^l = H t_i, l \in \mathbb{N}\}$, para cada $i = 1, ..., n$. Daí, o conjunto $\{H t_1, ..., H t_n\}$ é particionado em subconjuntos disjuntos na forma $\{H t_{i_j}, H t_{i_j} g, ..., H t_{i_j} g^{l_{i_j}' - 1}\}$, com $j \in \{1, ..., k\}$. Tome agora $s_j = t_{i_j}$ e $l_j = l_{i_j}'$, para cada $j \in \{1, ..., k\}$ e, assim, $S = \{s_1, s_1 g, ..., s_1 g^{l_1 - 1}\} \uplus ... \uplus \{s_k, s_k g, ..., s_k g^{l_k - 1}\}$ é uma transversal à direita de H em G, com $l_j = min\{l;\ H s_j g^l = H s_i, l \in \mathbb{N}\}$, para todo $j \in \{1, ..., k\}$. Note que se $v \in \{1, ..., k\}$ e $w \in \{0, 1, ..., l_v - 1\}$, então se $w \neq l_v - 1$, $(s_v g^w)_{(w)\sigma_g} = s_v g^{w+1}$ e se $w = l_w - 1$, $(s_v g^w)_{(w)\sigma_g} = s_v$, pois $(s_v g^w)_{(w)\sigma_g} = s_v g^w g$. Assim,

$$(s_v g (s_v)_{(1)\sigma_g}^{-1})^{\theta} (s_v g g (s_v g)_{(2)\sigma_g}^{-1})^{\theta} ... (s_v g^{l_v - 1} g (s_v g^{l_v - 1})_{(l_v - 1)\sigma_g}^{-1})^{\theta} =$$

$$= [s_v g (s_v g)^{-1} (s_v g) g (s_v g^2)^{-1} (s_v g^2) g (s_v g^3)^{-1} ... (s_v g^{l_v - 1})^{-1} (s_v g^{l_v - 1}) g s_v^{-1}]^{\theta} = (s_v g^{l_v} s_v^{-1})^{\theta}.$$

Portanto, $g^{\theta^*} = \prod_{j=1}^{k}(s_j g^{l_j} s_j^{-1})^{\theta}$. □

Agora, um outro teorema, também devido a Schur, que servirá como um lema para o teorema principal.

Teorema 1.28. ***(Schur)*** *Sejam G um grupo e H um subgrupo de $Z(G)$ com índice finito n em G. Então, o transfer $(Id_H)^*$ de Id_H com relação a H é dado por $g^{(Id_H)^*} = g^n$, para todo $g \in G$.*

Demonstração. Dado $g \in G$, pelo Lema 1.27, existe um transversal

$$S = \{s_1, s_1 g, ..., s_1 g^{l_1 - 1}\} \uplus ... \uplus \{s_k, s_k g, ..., s_k g^{l_k - 1}\}$$

à direita de H em G, com $l_j = min\{l;\ H s_j g^l = H s_i, l \in \mathbb{N}\}$, para todo $j \in \{1, ..., k\}$, tal que

$$g^{Id_H^*} = \prod_{j=1}^{k} (s_j g^{l_j} s_j^{-1})^{Id_H} = \prod_{j=1}^{k} s_j g^{l_j} s_j^{-1}.$$

Mas, $s_j g^{l_j} s_j^{-1} \in H$ e $H \leqslant Z(G)$, assim $g^{l_j} \in H$ e daí,

$$\prod_{j=1}^{k} s_j g^{l_j} s_j^{-1} = \prod_{j=1}^{k} g^{l_j} = g^{\sum_{j=1}^{k} l_j} = g^n,$$

pois $l_1 + ... + l_k = n$. O resultado segue. $\square$

Por fim, a demonstração do resultado principal dessa seção.

Teorema 1.29. ***(Schur)*** *Se G é um grupo tal que $|G : Z(G)| = n < \infty$, então G' é finito e $(G')^n = \{1\}$.*

Demonstração. Escreva $G/Z(G) = \{Z(G)g_1, ..., Z(G)g_n\}$. Se $x, y \in Z(G)$, então $[xg_i, yg_j] = [g_i, g_j]$. Isso implica que G' é gerado pelos $n(n-1)/2$ elementos da forma $[g_i, g_j]$, ou seja, G' é finitamente gerado. Do Segundo Teorema do Isomorfismo segue que $G'/(G' \cap Z(G)) \simeq G'Z(G)/Z(G)$. Como, por hipótese, $G'Z(G)/Z(G)$ é finito, $G'/(G' \cap Z(G))$ também o é. Assim, $G' \cap Z(G)$ é um subgrupo de índice finito no grupo finitamente gerado G', daí, pela Proposição 1.3, $G' \cap Z(G)$ é um grupo abeliano finitamente gerado. Pelo Teorema 1.28, colocando $H = Z(G)$, segue que $G' \leqslant Nuc(Id_H^*)$ e $(G')^n = \{1\}$, isto é, G' é de torção. Logo, $G' \cap Z(G)$ é um grupo abeliano finitamente gerado e de torção e, consequentemente, pela Proposição 1.20, é finito. Como $G'/(G' \cap Z(G))$ é também finito, G' é finito. $\square$

1.5 Grupos com Classes de Conjugação Finitas

Grupos que possuem classes de conjugação finitas são chamados FC-grupos. O matemático *B. H. Neumann* estudou amplamente esse tipo de grupo em um artigo dedicado ao também matemático *Issai Schur* (veja [11]). Quase todos os resultados desta seção se encontram nesse artigo, entretanto, as demonstrações feitas aqui seguem [2].

Definição 1.30. Sejam G um grupo e $g \in G$. O elemento g é chamado $FC - elemento$ se a classe de conjugação de g é finita, isto é, denotando $g^G = \{g^x = x^{-1}gx;\ \ x \in G\}$, então g é $FC - elemento$ se $|g^G| < \infty$.

A demonstração da seguinte proposição segue direto da definição de g^G.

Proposição 1.31. *([14]) Se G é um grupo e $g \in G$, então $|g^G| = |G : C_G(g)|$.*

Demonstração. Considere a função $f : g^G \to \{C_G(g)x;\ \ x \in G\}$ tal que $g^x \mapsto C_G(g)x$, para todo $x \in G$. Tem-se que f está bem definida. De fato, se $g^x = g^y$, então $gxy^{-1} = xy^{-1}g$, logo $xy^{-1} \in C_G(g)$ e assim $C_G(g)x = C_G(g)y$, ou seja, $(g^x)f = (g^y)f$. Claramente f é sobrejetora e, se $(g^x)f = (g^y)f$ tem-se $C_G(g)x = C_G(g)y$ e com isso $xy^{-1} \in C_G(g)$. Assim $gxy^{-1} = xy^{-1}g$, ou seja, $g^x = g^y$. Portanto, f é bijetora e $|g^G| = |G : C_G(g)|$. $\square$

Da Proposição 1.31 segue que um elemento $g \in G$ é um FC-elemento se, e somente se, $|G : C_G(g)| < \infty$. Assim, o subconjunto $\widehat{Z}(G)$ formados por todos os FC-elementos de G é dado por $\hat{Z}(G) = \{g \in G; |G : C_G(g)| < \infty\}$. Um fato relevante é que esse subconjunto é um subgrupo característico em G, como mostra o seguinte

Teorema 1.32. (Baer) *O subconjunto $\widehat{Z}(G)$ formado por todos os $FC - elementos$ de um grupo G é um subgrupo característico de G.*

Demonstração. Sejam $g, h \in \hat{Z}(G)$. É claro que $C_G(g) \cap C_G(h^{-1}) \leq C_G(gh^{-1})$ e, como $|G : C_G(g) \cap C_G(h^{-1})| \leq |G : C_G(g)||G : C_G(h^{-1})| < \infty$, segue que $\hat{Z}(G)$ é um subgrupo. Sejam agora $\alpha \in Aut(G)$ e $g \in \hat{Z}(G)$. Se $|G : C_G(g)| = n$ para algum inteiro positivo n, como $(C_G(g))^{\alpha}. = C_G(g^{\alpha})$ segue que $G = G^{\alpha} = (\bigcup_{i=1}^{n} C_G(g)x_i)^{\alpha} = \bigcup_{i=1}^{n} C_G(g^{\alpha})x_i^{\alpha}$ e, assim, $|G : C_G(g^{\alpha})| < \infty$, daí, $g^{\alpha} \in \hat{Z}(G)$. Portanto, o subgrupo $\hat{Z}(G)$ é característico em G. $\square$

O subgrupo $\widehat{Z}(G)$ é chamado *FC-centro* de G. Se $G = \widehat{Z}(G)$, G é dito ser um *FC-grupo*. Grupos finitos e grupos abelianos são exemplos simples de FC-grupos. O próximo resultado possibilita a construção de FC-grupos.

Proposição 1.33. *([14]) A classe dos FC-grupos é fechada com respeito a formação de subgrupos, grupos quocientes, imagens homomórficas e produtos diretos.*

Demonstração. Claramente essa classe é fechada para subgrupos, grupos quocientes e, consequentemente, também para imagens homomórficas. Agora seja $G = Dr_{i\in I}G_i$, com G_i FC-grupo para cada $i \in I$. Se $g \in G$, g se escreve de maneira única na forma $g = g_{i_1}...g_{i_n}$, com $g_{i_j} \in G_{i_j}$ e n inteiro não negativo. Sendo $\{t_{i_j1}, ..., t_{i_jm_j}\}$ a classe de conjugação de g_{i_j} em G_{i_j}, segue que g^G está no conjunto $\big\{t_{i_1k_1}...t_{i_nk_n};\ \ t_{i_jk_j} \in \{t_{i_j1}, ..., t_{i_jm_j}\}$ para $j = 1, ..., n\big\}$, que é finito. Portanto, G é FC-grupo. □

Dado G um grupo e Υ uma classe de grupos, G é chamado *residualmente por* Υ se para cada $g \in G\backslash\{1\}$, existe um subgrupo normal N_g de G tal que $g \notin N_g$ e $G/N_g \in \Upsilon$. Em particular, se Υ é a classe dos grupos finitos, G é dito ser *residualmente finito*.

Teorema 1.34. (Baer) *Se G é um FC-grupo, então $G/Z(G)$ é um grupo de torção residualmente finito.*

Demonstração. Seja $Z(G)g \in G/Z(G)$, com $g \notin Z(G)$ e considere $\{1, g_2, ..., g_n\}$ um transversal à direita de $C_G(g)$ em G. Pela Proposição 1.1, $C = C_G(g_2)\cap...\cap C_G(g_n)$ possui índice finito em G e, pela Proposição 1.2, C_G possui índice finito em G. Uma vez que $C_G/Z(G) \lhd G/Z(G)$, $Z(G)g \notin C_G/Z(G)$ e $(G/Z(G))/(C_G/Z(G)) \simeq G/C_G$, o qual é finito, obtém-se que $G/Z(G)$ é residualmente finito. Agora sejam $x \in G$ e $\{x_1, ..., x_r\}$ um transversal à direita de $C_G(x)$ em G. Pelo mesmo argumento dado acima, $K = \bigcap_{i=1}^{r} C_G(x_i)$ e K_G possuem índices finitos em G. Logo existe k tal que $(K_Gx)^k = K_Gx^k = K_G$. Mas, $K_G \leqslant K$ e daí $x^k \in K_G$ centraliza cada x_i, $i = 1, ..., n$. Como $G = \cup_{i=1}^{n} C_G(x)x_i$ tem-se $x^k \in Z(G)$ e $(Z(G)x)^k = Z(G)$. Portanto $G/Z(G)$ é de torção. □

Definição 1.35. Um subconjunto X de um grupo G é chamado *subconjunto normal* se satisfaz uma das seguintes condições:

(i) X é uma união de classes de conjugação de elementos de G;

(ii) Para todo $g \in G$, $g^{-1}Xg \subseteq X$;

(iii) Para todo $g \in G$, $g^{-1}Xg = X$.

É fácil ver que as afirmações (i), (ii) e (iii) da Definição 1.35 são equivalentes.

Lema 1.36. (Dicman) *Em um grupo G, um subconjunto normal e finito consistindo somente de elementos de ordens finitas gera um subgrupo normal e finito.*

Demonstração. Seja $X = \{x_1, ..., x_n\}$ um subconjunto normal e finito de G, com $|x_i| < \infty$ para todo $i = 1, ..., n$, e coloque $H = \langle X \rangle$. Claramente $H \lhd G$. Agora se $h \in H \backslash \{1\}$, então $h = x_{i_1}^{m_1} ... x_{i_r}^{m_r}$ com $1 \leqslant i_j \leqslant n$ para todo $j = 1, ..., r$. Em geral há muitas dessas expressões para h, entre as quais há algumas de menor comprimento. Seja r esse comprimento. Dentre as expressões de menor comprimento r, há uma que aparece em primeiro na ordem lexicográfica das r-uplas $(i_1, ..., i_r)$. Seja essa primeira expressão dada por $h = y_1 ... y_r$, com $y_j = x_{i_j}^{m_j}$. Suponha, por absurdo, que existam $l < k$ tais que $i_l = i_k$, assim $h = y_1 ... y_{l-1}(y_l y_k) y_{l+1}^{y_k} ... y_{k-1}^{y_k} y_{k+1} ... y_r$ é uma expressão para h de comprimento menor do que r, absurdo, consequentemente os i_j's são distintos e $r \leqslant n$. Suponha, novamente, por absurdo, que $i_j > i_{j+1}$, então $h = y_1 ... y_{j-1} y_{j+1} y_j^{y_{j+1}} y_{j+2} ... y_r$ é uma expressão que precede $h = y_1 ... y_r$ na ordem lexicográfica das r-uplas $(i_1, ..., i_r)$. Assim $i_1 < ... < i_r$. Como cada expressão, de menor comprimento e que aparece primeiro na ordem lexicográfica, é única, resulta que $|H| \leqslant \prod_{i=1}^{n} |x_i|$. Portanto H é finito. □

Se em um grupo G, cada subconjunto finito está contido em um subgrupo finito de G, então diz se que G é *localmente finito.* Quando, além disso, esse subgrupo finito é normal G é chamado *localmente finito e normal.* O teorema a seguir relaciona FC-grupos de torção com grupos localmente finitos e normais.

Teorema 1.37. *([14]) Um grupo G de torção é FC-grupo se, e somente se, é localmente finito e normal.*

Demonstração. Suponha que G é um FC-grupo e que F é um subconjunto finito de G. Então, o subconjunto X de todos os conjugados dos elementos de F em G é um subconjunto finito. Pelo Lema 1.36, $X \subseteq \langle X \rangle$ com $\langle X \rangle \lhd G$ e $|\langle X \rangle| < \infty$, o que mostra que a condição é necessária. Reciprocamente, seja $g \in G$. Por hipótese, existe $N \lhd G$ com $\{g\} \subseteq N$ e $|N| < \infty$ e, assim, todo conjugado de g está em N. Como $|N| < \infty$, segue que a condição é suficiente. □

Usando o Teorema de *Schur*, Teorema 1.29, é possível caracterizar o subgrupo derivado de um FC-grupo.

Teorema 1.38. (B. H. Neumann) *Se G é um FC-grupo, então G' é um grupo de torção. Além disso, o conjunto dos elementos de ordens finitas em G é um subgrupo totalmente invariante contendo G'.*

Demonstração. Como G é FC-grupo, então $G/Z(G)$ é FC-grupo e, pelo Teorema 1.34, é de torção. Logo, pelo Teorema 1.37, $G/Z(G)$ é localmente finito e normal. Agora seja X um subgrupo de G finitamente gerado. Então $XZ(G)/Z(G) = X/X \cap Z(G)$ é finitamente gerado e, sendo $G/Z(G)$ localmente finito e normal, $X/X \cap Z(G)$ é finito e, consequentemente, $X/Z(X)$ é finito, pois, $X \cap Z(G) \subset Z(X)$. Do Teorema de Schur, segue que X' é finito. Se $\mathfrak{F} = \{X \leqslant G;\ X$ é finitamente gerado $\}$, então $G' = \cup_{X \in \mathfrak{F}} X'$ e, com isso, G' é de torção. Agora sejam g e h elementos de G tais que $g^n = 1 = h^m$, com n e m inteiros positivos. De ser G/G' abeliano segue-se

$$(gh^{-1})^{mn} G' = g^{mn} h^{-mn} G' = G',$$

ou seja, $(gh^{-1})^{mn} \in G'$ e assim existe l inteiro positivo tal que $(gh^{-1})^{mnl} = 1$. Portanto, o conjunto de todos elementos de ordens finitas de G é um subgrupo e, por ser claramente totalmente invariante, o resultado segue. □

Contida na classe dos FC-grupos existe uma classe muito importante, a classe dos BFC-grupos. A definição de BFC-grupo vem a seguir.

Definição 1.39. Um FC-grupo G é chamado *BFC-grupo* se existe um inteiro positivo d tal que a quantidade de conjugados de qualquer elemento de G não ultrapassa d.

No artigo *Groups with finite classes of conjugate elements*, inicialmente citado, B. H. Neumann demonstra que o subgrupo derivado de um BFC-grupo é finito usando *produtos* *livres de grupos* (Para mais detalhes, consulte [11]). Para finalizar essa seção, segue esse resultado, cuja demonstração usa o Teorema de Schur e os resultados aqui já demonstrados.

Teorema 1.40. (**B. H. Neumann**) *Um grupo G é BFC-grupo se, e somente se, G' é finito.*

Demonstração. Suponha inicialmente que exista d tal que $|G'| = d < \infty$. Isso implica que se $g \in G$, então $|\{[g,x];\ x \in G\}| \leqslant d$ e com isso a quantidade de conjugados de g não excede d, como desejado. Reciprocamente, sejam G um BFC-grupo, $d = \max_{g \in G}\{|G : C_G(g)|\}$ e $a \in G$ satisfazendo $|G : C_G(a)| = d$. Escolha $\{t_1, ..., t_d\}$ um transversal à direita de $C_G(a)$ em G. Se $C = \cap_{i=1}^{d} C_G(t_i)$, o índice $|G : C|$ é finito e existe um transversal à direita finito $\{s_1, ..., s_k\}$ de C em G. Agora considere o subgrupo

$$N = \langle a, s_1, ..., s_k \rangle^G = \langle g^{-1}xg;\ \ x \in \{a, s_1, ..., s_k\}, g \in G \rangle,$$

o qual é um FC-grupo finitamente gerado. Pelo Teorema 1.34, $N/Z(N)$ é de torção e, do Teorema 1.37, é finito. Assim, pelo Teorema de Schur, N' é finito. Como N/N' é abeliano e finitamente gerado, pelo Teorema 1.24, tem-se que seu subgrupo de torção é também finitamente gerado, mas, esse subgrupo é dado por T_N/N', com $T_N = \{n \in N;\ |n| < \infty\}$, pois N' é finito. Logo, pela Proposição 1.20, T_N/N' é finito, assim T_N é finito. Uma vez que G' é de torção, resta mostrar que $G' \leqslant N$. De fato, se $c \in C$, então $(ca)^{t_i} = t_i^{-1}cat_i = ct_i^{-1}at_i = ca^{t_i}$, pois, $C \leqslant C_G(t_i)$ e disto segue que a classe de conjugação do elemento ca em G é igual ao conjunto $\{ca^{t_i};\ i = 1, ..., d\}$, pois a quantidade de conjugados de ca é no máximo d e $|\{ca^{t_i};\ i = 1, ..., d\}| = d$. Consequentemente, se $s \in C$, então existe i tal que $(ca)^s = ca^{t_i}$ e isto implica que $c^s = ca^{t_i}a^{-s}$ e $[c, s] = a^{t_i}a^{-s} \in N$. Portanto, $C' \leqslant N$ e $G' \leqslant NC' \leqslant N$, pois $G = NC$, como esperado. $\square$

Capítulo 2

Grupos de Automorfismos

A um grupo sempre é possível associar um grupo de automorfismos que age sobre ele. Por exemplo, dados um grupo G e $A \leqslant Aut(G)$, defina a ação de A à direita de G por $\rho : G \times A \to G$ em que $(g, \alpha)\rho = g^\alpha$, para todo $g \in G$ e todo $\alpha \in A$. Os subgrupos de $Aut(G)$ são chamados *grupos de automorfismos de* G. Em muitos casos, conhecendo a "natureza" de um grupo $A \leqslant Aut(G)$ e propriedades de sua ação, pode-se obter informações sobre o próprio grupo G. Neste capítulo se iniciará o estudo desse tipo de ação.

Na Seção 2.1 serão estabelecidos todos os conceitos e notações básicas. Já na Seção 2.2, a ação será de um grupo de automorfismos que age por um número finito de órbitas. Nela serão expostos e demonstrados fatos importantes dessa teoria.

2.1 Algumas Propriedades de Grupos de Automorfismos

Nesta seção, salvo menção contrária, G denotará um grupo e A um grupo de automorfismos de G.

Definição 2.1. Dado $g \in G$, a A-*órbita* de g é o conjunto $g^A = \{g^\alpha;\ \alpha \in A\}$. Se $g^\alpha \neq g$, para todo $\alpha \in A \backslash \{Id_G\}$, a A-órbita g^A é dita *regular*.

Como se trata de uma ação, G é particionado em A-órbitas disjuntas. Quando $g^\alpha = g$ para todo $\alpha \in A$, a órbita de g é unitária, ou seja, $g^A = \{g\}$. Dado $H \leqslant G$, o subconjunto $C_H(A) = \{h \in H;\ h^\alpha = h, \forall \alpha \in A\}$ é o "maior" subgrupo de G contido em H tal que as órbitas de $C_H(A)$ são unitárias, ou seja, A age trivialmente sobre $C_H(A)$. Se $C_H(A) = H$, diz-se que A *centraliza* H ou que H é *centralizado* por A. De modo análogo ao conjunto $C_H(A)$, define-se o subconjunto $C_A(H)$ de A colocando $C_A(H) = \{\alpha \in A;\ h^\alpha = h, \forall h \in H\}$. Esse é o "maior" subgrupo de A que centraliza H.

Definição 2.2. Um subgrupo H de G é dito A-*invariante* se para todo $h \in H$ e todo $\alpha \in A$ tem-se $h^\alpha \in H$.

Em um subgrupo A-invariante H de G, pode-se induzir um grupo de automorfismos de H por A. É o que mostra a

Proposição 2.3. *([6]) Se H é um subgrupo A-invariante de G, então existe um subgrupo $A|_H$ de $Aut(H)$ tal que $A|_H \simeq A/C_A(H)$.*

Demonstração. Defina $\varphi : A \to Aut(H)$ por $(\alpha)\varphi = \alpha|_H$, para todo $\alpha \in A$. Como H é A-invariante, $H^\alpha = H$, logo $\alpha|_H \in Aut(H)$, isto é, φ está bem definida. É imediato que $Nuc(\varphi) = C_A(H)$. Denote $A|_H = Im(\varphi)$ e, assim, pelo Primeiro Teorema do Isomorfismo, $A|_H \simeq A/C_A(H)$. $\square$

Uma seção H/K de G é dita A-invariante se K e H são subgrupos A-invariantes de G. Assim, cada $\alpha \in A$ induz um automorfismo $\overline{\alpha}$ de H/K, dado por $(hK)^{\overline{\alpha}} = h^\alpha K$ para todo $hK \in H/K$. É simples mostrar que $\overline{\alpha}$ está bem definido e que $\overline{\alpha} \in Aut(H/K)$. Defina $C_{H/K}(A) = \{hK; (hK)^{\overline{\alpha}} = hK, \forall \alpha \in A\}$ e $C_A(H/K) = \{\alpha \in A;\ \overline{\alpha} = Id_{H/K}\}$, assim, tem-se a seguinte proposição análoga à anterior, cuja demonstração é também análoga.

Proposição 2.4. *([6]) Se H/K é uma seção A-invariante de G, então existe um subgrupo $\overline{A}$ de $Aut(H/K)$ tal que $\overline{A} \simeq A/C_A(H/K)$.*

Desta proposição segue um resultado que será muito utilizado no decorrer dessas notas.

Proposição 2.5. *([6]) Se H/K é uma seção finita A-invariante de G, então o subgrupo $C_A(H/K)$ possui índice finito em A.*

Demonstração. Tem-se que $C_A(H/K) = Nuc(\varphi)$, em que $\varphi : A \to Aut(H/K)$ é dada por $(\alpha)\varphi = \overline{\alpha}$ com $(hK)^{\overline{\alpha}} = h^\alpha K$. Pela Proposição 2.4 segue que $A/C_A(H/K) \simeq \overline{A}$, com $\overline{A}$ um grupo de automorfismos de H/K. Como $Aut(H/K)$ é finito, segue que $\overline{A}$ é também finito, logo $A/C_A(H/K)$ é finito. O resultado segue. $\square$

Considere um subconjunto não vazio X do grupo G. É imediato ver que o subgrupo $X^A = \langle x^\alpha ; x \in X, \alpha \in A\rangle$ é o menor subgrupo A-invariante de G que contém X. Logo, dado $H \leqslant G$, se H é A-invariante, o subgrupo H^A é igual a H. Dados $g \in G$ e $\alpha \in A$, será usada a notação $[g, \alpha]$ para designar o elemento $g^{-1}g^\alpha$ de G. Nesses termos, define-se o subgrupo $[X, A] = \langle [x, \alpha]; x \in X, \alpha \in A\rangle$ de X^A. Note que $[x, \alpha]^{-1} = [x^\alpha, \alpha^{-1}]$, para todos $x \in X$ e $\alpha \in A$.

Proposição 2.6. *([6]) Se H é um subgrupo A-invariante de G, então $[H, A]$ é o "menor" subgrupo normal de H tal que $h^\alpha[H, A] = h[H, A]$, para todo $\alpha \in A$, ou seja, tal que A centraliza o grupo quociente $H/[H, A]$.*

Demonstração. Sejam $h \in H$ e $k \in [H, A]$. Logo, existem $k_1, ..., k_r \in H$ e $\alpha_1, ..., \alpha_r \in A$, com r inteiro positivo, tais que $k = k_1^{-1}k_1^{\alpha_1}...k_r^{-1}k_r^{\alpha_1}$. Assim,

$$h^{-1}kh = h^{-1}k_1^{-1}k_1^{\alpha_1}...k_r^{-1}k_r^{\alpha_1}h = (k_1h)^{-1}(k_1h)_1^{\alpha_1}h^{-\alpha_1}k_2^{-1}k_2^{\alpha_2}...k_r^{-1}k_r^{\alpha_1}h =$$

$$= (k_1h)^{-1}(k_1h)_1^{\alpha_1}(k_2h^{\alpha_1})^{-1}(k_2h^{\alpha_1})^{\alpha_2}h^{\alpha_1\alpha_2}...k_r^{-1}k_r^{\alpha_1}h =$$

$$= (k_1h)^{-1}(k_1h)_1^{\alpha_1}(k_2h^{\alpha_1})^{-1}(k_2h^{\alpha_1})^{\alpha_2}...(k_rh^{\alpha_1\alpha_2...\alpha_{r-1}})^{-1}(k_rh^{\alpha_1\alpha_2...\alpha_{r-1}})^{\alpha_r}h^{-\alpha_1\alpha_2...\alpha_r}h,$$

ou seja, $h^{-1}kh \in [H, A]$. Logo $[H, A] \lhd H$. Claramente $h^\alpha[H, A] = h[H, A]$, para todo $\alpha \in A$. Suponha agora que A centraliza o quociente H/K, com K normal em H. Desta forma, para todo $h \in H$ e $\alpha \in A$ segue que $h^\alpha K = hK$, ou seja, $h^{-1}h^\alpha \in K$. Como h e α são quaisquer, $[H, A] \lhd K$. $\square$

Definição 2.7. Um automorfismo $\alpha \in A$ é dito ser FPF (*"fixed-point-free"*), ou seja, *livre de pontos fixos*, se $C_G(\alpha) = \{g \in G;\ g^\alpha = g\} = \{1\}$. Se α é FPF para todo $\alpha \in A$, então A é dito ser FPF.

Exemplo 2.8. Sejam K um corpo, $G = K^+$ o grupo aditivo de K, $K^\times$ o grupo multiplicativo das unidades de K e T um subgrupo de $K^\times$. Considere para cada $t \in T$ o automorfismo $\alpha_t : G \to G$ definido por $(g)\alpha_t = gt$, para todo $g \in G$. Assim, $A_T = \{\alpha_t; t \in T\}$ é tal que $A_T \simeq T$ e $A_T \leqslant Aut(G)$. É fácil verificar que A_T é livre de pontos fixos.

Se $\alpha \in Aut(G)$, a função $T_\alpha : G \to G$ dado por $(g)T_\alpha = [g, \alpha]$, para todo $g \in G$, é *chamada função associada a α*. O automorfismo α é chamado *uniforme* se T_α é sobrejetor.

Tem-se claramente que α é FPF se, e somente se, T_α é injetivo. O mesmo não ocorre para a sobrejetividade de T_α. Por exemplo, se $G = \mathbb{Z}$ e $\imath$ é o automorfismo de G tal que $(k)\imath = -k$, para todo $k \in \mathbb{Z}$, segue que $\imath$ é FPF, mas não é uniforme.

2.2 Grupos de Automorfismos com um Número Finito de Órbitas

Na seção anterior, foi observado que se G é um grupo e A um grupo de automorfismos de G, então o grupo G é particionado em órbitas disjuntas, ou seja, existem um conjunto de índices I e $g_i \in G$, para todo $i \in I$, tais que $G = \biguplus_{i\in I} g_i^A$. Quando I é finito, existem um inteiro positivo n e elementos $g_1, ..., g_n$ em G tais que $G = \biguplus_{i=1}^n g_i^A$. Neste caso, diz-se que A *age sobre G por um número finito de órbitas.*

Exemplo 2.9. Seguindo o Exemplo 2.8, se o subgrupo T tem índice finito n em $K^\times$, tome $\{t_1, ..., t_n\}$ um transversal à direita de T em $K^\times$, logo $G = \{0\} \bigcup \biguplus_{i=1}^n t_i^{A_T}$. Assim A_T age sobre G por $|K^\times : T| + 1$ órbitas.

Daqui para frente, G denotará um grupo, A um grupo de automorfismos de G que age por um número finito n de A-órbitas, $g_1, ..., g_n \in G$ serão tais que $G = \biguplus_{i=1}^n g_i^A$, com $g_1 = 1$ e H denotará um subgrupo A-invariante de G. Quando não houver ambiguidade, será usado o mesmo signo A para designar o próprio A, $A|_H$ e $\overline{A}$. Com essas convenções, segue o seguinte resultado imediato:

Proposição 2.10. *([6]) Tem-se que:*

(i) H é uma união de um número $n_0 \leqslant n$ de A-órbitas e se $H < G$ tem-se $n_0 < n$;

(ii) Se H é normal em G, então G/H é uma união de um número $\overline{n} \leqslant n$ de A-órbitas e se $\{1\} < H$ tem-se $\overline{n} < n$;

(iii) Se B é um subgrupo de índice finito em A, então G é uma união de um número finito n' de B-órbitas, com $n' \leqslant (n-1)|A : B| + 1$. Se A é FPF, então vale a igualdade.

Demonstração. Os itens (i) e (ii) são imediatos. Para a primeira parte do item (iii), basta ver que $G = \biguplus_{1=1}^{n} g_i^A$, com $g_1 = 1$, e que existem um inteiro positivo r e $\alpha_1, ...\alpha_r \in A$ tais que $A = \biguplus_{j=1}^{r} \alpha_j B$, assim, $G = \biguplus_{1=1}^{n} g_i^A = \{1\} \cup \bigcup_{i=2}^{n} \bigcup_{j=1}^{r} (g_i^{\alpha_j})^B$, ou seja, G é uma união de um número finito n' de B-órbitas, com $n' \leqslant (n-1)|A : B| + 1$. Suponha, agora, que A é FPF e que $(g_i^{\alpha_j})^B = (g_i^{\alpha_{j'}})^B$, com $j \neq j'$, para algum i. Assim, existe $\beta \in B$ tal que $g_i^{\alpha_j \beta \alpha_{j'}^{-1}} = g_i$, mas, A é FPF, logo $\alpha_j \beta = \alpha_{j'}$, absurdo. A segunda parte de (iii) segue. □

Pelo item (i) da proposição acima, segue que a quantidade de subgrupos A-invariantes de G é finita, não podendo exceder 2^n. Pelo mesmo item segue, em particular, que G' e $Z(G)$ são uniões de quantidades finitas de A-órbitas, pois ambos são A-invariantes. Usando a proposição anterior segue o primeiro resultado significativo desta seção que é devido a *Enrico Jabara*, (veja [8]).

Teorema 2.11. *([8]) Um elemento α de $\widehat{Z}(A)$ é FPF se, e somente se, α é uniforme.*

Demonstração. Por hipótese $\alpha \in \widehat{Z}(A)$, logo $|A : C_A(\alpha)| < \infty$. Denotando $A_1 = C_A(\alpha)$, pela Proposição 2.10-(iii), G é uma união de um número finito de A_1-órbitas.

Suponha que α é FPF e seja $g \in G$. Assim a função T_α associado a α é injetiva. Note que $(z^{A_1})T_\alpha = ((z)T_\alpha)^{A_1}$, para todo $z \in G$. Além disso, se $x, y \in G$ com $((x)T_\alpha)^{A_1} = ((y)T_\alpha)^{A_1}$, existe $\beta \in A_1$ tal que $(x)T_\alpha = ((y)T_\alpha)^\beta$ e, assim,

$$x^{-1}x^\alpha = (y^{-1}y^\alpha)^\beta = y^{-\beta}y^{\alpha\beta}$$

e

$$y^\beta x^{-1} = y^{\alpha\beta}x^{-\alpha} = y^{\beta\alpha}x^{-\alpha} = (y^\beta x^{-1})^\alpha$$

Mas, por hipótese α é FPF, logo $x = y^\beta$, donde $x^{A_1} = y^{A_1}$. Daí, T_α induz uma função injetora $\overline{T}_\alpha : \{z^{A_1};\ z \in G\} \to \{z^{A_1};\ z \in G\}$ tal que $z^{A_1} \mapsto (z^{A_1})T_\alpha$, para todo $z \in G$. Como existem finitas A_1-órbitas, essa função também é sobrejetora. Disto, segue que existe $h \in G$ tal que $g^{A_1} = (h^{A_1})\overline{T}_\alpha = (h^{A_1})T_\alpha = ((h)T_\alpha)^{A_1}$. Tome $\gamma \in A_1$ tal que $g = ((h)T_\alpha)^\gamma$, logo $g = (h^\gamma)T_\alpha$. Portanto, α é uniforme.

Reciprocamente, suponha, por absurdo, que exista $g \in G \backslash \{1\}$ tal que $g^\alpha = g$. Defina indutivamente uma sequência $(x_n)_{n \in \mathbb{N}}$ de elementos de G, pondo $x_0 = 1$, $x_1 = g$ e, para

$n > 1$, escolha um elemento x_n de G tal que $(x_n)T_\alpha = x_{n-1}$. Isso é possível, pois α é uniforme. Note que $x_n \neq 1$, para todo $n > 1$. Como G é uma união de um número finito de A_1-órbitas, existem índices $i < j$ tais que $x_i^{A_1} = x_j^{A_1}$. Considere $\beta \in A_1$ tal que $x_j = x_i^\beta$, assim $x_i = (x_j)T_\alpha^{j-i} = (x_i^\beta)T_\alpha^{j-i} = ((x_i)T_\alpha^{j-i})^\beta$. Mas, $(x_i)T_\alpha^{j-1} = ((x_i)T_\alpha^i)T_\alpha^{j-1-i} = (1)T_\alpha^{j-1-i} = 1$, pois $j-1 \geqslant i$ e, assim, $1 \neq x_i = ((x_i)T_\alpha^{j-1})^\beta = 1$, uma contradição. Portanto α é FPF. $\square$

A seguir um resultado imediato deste teorema.

Corolário 2.12. *([13]) Suponha que G é infinito, A é FPF e que A contém um FC-subgrupo de índice finito. Se B é um subgrupo de índice finito em A, então G não contém subgrupo B-invariante próprio e não trivial .*

Demonstração. Suponha inicialmente que $B \leqslant \widehat{Z}(A)$ e A é FPF. Pelo Teorema 2.11 segue que cada elemento de B é uniforme. Seja $\{1\} < H \leqslant G$ um subgrupo B-invariante. Suponha agora, por contradição, que H é finito. Como A é infinito, existem $h \in H \backslash \{1\}$ e $\alpha_1, \alpha_2 \in A$, com $\alpha_1 \neq \alpha_2$, tais que $h^{\alpha_1} = h^{\alpha_2}$, ou seja, $h^{\alpha_1 \alpha_2^{-1}} = h$. Mas, A é FPF, então $\alpha_1 = \alpha_2$, absurdo. Logo H é infinito e, assim, gH também é infinito para cada $g \in G$. Tome agora $x \in G$. O número de B-órbitas é finito, com isto, existem $\beta \in B \backslash \{Id_G\}$ e $h_1, h_2 \in H$ tais que $(xh_1)^\beta = xh_2$ e, daí, $x^\beta \in xH$, ou seja, $x^{-1}x^\beta \in H$. Como β é uniforme, segue que existe $h \in H$ tal que $x^{-1}x^\beta = h^{-1}h^\beta$. Logo $(hx^{-1})^\beta = hx^{-1}$ e, uma vez que A é FPF, $x = h$. Então, $H = G$ e, assim, G não possui subgrupo B-invariante próprio e não trivial. Agora se $B \nleqslant \widehat{Z}(A)$, então $B \cap \widehat{Z}(A) \leqslant \widehat{Z}(A)$ possui índice finito em A, pois por hipótese, existe um FC-subgrupo A^* de A de índice finito e, assim, $A^* \leqslant \widehat{Z}(A)$, logo pela primeira parte, o resultado segue. $\square$

Quando A é FPF e FC-grupo, pelo Teorema 2.11, cada α de $A \backslash \{Id_G\}$ é uniforme. Neste caso é possível obter informações sobre a natureza do grupo G.

Teorema 2.13. *([8]) Se G é infinito e o grupo de automorfismos A é FC-grupo e FPF, então G é abeliano e ocorre somente um dos seguintes casos:*

(a) G é de torção: em tal caso, G é um p-grupo abeliano elementar, para algum primo p;

(b) G é livre de torção: em tal caso, G é divisível.

Demonstração. Se $g \in G\backslash\{1\}$, então conjugados distintos de g pertencem a A-órbitas distintas. De fato, suponha, por absurdo, que exista $h \in G$ tal que $h^{-1}gh \in g^A$ e $g \neq h^{-1}gh$. Seja $\alpha \in A\backslash\{Id_G\}$ com $g^\alpha = h^{-1}gh$. Como α é automorfismo uniforme, existe $k \in G$ tal que $h = k^{-1}k^\alpha$, assim $g^\alpha = k^{-\alpha}kgk^{-1}k^\alpha$ e $(kgk^{-1})^\alpha = kgk^{-1}$. Uma contradição, pois $g \neq 1$ e α é FPF. Se g^v e g^u, com u e $v \in G$, pertencem a uma mesma A-órbita, existe $\alpha \in A\backslash\{Id_G\}$ tal que $g^v = ((g^v)^{v^{-1}u})^\alpha$, absurdo pela primeira parte. Como existem apenas n A-órbitas, $|G : C_G(x)| \leqslant n$ para todo $x \in G$, ou seja, G é BFC-grupo. Assim, pelo Teorema 1.40, G' é finito. Mas, G' é A-invariante, logo é uma união de um número finito de A-órbitas e, como uma A-órbita não trivial é infinita, pois A é FPF e infinito, segue que G' é uma A-órbita trivial. Logo $G' = \{1\}$ e, consequentemente, G é abeliano.

Suponha que exista um elemento de torção não trivial em G. Logo existem $y \in G\backslash\{1\}$ e um primo p tais que $y^p = 1$. Seja $x \in G\backslash\{1\}$. Considere o subconjunto $\{xy^\alpha;\ \alpha \in A\}$ infinito de G. Como G é uma união de um número finito de A-órbitas, existem $\alpha_1, \alpha_2 \in A$, $\alpha_1 \neq \alpha_2$ e $\beta \in A\backslash\{Id_G\}$ tais que $xy^{\alpha_1} = (xy^{\alpha_2})^\beta$. Logo $x^p = (xy^{\alpha_1})^p = ((xy^{\alpha_2})^\beta)^p = (x^p)^\beta$ e, assim, $x^p = 1$, pois β é FPF. Portanto, G é um p-grupo abeliano elementar.

Suponha agora que G é livre de torção. Sejam $x \in G\backslash\{1\}$ e n um inteiro positivo. Como a ordem de x não é finita, segue que $\{x^{n^i};\ i \in \mathbb{N}\}$ é um subconjunto infinito de G. Assim existem $i < j$ inteiros positivos e $\alpha \in A\backslash\{Id_G\}$ tais que $x^{n^j} = (x^{n^i})^\alpha$, donde $x^\alpha = x^{n^{j-i}}$. Fazendo $y = (x^{n^{j-i-1}})^{\alpha^{-1}}$, segue que $y^n = x$. O resultado segue. □

Com as hipóteses do Corolário 2.12 e usando o teorema anterior, *Martin R. Pettet*, em [13], demonstra que é possível associar um corpo K ao grupo G de tal forma que $G \simeq K^+$ (o grupo aditivo de K). Esse é o próximo resultado.

Teorema 2.14. *([13]) Suponha que G é infinito e A é FPF. Se A contém um FC-subgrupo de índice finito, então existe um corpo K tal que:*

(i) $G \simeq K^+$;

(ii) O subgrupo $\widehat{Z}(A)$ é isomorfo a um subgrupo do grupo multiplicativo $K^\times$ de índice finito $(n-1)|A : \widehat{Z}(A)|$;

(iii) $A/\widehat{Z}(A)$ é isomorfo a um grupo $\mathcal{A}$ de automorfismos do corpo K;

Demonstração. Seja B um FC-subgrupo de A de índice finito. Pela Proposição 2.10, G é uma união de um número finito de B-órbitas e, como B é FC-grupo e FPF, pois A é FPF, do Teorema 2.13 segue que G é abeliano. Assim, se $\theta, \eta \in End(G) = \{\alpha;\ \alpha$ é um endomorfismo de $G\}$, então a função $\theta + \eta : G \to G$ dada por $g^{\theta+\eta} = g^\theta g^\eta$, para todo $g \in G$, é um endomorfismo de G. Não é difícil ver que $End(G)$ com a operação de adição definida acima e a operação de composição de funções é um anel. Considere o subconjunto K de $End(G)$ dado por $K = \{\theta \in End(G);\ |A : C_A(\theta)| < \infty\}$, onde $C_A(\theta) = \{\alpha \in A; \alpha\theta = \theta\alpha\}$. É fácil ver que K é um subanel de $End(G)$ contendo $\widehat{Z}(A)$. Seja $\theta \in K \backslash \{\mathbf{0}\}$, assim $C_A(\theta)$ é um subgrupo de índice finito em A e $Nuc(\theta)$, $Im(\theta)$ são subgrupos $C_A(\theta)$-invariantes de G. Do Corolário 2.12 segue que $Nuc(\theta) = 1$ e $Im(\theta) = G$, ou seja, $\theta \in Aut(G)$. Logo K é um anel com divisão. Além disso, $K^\times$ é FPF, pois se $\theta \in K^\times \backslash \{Id_G\}$, então $\theta - Id_G \in K^\times$ e, assim, $\theta - Id_G$ possui núcleo trivial.

Para concluir que K é um corpo falta apenas mostrar que o grupo $K^\times$ é abeliano. De fato, sejam $\theta \in K^\times$ e $g \in G\backslash\{1\}$. Se $H = g^{C_K(\theta)} = \{g^\eta;\ \eta \in C_K(\theta)\}$, então $H \leqslant G$, pois $C_K(\theta)$ é um grupo aditivo. Além disso, H é $C_{K^\times}(\theta)$-invariante, assim é $C_{\widehat{Z}(A)}(\theta)$-invariante. Pelo Corolário 2.12, $H = G$. Tome agora $\epsilon \in K^\times$, assim existe $h \in G$ tal que $h^\epsilon = g$. Como $H = G$, existe $\eta \in C_{K^\times}(\theta)$ tal que $g^\eta = h$ e, assim, $g^{\eta\epsilon} = g$. Como $\eta\epsilon \in K^\times$ e $K^\times$ é FPF segue que $\eta\epsilon = Id_G$ e $\epsilon \in C_{K^\times}(\theta)$. Portanto, $C_{K^\times}(\theta) = K^\times$ e uma vez que θ é arbitrário, o grupo $K^\times$ é abeliano.

Agora $G \simeq K^+$, pois, fixado $g \in G\backslash\{1\}$, vem que $\varphi : K^+ \to G$ dada por $\theta \mapsto g^\theta$, para todo $\theta \in K^+$, é um isomorfismo. De fato, pelo parágrafo anterior, claramente φ é homomorfismo sobrejetor e se $\theta_1, \theta_2 \in K^+$ são tais que $g^{\theta_1} = g^{\theta_2}$ segue que $\theta_1 - \theta_2 = \mathbf{0}$, isto é, $\theta_1 = \theta_2$. Fica, assim, demonstrado o item (i).

Como $|A : B| < \infty$ e $B \leqslant \widehat{Z}(A)$, segue que o grupo $\widehat{Z}(A)$ possui índice finito em A e uma vez que A é FPF, pela Proposição 2.10, o grupo G é uma união de $s = (n-1)|A : \widehat{Z}(A)| + 1$ $\widehat{Z}(A)$-órbitas. Logo, existem $h_2, ..., h_s \in G\backslash\{1\}$ tais que $G\backslash\{1\} = \biguplus_{i=2}^s h_i^{\widehat{Z}(A)}$. Se $\theta \in K^\times$, existe um único $i \in \{2, ..., s\}$ e um único $\alpha \in \widehat{Z}(A)$ tais que $g^\theta = h_i^\alpha$. Pelo isomorfismo φ, existe um único $\theta_i \in K^\times$ tal que $h_i^{\theta_i^{-1}} = g$, logo $\theta = \alpha\theta_i$. Portanto, $K^\times = \biguplus_{i=2}^s \widehat{Z}(A)\theta_i$. Isto prova o item (ii).

Uma vez que $\widehat{Z}(A) \leqslant K^\times$ e $|A : \widehat{Z}(A)| < \infty$ segue que $C_A(K^\times) = \widehat{Z}(A)$. De fato, claramente $\widehat{Z}(A) \leqslant C_A(K^\times)$. Por outro lado, tem-se $C_A(K^\times) \leqslant C_A(\widehat{Z}(A))$. Suponha, por absurdo, que exista $\alpha \in A \backslash \widehat{Z}(A)$ tal que $\alpha\theta = \theta\alpha$ para todo $\theta \in \widehat{Z}(A)$. Seja $\{\beta_1, ..., \beta_{|A:\widehat{Z}(A)|}\}$ um transversal à direita de $\widehat{Z}(A)$ em A. Logo, se $\beta \in A$, existem $i \in \{1, ..., |A : \widehat{Z}(A)|\}$ e $\omega \in \widehat{Z}(A)$ tais que $\beta = \omega\beta_i$ e, assim, $\beta^{-1}\alpha\beta = (\omega\beta_i)^{-1}\alpha(\omega\beta_i) = \beta_i^{-1}\alpha\beta_i$, ou seja, $|\{\alpha^\beta; \beta \in A\}| \leqslant |A : \widehat{Z}(A)|$, uma contradição, pois $\alpha \notin \widehat{Z}(A)$. Resulta que $C_A(\widehat{Z}(A)) = \widehat{Z}(A)$ e, consequentemente, $C_A(K) \leqslant \widehat{Z}(A)$. Defina agora $\phi : A \to Aut(K)$ por $\alpha \mapsto \phi_\alpha$, para todo $\alpha \in A$, com $\phi_\alpha : K \to K$ dado por $\beta \mapsto \alpha^{-1}\beta\alpha$, para todo $\beta \in K$. Claramente ϕ é um homomorfismo, cujo núcleo é $\widehat{Z}(A)$. Portanto, se $\mathcal{A} = Im(\phi)$, segue pelo Primeiro Teorema do Isomorfismo que $A/\widehat{Z}(A) \simeq \mathcal{A}$, demonstrando assim (iii). □

Em particular, se, além das hipóteses do Teorema 2.14, A é FC-grupo, tem-se o seguinte:

Corolário 2.15. *([13]) Suponha que G é infinito e que A é FPF. Se A é FC-grupo, então existe um corpo K tal que:*

(i) $G \simeq K^+$;

(ii) A é isomorfo a um subgrupo com índice finito $n - 1$ no grupo multiplicativo $K^\times$;

(iii) Identificando G com K^+, a ação de A sobre G é a multiplicação em K.

Demonstração. Seguindo as notações do teorema anterior, os itens (i) e (ii) seguem direto. Agora, seja $h \in G \backslash \{1\}$. Identificando G com K^+ pelo isomorfismo $\varphi : K^+ \to G$, dado por $\theta \mapsto h^\theta$, para cada $g \in G$, existe $\theta \in K^+$ tal que $g = h^\theta$. Logo, se $\alpha \in A$, então α leva g em $g^\alpha = h^{\theta\alpha}$. Daí, α pode ser dado por $\alpha : h^\theta \mapsto h^{\theta\alpha}$. Seja $\psi : A \to Aut(K^+)$, definido por $\beta \mapsto \psi_\beta$, onde $\psi_\beta : K^+ \to K^+$ é tal que $(\theta)\psi_\beta = \theta\beta$, para todo $\theta \in K^+$. É claro que ψ é um homomorfismo injetor. Portanto, A se identifica com o subgrupo $Im(\psi) = \{\psi_\beta;\ \beta \in A\}$ de $Aut(K^+)$. Como esperado. □

Será usado o símbolo $\mathcal{L}_A(G)$ para representar o conjunto de todos os subgrupos A-invariantes de G. Pela Proposição 2.10 esse conjunto é finito. Se H é um subgrupo A-invariante de G, define-se os subconjuntos $I_G^A(H)$, $S_G^A(H)$ de $\mathcal{L}_A(G)$, respectivamente, por:

$$I_G^A(H) = \{K \in \mathcal{L}_A(G); K \leqslant H, |H : K| < \infty\}$$

e

$$S_G^A(H) = \{K \in \mathcal{L}_A(G); H \leqslant K, |K : H| < \infty\}.$$

Definição 2.16. Seja H um subgrupo A-invariante de G. O *mínimo* e o *máximo* de H em relação a A e G são dados, respectivamente, por

$$min_G^A(H) = \bigcap_{K \in I_G^A(H)} K$$

e

$$max_G^A(H) = \langle K;\ K \in S_G^A(H)\rangle.$$

Claramente a interseção e o subgrupo gerado por subgrupos A-invariantes são também A-invariantes. Logo $min_G^A(H)$ e $max_G^A(H)$ são A-invariantes. Como $\mathcal{L}_A(G)$ é finito, os conjuntos $I_G^A(H)$ e $S_G^A(H)$ são também finitos, para todo $H \in \mathcal{L}_A(G)$. Assim, fica claro que $|H : min_G^A(H)| < \infty$. O próximo resultado mostra que isso também ocorre para $max_G^A(H)$.

Proposição 2.17. *([6]) Para todo $H \in \mathcal{L}_A(G)$ tem-se que $min_G^A(H)$ é um subgrupo normal de $max_G^A(H)$, com índice finito.*

Demonstração. Uma vez que $|H : min_G^A(H)| < \infty$, pela Proposição 1.2, segue que o "core" $(min_G^A(H))_H$ de $min_G^A(H)$ em H possui índice finito em H. E como esse "core" é também A-invariante, tem-se que $(min_G^A(H))_H = min_G^A(H)$ e, então, $min_G^A(H)$ é normal em H. Agora, dados H_1 e H_2 em $\mathcal{L}_A(G)$, tais que $H_1 \leqslant H_2$ e $|H_2 : H_1| < \infty$, claramente, deve-se ter $min_G^A(H_1) = min_G^A(H_2)$; em particular, para cada $K \in S_G^A(H)$ deve-se ter $min_G^A(K) = min_G^A(H)$ e, assim, $min_G^A(H)$ é normal em cada $K \in S_G^A(H)$, logo normal em $max_G^A(H)$.

Suponha que $S_G^A(H) = \{K_1, ..., K_s\}$, com s um número inteiro positivo. Para cada $i \in \{1, ..., s\}$ tem-se que $K_i/min_G^A(H)$ é uma seção A-invariante finita de G e, assim, pela Proposição 2.5, $A_i = C_A(K_i/min_G^A(H))$ é um subgrupo de A de índice finito. Logo, o subgrupo $B = \bigcap_{i=1}^s A_i$ também possui índice finito em A. Como G é uma união de um número finito de A-órbitas segue, pela Proposição 2.10, que G é uma união de um número finito de B-órbitas. Mas, B centraliza cada seção $K_i/min_G^A(H)$ e, assim, centraliza $max_G^A(H)/min_G^A(H)$. Sendo $max_G^A(H)/min_G^A(H)$ uma união de um número finito de B-órbitas segue que é finito. □

Segue da proposição anterior que $|max_G^A(H) : H| < \infty$, para todo $H \in \mathcal{L}_A(G)$.

Proposição 2.18. *Sejam $H, K \in \mathcal{L}_A(G)$ tais que $H \leqslant K$. Então, $max_G^A(H) = max_G^A(K)$ se, e somente se, $|K : H| < \infty$.*

Demonstração. Suponha que $|K : H| < \infty$. É claro que $S_G^A(K) \subseteq S_G^A(H)$ e, assim, $max_G^A(K) \leqslant max_G^A(H)$. Para mostrar a implicação contrária, seja $L \in S_G^A(H)$ e considere o subgrupo $M = \langle K \cup L \rangle$. É claro que M é A-invariante e $H \leqslant M \leqslant max_G^A(H)$, pois $K, L \in S_G^A(H)$. Como $|max_G^A(H) : H| < \infty$, segue que $|M : H| < \infty$ e, consequentemente, $|M : K| < \infty$. Logo $L \leqslant M \leqslant max_G^A(K)$, para todo $L \in S_G^A(H)$ e, portanto, $max_G^A(H) = max_G^A(K)$.

Reciprocamente, suponha, por absurdo, que $|K : H|$ é infinito. Então, $|max_G^A(K) : H|$ é infinito e, como $|max_G^A(H) : H|$ é finito, segue que $max_G^A(H) \neq max_G^A(K)$, absurdo □

Uma consequência imediata desta proposição é a

Proposição 2.19. *Se $H, K \in \mathcal{L}_A(G)$ e os índices $|H : H \cap K|$ e $|K : H \cap K|$ são finitos, então $max_G^A(H) = max_G^A(K)$.*

Um outro fato interessante que segue da Proposição 2.17 é que se B é um subgrupo de índice finito em A, então os subconjuntos definidos na Definição 2.16 em relação a B são iguais aos respectivos, em relação a A, como mostra a

Proposição 2.20. *([6]) Se B é um subgrupo de índice finito em A, então para cada $H \in \mathcal{L}_A(G)$ tem-se que $min_G^B(H) = min_G^A(H)$ e $max_G^B(H) = max_G^A(H)$.*

Demonstração. Não há perda de generalidade em supor que B é um subgrupo normal de A, pois, se acontecer o contrário, basta tomar B_A, o "core" de B em A, que possui índice finito em A, já que B possui índice finito em A. Sejam $M = min_G^A(H)$ e $M_1 = min_G^B(H)$. Claramente $M_1 \leqslant M$. Sejam $\alpha_1, ..., \alpha_n \in A$, com $n = |A : B|$, tais que $A = \biguplus_{i=1}^n B\alpha_i$. Assim o conjunto $\{M_1^\alpha; \alpha \in A\}$ é finito e igual a $\{M_1^{\alpha_i}; i = 1, ..., n\}$. Uma vez que H é A-invariante e $|H : M_1| < \infty$ tem-se que $|H : M_1^{\alpha_i}| < \infty$, para todo $i = 1, ..., n$. Logo, $M_2 = \bigcap_{i=1}^n M_1^{\alpha_i}$ é um subgrupo A-invariante que possui índice finito em H. Assim, pela Proposição 2.17, $M = min_G^A(H) = min_G^A(M) = min_G^A(M_2) \lhd M_2$ e, como $M_2 \leqslant M_1$, segue que $M \leqslant M_1$. Portanto, $min_G^B(H) = min_G^A(H)$.

Agora, considere M como acima, $K = max_G^A(H)$ e $K_1 = max_G^B(H)$. Claramente $K \leqslant K_1$. Pela Proposição 2.17 os índices $|K : M|$ e $|K_1 : M|$ são finitos e $M \lhd K_1$. Considere N o normalizador de M em G, ou seja, $N = N_G(M)$ e $\overline{N} = N/M$. Com isso, $\overline{K_1} = K_1/M$ é um subgrupo finito de $\overline{N}$. Assim, para cada $i = 1, ..., n$, o subgrupo $\overline{K_1^{\alpha_i}} = K_1^{\alpha_i}/M$ também é finito em $\overline{N}$. Para cada $i = 1, ..., n$, seja $B_i = C_B(\overline{K_1^{\alpha_i}})$, que possui índice finito em B, em virtude da Proposição 2.5. Com isso, $\overline{B} = \bigcap_{i=1}^n B_i$ possui índice finito em B. Uma vez que $\overline{B}$ centraliza $\overline{K_1^{\alpha_i}}$ para cada $i = 1, ..., n$, $\overline{B}$ centraliza $\overline{K_2} = \langle \overline{K_1^{\alpha_i}};\ i = 1, ..., n\rangle$. Como $\overline{B}$ possui índice finito em B, então $\overline{K_2}$ é uma união de um número finito de $\overline{B}$-órbitas, daí, $\overline{K_2}$ é finito. Se K_2 é tal que $\overline{K_2} = K_2/M$, então $|K_2 : M| < \infty$ e, como $M \leqslant H \leqslant K_1 \leqslant K_2$ e K_2 é A-invariante, $K_2 \in S_G^A(H)$. Assim, $K_1 \leqslant K_2 \leqslant K$. Portanto, $max_G^B(H) = max_G^A(H)$. $\square$

Um *reticulado* é um par (L, R), em que L é um conjunto parcialmente ordenado por uma relação de ordem parcial R, tal que para todos os subconjuntos $\{l, k\}$ de L existem em L o *supremo* ($sup\{l, k\}$) e o *ínfimo* ($inf\{l, k\}$) de $\{l, k\}$. Por vezes, denota-se a estrutura (L, R) por $(L, \wedge, \vee)$, onde $l \wedge k = inf\{l, k\}$ e $l \vee k = sup\{l, k\}$. Dois reticulados $(L_1, \wedge_{L_1}, \vee_{L_1})$ e $(L_2, \wedge_{L_2}, \vee_{L_2})$ são isomorfos se existe uma bijeção $\varphi : L_1 \to L_2$ tal que se $a, b \in L_1$, então

$$(a \wedge_{L_1} b)\varphi = (a)\varphi \wedge_{L_2} (b)\varphi \quad \text{e} \quad (a \vee_{L_1} b)\varphi = (a)\varphi \vee_{L_2} (b)\varphi.$$

Assim, é um reticulado a estrutura $(\bar{\mathcal{L}}_A(G), \bar{\wedge}, \bar{\vee})$, em que $\bar{\mathcal{L}}_A(G) = \{max_G^A(H); H \in \mathcal{L}_A(G)\}$ e se $H_1, H_2 \in \bar{\mathcal{L}}_A(G)$, então $H_1 \bar{\wedge} H_2 = max_G^A(H_1 \cap H_2)$ e $H_1 \bar{\vee} H_2 = max_G^A(\langle H_1, H_2\rangle)$. Como também é um reticulado a estrutura $(\underline{\mathcal{L}}_A(G), \underline{\wedge}, \underline{\vee})$, em que $\underline{\mathcal{L}}_A(G) = \{min_G^A(H); H \in \mathcal{L}_A(G)\}$ e se $H_1, H_2 \in \underline{\mathcal{L}}_A(G)$, então $H_1 \underline{\wedge} H_2 = min_G^A(H_1 \cap H_2)$ e $H_1 \underline{\vee} H_2 = min_G^A(\langle H_1, H_2\rangle)$. Segue diretamente da Proposição 2.17 que os reticulados $(\bar{\mathcal{L}}_A(G), \bar{\wedge}, \bar{\vee})$ e $(\underline{\mathcal{L}}_A(G), \underline{\wedge}, \underline{\vee})$ são isomorfos.

Exemplo 2.21. Seja S_3 o grupo das permutações do conjunto $\{1, 2, 3\}$. Seja G o produto direto dos grupos $\mathbb{Q}^+$ e S_3. Defina para cada t em $\mathbb{Q}_{>0}$ o automorfismo $\alpha_t : G \to G$, pondo $(q, s)\alpha_t = (qt, s)$. Seja $A = \{\alpha_t;\ t \in \mathbb{Q}_{>0}\}$. Então, $A \leqslant Aut(G)$ e A age por multiplicação sobre $\mathbb{Q}^+$ e como a identidade sobre S_3. Observe que

$$G = \biguplus_{s \in S_3} (0, s)^A \uplus \biguplus_{s \in S_3} (1, s)^A \uplus \biguplus_{s \in S_3} (-1, s)^A,$$

ou seja, G é uma união de 18 A-órbitas. Como os A-invariantes de G são da forma $Q \times S$, onde $Q = \{0\}$ ou $Q = \mathbb{Q}^+$ e S é um subgrupo arbitrário de S_3, então

$$\bar{\mathcal{L}}_A(G) = \{\{0\} \times S_3, G\} \quad \text{e} \quad \underline{\mathcal{L}}_A(G) = \{\{1_G\}, \mathbb{Q} \times 1_{S_3}\}.$$

Definição 2.22. Seja m o comprimento máximo de uma cadeia em $(\bar{\mathcal{L}}_A(G), \bar{\wedge}, \bar{\vee})$ (ou equivalentemente em $(\underline{\mathcal{L}}_A(G), \underline{\wedge}, \underline{\vee})$). O *comprimento de G com respeito a A*, denotado por $\ell_A(G)$, é definido por $\ell_A(G) = m - 1$.

Esse comprimento revela um critério para determinar se o grupo G é finito ou infinito.

Proposição 2.23. *([6]) $\ell_A(G) = 0$ se, e somente se, G é finito.*

Demonstração. Suponha inicialmente que $\ell_A(G) = 0$. Assim, o comprimento máximo de uma cadeia em $(\bar{\mathcal{L}}_A(G), \bar{\wedge}, \bar{\vee})$ é 1. Desta forma, $\{max_G^A(H)\}$ é uma cadeia máxima para todo H A-invariante. Assim, se $H \leqslant G$, então $max_G^A(H) = G$ e, daí, $\{G\}$ é uma cadeia de comprimento máximo em $(\bar{\mathcal{L}}_A(G), \bar{\wedge}, \bar{\vee})$. Logo, $max_G^A(H) = G$ para todo subgrupo H de G A-invariante. Em particular $max_G^A(\{1\}) = G$, ou seja, G é finito pela Proposição 2.17. A recíproca é imediata. □

Lema 2.24. *Seja K um subgrupo A-invariante de índice finito em um grupo infinito G. Se $G_1, G_2 \in \bar{\mathcal{L}}_A(G)$ e $G_1 < G_2$, então $max_K^A(K \cap G_1) < max_K^A(K \cap G_2)$.*

Demonstração. Primeiro observe que se $H_1, H_2 \in \mathcal{L}_A(G)$ e $max_G^A(H_1) < max_G^A(H_2)$, então $|max_G^A(H_1) : max_G^A(H_2)|$ é infinito. Logo, como $G_1 < G_2$, tem-se $|G_2 : G_1| = \infty$. Suponha, por absurdo, que $max_K^A(K \cap G_1) = max_K^A(K \cap G_2)$. Uma vez que $|G_1 : K \cap G_1|, |G_2 : K \cap G_2| < \infty$, pela Proposição 2.18 tem-se que

$$max_G^A(G_1) = max_G^A(K \cap G_1) = max_G^A(K \cap G_2) = max_G^A(G_2),$$

ou seja, $|G_2 : G_1| < \infty$, um absurdo. □

Proposição 2.25. *Se K é um subgrupo A-invariante de índice finito no grupo G, então $\ell_A(K) = \ell_A(G)$.*

Demonstração. Se G é finito isso é claro. Caso contrário, seja $\{G_1, ..., G_{\ell_A(G)+1}\}$ uma cadeia de comprimento máximo em $\bar{\mathcal{L}}_A(G)$. Segue do lema anterior que

$$\{max_K^A(K \cap G_1), ..., max_K^A(K \cap G_{\ell_A(G)+1})\}$$

é uma cadeia de comprimento $\ell_A(G) + 1$ em $\bar{\mathcal{L}}_A(K)$ e, assim, $\ell_A(K) \geqslant \ell_A(G)$. Como claramente $\ell_A(K) \leqslant \ell_A(G)$. O resultado segue. $\square$

Capítulo 3

Grupos de Automorfismos Abelianos com um Número Finito de Órbitas

O objetivo principal deste capítulo é demonstrar o seguinte resultado:

Teorema A. *Sejam G um grupo infinito e A um subgrupo abeliano de $Aut(G)$ tais que G é uma união de um número finito de A-órbitas e A centraliza toda seção finita A-invariante de G. Então*

(a) G é abeliano-por-finito;

(b) Se G é livre de torção, então G é abeliano e divisível;

(c) O grupo A possui expoente infinito.

Este resultado responde, de uma maneira parcial, a seguinte questão levantada, em 1998, pelos matemáticos Peter M. Neumann e Peter J. Rowley, em [12]: *"O que se pode dizer sobre um grupo G que admite um grupo abeliano A de automorfismos de G tal que G é uma união de um número finito de A-órbitas?"*.

Na Seção 3.1, são estudados os grupos que admitem um grupo abeliano de automorfismos que age por uma quantidade finita de órbitas. A Seção 3.2 é dedicada para a demonstração do Teorema B, cujo enunciado é

Teorema B. *Sejam G um grupo abeliano infinito e A um grupo abeliano de automorfismos de G, tal que G é uma união de um número finito de A-órbitas e A centraliza toda seção finita A-invariante de G. Então existem um inteiro positivo r, subgrupos $B_1, ..., B_r$ de A e* *subgrupos A-invariantes $G_1, ..., G_r$ de G tais que $B = B_1 \times ... \times B_r$ possui índice finito em A, $G = C_G(A) \times G_1 \times ... \times G_r$ e*

(a) B_i age trivialmente sobre G_j, para todo $i \neq j$, com $i, j = 1, ..., r$;

(b) G_i é um subgrupo B_i-monolítico de G, para todo $i = 1, ..., r$.

Além disso, cada G_i ou é um p-grupo de expoente no máximo $\ell(G_i)$, para algum primo p, ou é um grupo livre de torção e divisível.

Finalizando, a Seção 3.2 é dedicada exclusivamente para a demonstração do Teorema A.

Todos os resultados deste capítulo são devidos a Enrico Jabara [6]; desta forma, não haverá citações, ficando assim subentendido que tais fatos são devidos a este autor.

3.1 Grupos de Automorfismos Abelianos

Nesta seção são incluídos alguns resultados sobre grupos que admite um grupo abeliano de automorfismos que age por uma quantidade finita de órbitas. Daqui até o final deste capítulo, G denotará um grupo que admite um grupo de automorfismos A, que age sobre G por um número finito n de A-órbitas, e $g_1, ..., g_n \in G$ são tais que $G = \biguplus_{i=1}^{n} g_i^A$, com $g_1 = 1$.

Definição 3.1. *O par (G, A) satisfaz a condição $(*)$ se*

$(*_1)$ G é infinito;

$(*_2)$ A é abeliano;

$(*_3)$ A centraliza cada seção finita A-invariante de G.

Exemplo 3.2. Sejam $G = \mathbb{Q} \times S_3$ e $A = \{\alpha_t;\, t \in \mathbb{Q}_{>0}\}$ como no Exemplo 2.21. Observe que o grupo G é infinito e não é abeliano, A é abeliano e A centraliza toda seção A-invariante finita de G, pois cada uma destas é da forma $(Q \times H_1)/(Q \times H_2)$, onde $Q = \{0\}$ ou $Q = \mathbb{Q}^+$ e H_1, H_2 são subgrupos de S_3 tais que $H_2 \lhd H_1$. Portanto, o par (G, A) satisfaz a condição $(*)$.

Proposição 3.3. *Suponha que o par (G, A) satisfaz a condição $(*)$, H é um subgrupo de G infinito e A-invariante, N um subgrupo normal de G A-invariante, com G/N infinito, $B \leqslant A$ de índice finito e $C = C_G(A)$. Então,* *(a) Os pares $(H, A), (G/N, A)$ e (G, B) satisfazem a condição $(*)$;*

(b) C é o "maior" subgrupo A-invariante finito de G. Em particular, todas as A-órbitas dos elementos de $G \backslash C$ são infinitas.

Demonstração. O item (a) é imediato. Que C é finito segue do fato que G é uma união de um número finito de A-órbitas. Agora sejam K um subgrupo finito A-invariante de G e $k \in K$. Como A centraliza toda seção finita A-invariante de G, A centraliza a seção finita $K/\{1\}$, ou seja, $k^\alpha\{1\} = k\{1\}$, para todo $\alpha \in A$, e, assim, $k^\alpha = k$, para todo $\alpha \in A$. Portanto, $K \leqslant C$. □

Observe que se $C_G(A) = \{1\}$, não se pode garantir que $C_G(\alpha) = \{1\}$ para todo $\alpha \in A$. Porém, a proposição a seguir mostra que quando o par (G, A) satisfaz $(*)$ existe pelo menos um $\alpha \in A$ tal que $C_G(\alpha) = \{1\}$.

Proposição 3.4. *Se o par (G, A) satisfaz a condição $(*)$ e $C_G(A) = \{1\}$, então existe um automorfismo livre de pontos fixos $\alpha \in A$.*

Demonstração. Pela proposição anterior $|g_i^A| = \infty$ para cada $i = 2, ..., n$. Se $A_i = C_A(g_i)$, segue que $|A : A_i| = \infty$, para cada $i = 2, ..., n$, pois, caso contrário, tem-se $|g_i^A| < \infty$. Pelo Teorema 1.4, $\bigcup_{i=2}^n A_i \subsetneq A$. Seja $\alpha \in A \backslash \bigcup_{i=2}^n A_i$ e suponha que $g^\alpha = g$, para algum $g \in G \backslash \{1\}$. Existe $i = 2, ..., n$ tal que $g = g_i^\beta$, para algum $\beta \in A$; desta forma, por um lado, tem-se $g_i^{\beta\alpha} = g_i^{\alpha\beta}$ e, por outro, $g_i^{\beta\alpha} = g_i^\beta$, assim $g_i^\alpha = g_i$; absurdo, pois $\alpha \notin A_i$. Portanto, α é FPF. □

Agora, com as mesmas hipóteses da proposição anterior, é possível mostrar que não existe seção finita A-invariante não trivial em G, como mostra a

Proposição 3.5. *Se o par (G, A) satisfaz a condição $(*)$ e $C_G(A) = \{1\}$, então não existe seção finita A-invariante não trivial em G.*

Demonstração. Suponha que H/K seja uma seção finita A-invariante não trivial de G. Assim A centraliza H/K. Mas, pela Proposição 3.4, existe $\alpha \in A$ livre de pontos fixos sobre H e, assim, pelo Teorema 2.11, α é uniforme sobre H. Logo, α é uniforme sobre H/K e, consequentemente, α é livre de pontos fixos sobre H/K. Mas isto contradiz o fato que $C_A(H/K) = A$. Portanto não existe seção finita A-invariante não trivial em G. $\square$

Recordando, a A-órbita g^A é dita *regular* se $g^\alpha \neq g$ para todo $\alpha \in A$.

Proposição 3.6. *Se o par (G, A) satisfaz a condição $(*)$ e $[G, A] = G$, então*

(i) G não contém subgrupo A-invariante próprio com índice finito;

(ii) G contém pelo menos uma A-órbita regular.

Demonstração. Seja H um subgrupo A-invariante de G com índice finito. Pela Proposição 2.17, $min_G^A(G)$ é um subgrupo normal de $max_G^A(G) = G$ com índice finito. Logo, como o par (G, A) satisfaz a condição $(*)$, o grupo A centraliza a seção $G/min_G^A(G)$. Mas, pela Proposição 2.6, $[G, A]$ é o "menor" subgrupo de índice finito A-invariante de G, tal que A centraliza a seção $G/[G, A]$. Logo, $G \geqslant H \geqslant min_G^A(G) \geqslant [G, A] = G$, provando o item (i). Agora, se $\alpha \in A \backslash \{Id_G\}$, pelo item (i), $C_G(\alpha)$ possui índice infinito em G, pois $C_G(\alpha)$ é A-invariante e próprio. Como $\mathcal{L}_A(G)$ é finito, existe apenas um número finito de conjuntos $C_G(\alpha)$'s, com α percorrendo $A \backslash \{Id_G\}$. Logo, pelo Teorema 1.4, existe $g \in G \backslash \bigcup_{\alpha \in A \backslash \{Id_G\}} C_G(\alpha)$. Assim $C_A(g) = \{1\}$, ou seja, g^A é regular. $\square$

Considere $\mathcal{G}$ um grupo e $\mathcal{A}$ um grupo de autormorfismos de $\mathcal{G}$. Com a notação $E(\mathcal{A})$ é designado o conjunto $E(\mathcal{A}) = \{\epsilon = \Sigma_{i=1}^s \xi_i \alpha_i;\ s \in \mathbb{N}, \xi_i = \pm 1, \alpha_i \in \mathcal{A}\}$. Se $\mathcal{G}$ é abeliano, então $E(\mathcal{A})$ é um subanel do anel $End(\mathcal{G})$ e se, além disso, $\mathcal{A}$ é abeliano, esse subanel é abeliano. É claro que T_α pertence a $E(\mathcal{A})$, para todo $\alpha \in \mathcal{A}$.

Proposição 3.7. *Sejam $\mathcal{G}$ um grupo, $\mathcal{A}$ um grupo abeliano de automorfismos de $\mathcal{G}$, $\alpha, \beta \in \mathcal{A}$ e $\epsilon \in E(\mathcal{G})$. Dado $g \in \mathcal{G}$, então*

(i) $g^{-1}g^\alpha \in C_\mathcal{G}(\beta)$ se, e somente se, $g^\beta g^{-1} \in C_\mathcal{G}(\alpha)$;

(ii) Se $\mathcal{G}$ é abeliano e $g^{-\beta}g^\epsilon \in C_\mathcal{G}(\alpha)$, então $[g, \alpha]^\beta = [g, \alpha]^\epsilon$.

Demonstração. Para provar o item (i) suponha que $g^{-1}g^\alpha \in C_\mathcal{G}(\beta)$, isso é, $(g^{-1}g^\alpha)^\beta = g^{-1}g^\alpha$, que equivale a igualdade $g^\beta g^{-1} = (g^{\alpha\beta}g^{-\alpha})$ e, como $\mathcal{A}$ é abeliano, por sua vez, essa última igualdade equivale a $g^{\beta}g^{-1} \in C_{\mathcal{G}}(\alpha)$.

Agora suponha que $g^{-\beta}g^{\epsilon} \in C_{\mathcal{G}}(\alpha)$. Então, $(g^{-\beta}g^{\epsilon})^{\alpha} = g^{-\beta}g^{\epsilon}$, logo $g^{\beta}g^{-\beta\alpha} = g^{\epsilon}g^{-\epsilon\alpha}$. Como $\mathcal{G}$ e $\mathcal{A}$ são abelianos, segue que $g^{-\beta}g^{\alpha\beta} = g^{-\epsilon}g^{\alpha\epsilon}$, ou seja, $[g,\alpha]^{\beta} = [g,\alpha]^{\epsilon}$. E (ii) está demonstrado. $\square$

Voltando às hipóteses do início deste capítulo, obtém-se agora uma condição suficiente para que $C_G(A) = \{1\}$.

Teorema 3.8. *Se o par (G, A) satisfaz a condição $(*)$, G é abeliano e $[G, A] = G$, então $C_G(A) = \{1\}$.*

Demonstração. Pela Proposição 3.6, o grupo G não possui subgrupo A-invariante próprio de índice finito. A demonstração será feita por indução sobre o comprimento de G com respeito a A, ou seja, sobre o número $\ell_A(G)$. Se $\ell_A(G) = 1$, então todo subgrupo A-invariante próprio de G é finito. De fato, se H é um subgrupo próprio de G A-invariante, segue que $max_G^A(H) < G$ (pois se $max_G^A(H) = G$, então, pela Proposição 2.17, $|G : H| < \infty$, absurdo). Assim, se K é um subgrupo de H A-invariante, deve-se ter $max_H^A(K) = H$, pois, caso $max_H^A(K) < H$, a cadeia $\{max_G^A(K), max_G^A(H), G\}$ seria uma cadeia de comprimento 3 em $\overline{\mathcal{L}}_A(G)$, absurdo. Portanto, $\ell_A(H) = 0$ e, então, H é finito. Daí, pela Proposição 3.3, $C_G(A)$ contém todo subgrupo próprio A-invariante de G. Por hipótese, $G = [G, A]$, logo existem $x \in G$ e $\beta \in A$ tais que $g = x^{-1}x^{\beta} \in G \backslash C_G(A)$. Assim, $\langle g^A \rangle = G$, pois caso contrário, $\langle g^A \rangle$ seria um subgrupo próprio A-invariante de G e, então, $\langle g^A \rangle \leqslant C_G(A)$, absurdo. Suponha agora, novamente por absurdo, que $C_G(A) \neq \{1\}$. Assim, existem inteiro positivo s e $\gamma_1, ..., \gamma_s \in A$ tais que $1 \neq g^{\gamma_1}...g^{\gamma_s} \in C_G(A)$. Defina $\epsilon = \sum_{i=1}^{s} \gamma_i \in E(A)$ e assim $g^{\epsilon} \in C_G(A)$, isto é, $g^{\epsilon} = (x^{-1}x^{\beta})^{\epsilon} \in C_G(\alpha)$ para todo $\alpha \in A$. Pela Proposição 3.7, $(x^{-1}x^{\alpha})^{\beta} = (x^{-1}x^{\alpha})^{\epsilon}$, para cada $\alpha \in A$. Em particular, se $\alpha = \beta$ tem-se $g^{\beta} = g^{\epsilon} \in C_G(A)$, logo $g \in C_G(A)$, absurdo. Portanto, $C_G(A) = \{1\}$.

Se $\ell_A(G) > 1$, escolha um subgrupo A-invariante K de G tal que $\ell_A(K) = \ell_A(G) - 1$. Fazendo $H = [K, A]$, pela Proposição 2.6 e condição $(*)$, tem-se $[K, A] = [[K, A], A]$, ou seja, $[H, A] = H$ e pela Proposição 2.6, $|K : H| < \infty$. Assim, pela Proposição 2.25, $\ell_A(H) = \ell_A(K)$. Logo, por hipótese de indução, $C_H(A) = \{1\}$. Como $\ell_A(H) = \ell_A(G) - 1$, segue que $\ell_A(G/H) = 1$ e $[G/H, A] = G/H$, donde $C_{G/H}(A) = \{1\}$. Portanto, $C_G(A) = \{1\}$. $\square$

Pela mesma argumentação feita na demonstração do teorema anterior, obtém-se que se o par (G, A) satisfaz a condição $(*)$, então $[G, A] = [[G, A], A]$ e, assim, se G é abeliano, pelo Teorema 3.8, $[G, A] \cap C_G(A) = \{1\}$. Logo, $\langle [G, A], C_G(A) \rangle$ é um produto direto entre o subgrupo $[G, A]$ e o subgrupo finito $C_G(A)$. Em verdade, G é esse produto.

Teorema 3.9. *Suponha que o par (G, A) satisfaz a condição $(*)$ e que G é abeliano. Então $G = [G, A] \times C_G(A)$.*

Demonstração. Se $G = [G, A]$ nada há para fazer. Caso contrário, seja $g \in G \setminus [G, A]$. Pelo Teorema 3.8, $C_{[G,A]}(A) = \{1\}$ e, assim, pela Proposição 3.4, existe α em A livre de pontos fixos sobre $[G, A]$. Como A é abeliano, tem-se que α é uniforme, em virtude do Teorema 2.11. Uma vez que $g^{-1}g^{\alpha} \in [G, A]$, existe $x \in [G, A]$ tal que $x^{-1}x^{\alpha} = g^{-1}g^{\alpha}$, pois α é uniforme em $[G, A]$, daí, $gx^{-1} \in C_G(\alpha)$. Então, $g = gx^{-1}x = xgx^{-1} \in [G, A]C_G(\alpha)$. Porém, $|G : [G, A]| < \infty$ e $[G, A] \cap C_G(\alpha) = \{1\}$ e, daí, $C_G(\alpha)$ é finito. Pela condição $(*)$ e por $C_G(A) \leqslant C_G(\alpha)$ segue que $C_G(\alpha) = C_G(A)$. Portanto, $G = [G, A]C_G(A)$ e $[G, A] \cap C_G(A) = \{1\}$, logo $G = [G, A] \times C_G(A)$, por ser G abeliano. □

Observe que a hipótese do grupo G ser uma união de um número finito de A-órbitas é fundamental, como mostra o seguinte exemplo: Se $Q = \mathbb{Q}^{\times}$ e $B = \langle \imath \rangle$, onde $\imath$ é o automorfismo que induz a inversão em H, então $Q \neq [Q, B] \times C_Q(B)$, pois $[Q, B] = \langle q^2; q \in \mathbb{Q}^{\times} \rangle$ e $C_Q(B) = \{1, -1\}$. Veja que o grupo Q não é uma união de um número finito de B-órbitas.

Os dois próximos resultados são, em certo sentido, técnicos e serão usados na demonstração do Teorema A.

Proposição 3.10. *Suponha que o par (G, A) satisfaz a condição $(*)$ e que G é abeliano e possui um único subgrupo próprio A-invariante não trivial N. Então, se $B = C_A(N)$, tem-se que $B = C_A(G/N)$. Em particular, $[G, B] = N$.*

Demonstração. Primeiramente, veja que $B \neq \{Id_G\}$, pois caso contrário, para cada $\alpha \in A \backslash \{Id_G\}$ o subgrupo $C_G(\alpha)$ seria igual a $\{1\}$ (Isso vem de $C_G(\alpha)$ pertencer a $\mathcal{L}_A(G)$ e ser diferente de N e de G). Daí, A seria FPF e, como é abeliano, seria FC-grupo. Assim, tem-se um absurdo, em virtude do Corolário 2.12. Portanto, $B \neq \{Id_G\}$.

Seja agora $\beta \in B\backslash\{Id_G\}$. Tem-se que $Nuc(T_\beta) = N$, pois $N \leqslant Nuc(T_\beta) < G$ e, então, o subgrupo não trivial e A-invariante $Im(T_\beta)$ é diferente de G. Logo $Im(T_\beta) = N$, ou seja, $[G, \beta] = N$ e, como β é qualquer em $B\backslash\{Id_G\}$, tem-se $[G, B] = N$. Então, $B \leqslant C_A(G/N)$. Por outro lado, considere $\alpha \in C_A(G/N)\backslash\{Id_G\}$. Assim $[G, \alpha] \leqslant N$ e, daí, $Im(T_\alpha) \leqslant N$, ou seja, α não é uniforme e, consequentemente, α não é FPF. Desta forma, $N \leqslant C_G(\alpha)$ e, então, $\alpha \in B$ e $C_A(G/N) \leqslant B$. Portanto $B = C_A(G/N)$. □

Proposição 3.11. *Suponha que o par (G, A) satisfaz a condição $(*)$, G é abeliano e que existam subgrupos A-invariantes G_1 e G_2 de G tais que $G = G_1 \times G_2$ e $\ell_A(G_1), \ell_A(G_2) > 0$. Então, se $A_1 = C_A(G_2)$ e $A_2 = C_A(G_1)$, tem-se $A_1 \cap A_2 = \{Id_G\}$ e $|A : A_1 \times A_2| < \infty$.*

Demonstração. Se $\alpha \in A_1 \cap A_2$, então $\alpha|_{G_1} = Id_{G_1}$ e $\alpha|_{G_2} = Id_{G_2}$, assim $\alpha = Id_G$. Logo, $A_1 \cap A_2 = \{Id_G\}$ e, sendo A abeliano, tem-se $\langle A_1, A_2\rangle = A_1 \times A_2$.

Por hipótese, $\ell_A(G_1) > 0$, assim G_1 é infinito. Pela Proposição 3.3, o par $(G_1, A/A_2)$ satisfaz $(*)$ e, daí, pelo Teorema 3.9, tem-se $G_1 = [G_1, A/A_2] \times C_{G_1}(A/A_2)$. Logo, o subgrupo $[G_1, A/A_2]$ é infinito e, como é A/A_2-invariante, o par $([G_1, A/A_2], A/A_2)$ satisfaz a condição $(*)$. Além disso, $[[G_1, A/A_2], A/A_2] = [G_1, A/A_2]$. Assim, pela Proposição 3.6, existe uma A/A_2-órbita g^{A/A_2} regular em $[G_1, A/A_2]$. Analogamente, prova-se que existe uma A/A_2-órbita h^{A/A_1} regular sobre $[G_2, A/A_2]$.

Sejam I e J conjuntos de índices tais que $g^{A/A_2} = \biguplus_{i\in I}(g^{\alpha_i})^{\bar{A}_1}$ e $h^{A/A_1} = \biguplus_{j\in J}(h^{\beta_j})^{\bar{A}_2}$, em que $\bar{A}_1 = \{A_2\alpha;\, \alpha \in A_1\}$ e $\bar{A}_2 = \{A_1\alpha;\, \alpha \in A_2\}$. Considere agora os conjuntos $[[g]] = \{(g^{\alpha_i})^{\bar{A}_1}; i \in I\}$ e $[[h]] = \{(h^{\beta_j})^{\bar{A}_2}; j \in J\}$ e as ações

$$\rho : [[g]] \times A/(A_1 \times A_2) \to [[g]]$$

$$(g^{\alpha_i \bar{A}_1}, \bar{\alpha}) \mapsto g^{\alpha_{k_i} \bar{A}_1}$$

e

$$\varphi : [[h]] \times A/(A_1 \times A_2) \to [[h]]$$

$$(h^{\beta_i \bar{A}_2}, \bar{\beta}) \mapsto h^{\beta_{l_j} \bar{A}_2}$$

em que $k_i \in I$ e $l_j \in J$ são tais que $g^{\alpha_i \alpha \bar{A}_1} = g^{\alpha_{k_i} \bar{A}_1}$ e $g^{\beta_j \beta \bar{A}_2} = g^{\beta_{l_j} \bar{A}_2}$. Não é difícil verificar que essas ações estão bem definidas.

A ação ρ é regular, no sentido que para cada par $i_1, i_2 \in I$ existe único $\bar{\alpha}$ tal que $(g^{\alpha_{i_1}})^{A_1\bar{\alpha}} = (g^{\alpha_{i_2}})^{A_1}$. De fato, se $i_1, i_2 \in I$, tomando $\bar{\alpha} = \bar{\alpha}_{i_1}\bar{\alpha}_{i_2}^{-1}$ tem-se $((g^{\alpha_{i_1}})^{\bar{A}_1})^{\bar{\alpha}} = (g^{\alpha_{i_2}})^{\bar{A}_1}$. Além disso, se existem $\bar{\alpha}, \bar{\beta} \in A/(A_1 \times A_2)$ tais que $((g^{\alpha_{i_1}})^{\bar{A}_1})^{\bar{\alpha}} = ((g^{\alpha_{i_1}})^{\bar{A}_1})^{\bar{\beta}}$, então, como A é abeliano, existe $a \in A_1$ tal que $g^{a\alpha\beta^{-1}} = g$ e, como g^{A/A_2} é regular, tem-se $a\alpha\beta^{-1} \in A_2$, logo $\bar{\alpha} = \bar{\beta}$. Analogamente, no mesmo sentido, a ação φ é regular. Fixado um $x \in [[g]]$ e dado $y \in [[g]]$, então x é levado pela ação ρ em y por um único $\bar{\alpha} \in A/(A_1 \times A_2)$, com isso, $|A/(A_1 \times A_2)| = |I| = |J|$.

Fixe agora $i_1 \in I$ e $j_1 \in J$ e sejam $i_2 \in I$ e $j_2 \in J$ tais que $(g^{\alpha_{i_1}}h^{\beta_{j1}})^{\alpha} = g^{\alpha_{i_2}}h^{\beta_{j_2}}$, para algum $\alpha \in A$, desta forma, $g^{\alpha_{i_1}\alpha}g^{-\alpha_{i_2}} = h^{\beta_{j_2}}h^{(-\beta_{j_1}\alpha)} \in G_1 \cap G_2 = \{1\}$ e, assim, $\alpha_{i_1}\alpha\alpha_{i_2}^{-1}$ fixa g, logo esse automorfismo pertence a A_2, pois g^{A/A_2} é A/A_2-regular. Analogamente $\beta_{j_1}\alpha\beta_{j_2}^{-1}$ pertence a A_1. Daí, $\beta_{j_1}\alpha\beta_{j_2}^{-1}(\alpha_{i_1}\alpha\alpha_{i_2}^{-1})^{-1} = \beta_{j_1}\beta_{j_2}^{-1}\alpha_{i_1}\alpha_{i_2}^{-1} \in A_1 \times A_2$, ou seja, $\alpha_{i_2}^{-1}\beta_{j_2} \in \alpha_{i_1}^{-1}\beta_{j_1}A_1 \times A_2$. Logo, se $g^{\alpha_{i_1}}h^{\beta_{j1}}$ e $g^{\alpha_{i_2}}h^{\beta_{j2}}$ pertencem a mesma A-órbita, então $\alpha_{i_2}^{-1}\beta_{j_2} \in \alpha_{i_1}^{-1}\beta_{j_1}(A_1 \times A_2)$, mas há $|I|$ classes da forma $\gamma(A_1 \times A_2)$, com $\gamma \in A$. Disto e do fato que o número de A-órbitas é n, segue que $|I| \leqslant n$. Portanto, $|A/(A_1 \times A_2)| = n < \infty$. $\square$

Observação 3.12. Salvo menção contrária, serão usadas as seguintes convenções:

- Quando o par (G, A) satisfizer a condição $(*)$, o símbolo C será usado para denotar o conjunto $C_G(A)$, o qual será finito, pela Proposição 3.3. Logo existirão um inteiro positivo k e $y_1, ..., y_k \in G$ tais que C é dado por $C = \{y_1, ..., y_k\}$, com $y_1 = 1$;

- Os símbolos $N_1, ..., N_s$ denotarão todos os subgrupos A-invariantes minimais de G com respeito a $\ell_A(N_i) = 1$, para todo $i \in I = \{1, ..., s\}$;

- Para cada $i \in I$, o símbolo A_i denotará o conjunto $\{\alpha \in A;$ existe $y \in C$ tal que $x^{\alpha} = x^{y}$ para todo $x \in N_i\}$ e o símbolo $\mathfrak{U}(A)$ o conjunto $A \setminus \cup_{i\in I}A_i$.

É fácil ver que $\mathfrak{U}(A)$ não é um subgrupo de A, pois, $Id_G \notin \mathfrak{U}(A)$. Pode-se estender o conceito de órbita para um subconjunto qualquer de $Aut(G)$ da seguinte forma: se $X \subseteq Aut(G)$ e $g \in G$, define-se a X-órbita de $g \in G$ por $g^X = \{g^{\gamma}; \gamma \in X\}$. Assim, para cada $g \in G$, a $\mathfrak{U}(A)$-órbita de g é o conjunto $g^{\mathfrak{U}(A)} = \{g^{\alpha}; \alpha \in \mathfrak{U}(A)\}$.

Proposição 3.13. *Suponha que o par (G, A) satisfaz a condição $(*)$. Então, existem $\alpha_1, ..., \alpha_t \in$*

A tais que $A = \bigcup_{i=1}^{t} \mathfrak{U}(A)\alpha_i$. Em particular, G é uma união de um número finito de $\mathfrak{U}(A)$-órbitas. Além disso, para todo $\alpha \in \mathfrak{U}(A)$ tem-se que $C_G(\alpha) = C$.

Demonstração. Dado $i \in I$ se $B_i = C_A(N_i)$, então $B_i \leqslant A_i$, pois, para todo $\alpha \in B_i$ e todo $x \in N_i$, tem-se $x^\alpha = x = x^{y_1}$. Agora, suponha que $|A : B_i| < \infty$, assim, (G, B_i) satisfaz a condição $(*)$, daí $|C_G(B_i)| < \infty$, contradizendo o fato de $|N_i| = \infty$ e $N_i \leqslant C_G(B_i)$. Logo, $|A : B_i| = \infty$. Para $\alpha, \beta \in A_i$ e $i \in I$, defina $\alpha \backsim \beta$ se, e somente se, existe $y \in C$ tal que $x^\alpha = x^y = x^\beta$, para todo $x \in N_i$. É fácil ver que essa relação é de equivalência sobre A_i e possui no máximo $|C|$ classes. Se $[\alpha]$ denota a classe de α, é fácil ver que $R = \{[\alpha]; \alpha \in A_i\}$ é um grupo munido da operação $[\alpha][\beta] = [\alpha\beta]$, a qual está bem definida, pois $C = C_G(A)$, com $[Id_G]$ o elemento neutro e $[\alpha^{-1}]$ o inverso de $[\alpha]$ nessa operação. Logo, dado $\beta \in [\alpha]$ tem-se $\beta\alpha^{-1} = \gamma \in B_i$, ou seja, $\beta = \gamma\alpha$. Daí, $|A_i : B_i| < \infty$. Como $|A : B_i| = \infty$, segue que $|A : A_i| = \infty$ e, assim, pelo Teorme 1.4, tem-se $\bigcup_{i \in I} A_i \subsetneq A$, ou seja, $\mathfrak{U}(A) = A \backslash \bigcup_{i \in I} A_i \neq \emptyset$. Pela Proposição 1.5, existem $\alpha_1, ..., \alpha_t \in A$ tais que $A = \bigcup_{i \in I} \mathfrak{U}(A)\alpha_i$. Com isso, $G = \bigcup_{j=1}^{n} g_j^A = \bigcup_{j=1}^{n} \bigcup_{i=1}^{t} (g_j^{\alpha_i})^{\mathfrak{U}(A)}$, provando, assim, a primeira asserção. Agora, considere $\alpha \in \mathfrak{U}(A)$ e $H = C_G(\alpha)$. Suponha, por absurdo, que $H \neq C$. Então $\ell_A(H) \geqslant 1$. Logo, existe $i \in I$ tal que $N_i \leqslant H$, daí $\alpha \in B_i \leqslant A_i \subseteq A \setminus \mathfrak{U}(A)$, absurdo. Portanto, o resultado segue. $\square$

Observe que, apesar de $\mathfrak{U}(A)$ não ser grupo, se $\alpha \in \mathfrak{U}(A)$, então $\alpha^{-1} \in \mathfrak{U}(A)$. Também, pode acontecer de $g \in G$ não pertencer à sua $\mathfrak{U}(A)$-órbita; para isso basta que a A-órbita de g seja regular.

Proposição 3.14. *Sejam $g \in G$ e $\alpha \in \mathfrak{U}(A)$. Então:*

(i) Se $g^\alpha = g^y$ para algum $y \in C$, então $g \in C$. Em particular $[g, y] = 1$;

(ii) Se $g^{-1}g^\alpha \in C$, então $g \in C$;

(iii) Se existem $y, z \in C$ tais que $g^\alpha = y^{-1}gz$, então $g \in C$.

Demonstração. Para provar o item (i) suponha, por absurdo, que $g \notin C$. Considere o conjunto $X = \{x \in G;\ x^\alpha = x^y\}$. É claro que X é um subgrupo A-invariante de G contendo

g. Assim, $\ell_A(X) \geqslant 1$ e existe $i \in I$ com $N_i \leqslant X$, ou seja, $\alpha \in A_i$, absurdo. Isto prova o item (i).

Já para demonstrar o item (ii), seja, por hipótese, $y \in C$ tal que $g^{-1}g^{\alpha} = y$, ou seja, $g^{\alpha} = gy$. Para $\beta \in A$, tem-se que

$$(g^{-1}g^{\beta})^{\alpha} = g^{-\alpha}g^{\beta\alpha} = g^{-\alpha}g^{\alpha\beta} = y^{-1}(g^{-1}g^{\beta})y.$$

Pelo item anterior, $g^{-1}g^{\beta} \in C$ para todo $\beta \in A$ e, com isso, a A-órbita g^A é finita. Sejam $\alpha, \beta \in A$ e defina $\alpha \backsim \beta$ se, e somente se, $g^{\alpha} = g^{\beta}$. A relação $\backsim$ sobre A é evidentemente de equivalência, com no máximo $|g^A|$ classes de equivalência. Logo, se $\beta \in [\alpha]$, onde $[\alpha]$ é a classe à qual α pertence, então $\alpha^{-1}\beta \in C_A(g)$, ou seja, existe $\eta \in C_A(g)$ tal que $\beta = \alpha\eta$, daí $|A : C_A(g)| < \infty$. Colocando $B = C_A(g)$, tem-se $g \in C_G(B)$. Mas, $|A : B| < \infty$ e, então, pela Proposição 3.3, o par (G, B) satisfaz a condição $(*)$. Assim, o subgrupo $C_G(B)$ de G é A-invariante finito, em virtude da Proposição 3.3. Portanto, $C_G(B) = C$ e, assim, $g \in C$, isto demonstra o item (ii).

No item (iii) tem-se $(g^{-1}g^{\alpha})^{\alpha} = (g^{\alpha})^{-1}(g^{\alpha})^{\alpha} = z^{-1}g^{-1}g^{\alpha}z$. Assim, pelo item (i) segue que $g^{-1}g^{\alpha} \in C$ e, daí, pelo item (ii), tem-se $g \in C$. O resultado está demonstrado. $\square$

Existe uma relação entre FC-grupos e BFC-grupos quando o par (G, A) satisfaz a condição $(*)$, conforme estabelece o seguinte resultado.

Teorema 3.15. *Suponha que o par (G, A) satisfaz a condição $(*)$. Se G é um FC-grupo, então é BFC-grupo. Além disso, $[G, A]$ é um grupo nilpotente de classe no máximo 2 e, se $C_0 = [G, A] \cap C$, então $C_0 \leqslant Z([G, A])$ e $C_0 \lhd G$.*

Demonstração. Sejam $g \in G$ e $m = max\{|G : C_G(g_i)|; i = 1, ..., n\}$, que é finito, pois G é FC-grupo. Existe $i \in \{1, ..., n\}$ tal que $g \in g_i^A$, ou seja, existe $\alpha \in A$ tal que $g = g_i^{\alpha}$. Logo, $C_G(g) = (C_G(g_i^{\alpha})) = (C_G(g_i))^{\alpha}$ e, assim, $|G : C_G(g)| \leqslant |G : C_G(g_i)| \leqslant m$. Portanto, G é BFC-grupo. Pela Proposição 3.6 e condição $(*)$, $[G, A]$ não possui subgrupo próprio com índice finito. Se $c \in C_0$, então $C_{[G,A]}(c)$ é um subgrupo A-invariante com índice finito em $[G, A]$, pois $[G, A]$ é FC-grupo, daí $C_{[G,A]}(c) = [G, A]$, ou seja, $C_0 \leqslant Z([G, A])$. Pelo Teorema 1.40, o subgrupo G' é finito, assim $[G, A]'$ também o é e, como $[G, A]'$ é A-invariante e o par $([G, A], A)$ satisfaz $(*)$, segue que $[G, A]' \leqslant C_{[G,A]}(A) = C_0 \leqslant Z([G, A])$. Assim,

$\{1\} \lhd [G,A]' \lhd [G,A]$ é uma série central de $[G,A]$, ou seja, $[G,A]$ é nilpotente de classe no máximo 2. Para finalizar, sejam $g \in G$ e $c \in C_0$ e suponha, por contradição, que $c^g \notin C_0$. Com isso, existe $\alpha \in A$ com $(c^g)^\alpha \neq c^g$, daí, $c \neq c^{gg^{-\alpha}}$, mas $c \in Z([G,A])$ e $gg^{-\alpha} \in [G,A]$, absurdo. Logo, $C_0 \leqslant G$ e o resultado segue, como esperado. □

Agora, já há resultados suficientes para mostrar que quando o par (G,A) satisfaz a condição $(*)$, seu subgrupo $[G,A]$ é BFC-grupo, é o que assegura o

Teorema 3.16. *Se o par (G,A) satisfaz a condição $(*)$, então o subgrupo $[G,A]$ de G é um BFC-grupo.*

Demonstração. Não há perda de generalidade em supor que $G = [G,A]$, pois, $[G,A] = [[G,A],A]$ e, uma vez que $|G : [G,A]| < \infty$, o par $([G,A],A)$ também satisfaz $(*)$. A demonstração será feita por indução sobre o número $m + |\mathcal{L}_A(G)|$, em que m é o menor número inteiro tal que $G = \bigcup_{i=1}^m h_i^{\mathcal{U}(A)}$. Nada há para fazer se $|\mathcal{L}_A(G)| = 1$, pois nesse caso G seria finito e, então, um BFC-grupo. Se $|\mathcal{L}_A(G)| = 2$, então $\mathcal{L}_A(G) = \{\{1\}, G\}$. Assim, para cada $\alpha \in A \setminus \{Id_G\}$, tem-se que $C_G(\alpha) = \{1\}$; desta forma, A é FPF. Uma vez que A é abeliano, é também FC-grupo. Logo, pelo Teorema 2.13, G é abeliano; daí, é também um BFC-grupo e fica provada a base da indução.

Agora suponha que $m + |\mathcal{L}_A(G)| \geqslant m + 2$. A indução ficará completa demonstrando seis passos, cada um dado como uma afirmação que é em seguida demonstrada.

Afirmação 1: Se $k = |C|$, então existem um inteiro positivo r e $h_1, ..., h_r \in G$, com $h_1 = 1$, tais que $m = kr$, $G = \bigcup_{i=1}^k \bigcup_{j=1}^r (y_i h_j)^{\mathcal{U}(A)}$ e se $(i_1, j_1) \neq (i_2, j_2)$, então $(y_{i_1} h_{j_1})^{\mathcal{U}(A)} \neq (y_{i_2} h_{j_2})^{\mathcal{U}(A)}$.

De fato,é claro que $\{y_1\}, ..., \{y_k\}$ são $\mathcal{U}(A)$-órbitas distintas. Tome $h_2 \in G \setminus C$, assim $h_2^{\mathcal{U}(A)}$, $(y_2 h_2)^{\mathcal{U}(A)}$, ..., $(y_k h_k)^{\mathcal{U}(A)}$ são também distintas, pois, se existir $\alpha \in \mathcal{U}(A)$ tal que $(y_{i_1} h_2)^\alpha = y_{i_2} h_2$, então $h_2 h^{-\alpha} = y_{i_2}^{-1} y_{i_1}^\alpha = y_{i_2}^{-1} y_{i_1}$ e, como $y_{i_2}^{-1} y_{i_1} \in C$, pelo item (ii) da Proposição 3.14, $h_2 \in C$, absurdo. Daí, $h_2^{\mathcal{U}(A)}$, $(y_2 h_2)^{\mathcal{U}(A)}$, ..., $(y_k h_2)^{\mathcal{U}(A)}$ são $\mathcal{U}(A)$-órbitas distintas. Além disso,

$$y_s h_2 \notin C \cup \bigcup_{i=1}^{s-1} (y_i h_2)^{\mathcal{U}(A)},$$

para $s = 2, ..., k$. Se $G = \bigcup_{i=1}^{k}\bigcup_{j=1}^{2}(y_ih_j)^{\mathcal{U}(A)}$, a segunda asserção está provada, caso contrário, tome $h_3 \in G \setminus \bigcup_{i=1}^{k}\bigcup_{j=1}^{2}(y_ih_j)^{\mathcal{U}(A)}$. Novamente, pela Proposição 3.14, as $\mathcal{U}(A)$-órbitas $h_3^{\mathcal{U}(A)}, (y_2h_3)^{\mathcal{U}(A)}, ..., (y_kh_3)^{\mathcal{U}(A)}$ são distintas, duas a duas. Também

$$y_sh_3 \notin C \cup \bigcup_{i=1}^{k}(y_ih_2)^{\mathcal{U}(A)} \cup \bigcup_{i=1}^{s-1}(y_ih_3)^{\mathcal{U}(A)},$$

para $s = 2, ..., k$. Se $G = \bigcup_{i=1}^{k}\bigcup_{j=1}^{3}(y_ih_j)^{\mathcal{U}(A)}$, a afirmação está provada, caso contrário, repita o processo acima. Como G é uma união de um número finito de $\mathcal{U}(A)$-órbitas, esse processo termina após uma quantidade finita r de passos. Portanto, $G = \bigcup_{i=1}^{k}\bigcup_{j=1}^{r}(y_ig_j)^{\mathcal{U}(A)}$. Claramente $m = kr$, pois essas $\mathcal{U}(A)$-órbitas são distintas, em verdade, disjuntas.

Afirmação 2: Dado $\alpha \in \mathcal{U}(A)$, então $G = \bigcup_{i=1}^{k}\bigcup_{j=1}^{r}(g_j^{-1}y_ig_j^{\alpha})^{\mathcal{U}(A)}$.

Como $m = kr$ é suficiente mostrar que se $(i_1, j_1) \neq (i_2, j_2)$, então $h_{j_1}^{-1}y_{i_1}h_{j_1}^{\alpha}$ e $h_{j_2}^{-1}y_{i_2}h_{j_2}^{\alpha}$ pertencem a $\mathcal{U}(A)$-órbitas distintas. Suponha, por contradição, que isso não ocorra, ou seja, que existam $(i_1, j_1) \neq (i_2, j_2)$ e $\beta \in \mathcal{U}(A)$ tais que $h_{j_1}^{-1}y_{i_1}h_{j_1}^{\alpha} = (h_{j_2}^{-1}y_{i_2}h_{j_2}^{\alpha})^{\beta}$. Tome $h = h_{j_1}h_{j_2}^{-\beta}$, daí, $h^{\alpha}h_{j_1}^{\alpha}h_{j_2}^{-\alpha\beta} = y_{i_1}^{-1}hy_{i_2}$. Da Proposição 3.14, segue que $h \in C$. Como $h_{j_2}^{\beta} = h^{-1}h_{j_1}$, pela construção dos h_j's na *Afirmação 1*, tem-se $h_{j_1} = h_{j_2}$. Considere $j = j_1 = j_2$. A igualdade $h_j^{-1}y_{i_1}h_j^{\alpha} = (h_j^{-1}y_{i_2}h_j^{\alpha})^{\beta}$ é equivalente a $y_{i_2}^{-1}h_j^{\beta}h_j^{-1}y_{i_1} = (h_j^{\beta}h_j^{-1})^{\alpha}$. Como $\alpha \in \mathcal{U}(A)$, pela Proposição 3.14, tem-se $h_j^{\beta}h_j^{-1} = (h_j^{-\beta})^{-1}(h_j^{-\beta})^{\beta^{-1}} \in C$ e como $\beta^{-1} \in \mathcal{U}(A)$, também pela Proposição 3.14, $h_j^{-\beta} \in C$, logo $h_j \in C$. Desta forma, só se pode ter $h_j = 1$ e disto resulta que $y_{i_1} = y_{i_2}^{\beta} = y_{i_2}$, logo $i_1 = i_2$, absurdo. O resultado segue.

Afirmação 3: Se $h \in G$ e $h^G \cap C = \emptyset$, então $h \in \widehat{Z}(G)$.

É suficiente mostrar que conjugados distintos de h pertencem a $\mathcal{U}(A)$-órbitas distintas, pois como há uma quantidade finita de $\mathcal{U}(A)$-órbitas em G, obtem-se $|h^G| < \infty$ e, assim, $h \in \widehat{Z}(G)$. Para tanto, suponha, por absurdo, que existam $x \in G$ e $\alpha \in \mathcal{U}(A)$ tais que $h^{\alpha} = h^x$. Pela *Afirmação 2*, existem índices i e j e $\beta \in \mathcal{U}(A)$ tais que $x = (h_j^{-1}y_ih_j^{\alpha})^{\beta}$. Assim, $h^{\alpha} = (h_j^{-1}y_ih_j^{\alpha})^{-\beta}h(h_j^{-1}y_ih_j^{\alpha})^{\beta}$ e isso resulta em $(h_j^{\beta}hh_j^{-\beta})^{\alpha} = (h_j^{\beta}hh_j^{-\beta})^{y_i}$. Mas $\alpha \in \mathcal{U}(A)$, logo pela Proposição 3.14, $h^{h_j^{-\beta}} \in C$, o que contradiz a hipótese.

Afirmação 4: Existe $h \in G$ tal que $h^G \cap C = \emptyset$. Em particular $\widehat{Z}(G) \neq \{1\}$.

Com efeito, suponha, por absurdo, que para qualquer elemento $h \in G$ tem-se $h^G \cap C \neq \emptyset$, ou seja, h é um conjugado de algum $y \in C$, donde $G = \bigcup_{i=1}^{k} y_t^G$. Pela *Afirmação 1*, tem-se que $G = \bigcup_{i=1}^{k} \bigcup_{j=1}^{r} (y_i g_j)^{\mathcal{U}(A)}$ e, daí,

$$G = \bigcup_{t=1}^{k} y_t^{\bigcup_{i=1}^{k} \bigcup_{j=1}^{r} (y_i g_j)^{\mathcal{U}(A)}} = \bigcup_{t=1}^{k} \bigcup_{i=1}^{k} \bigcup_{j=1}^{r} y_t^{(y_i g_j)^{\mathcal{U}(A)}} = \bigcup_{t=1}^{k} \bigcup_{i=1}^{k} \bigcup_{j=1}^{r} (y_t^{y_i})^{g_j \mathcal{U}(A)}.$$

Como $y_t^{y_i} \in C$ percorre todo C a medida que i e t percorrem $\{1, ..., k\}$, com $y_1 = 1$, tem-se que

$$G = \bigcup_{i=1}^{k} \bigcup_{j=1}^{r} y_t^{g_j \mathcal{U}(A)} = \{1\} \cup \bigcup_{i=2}^{k} \bigcup_{j=1}^{r} y_t^{g_j \mathcal{U}(A)}$$

e, assim, G é uma união de no máximo $1 + (k-1)r$ $\mathcal{U}(A)$-órbitas. Logo, $kr \leqslant 1 + (k-1)r$, ou seja, $r = 1$, daí $G = C$, absurdo. Portanto, existe $h \in G$ tal que $h^G \cap C = \emptyset$. É claro que $h \neq 1$ e, então, pela *Afirmação 3*, $\widehat{Z}(G) \neq \{1\}$, como desejado.

Afirmação 5: O subgrupo A-invariante $\widehat{Z}(G)C$ é normal em G.

Pelo Teorema 1.32, o subgrupo $\widehat{Z}(G)$ é característico em G, logo é normal e A-invariante. Considere então o grupo quociente $G/\widehat{Z}(G)$, que é uma união de um número $\bar{m} \leqslant m$ de $\mathcal{U}(A)$-órbitas. Como $\widehat{Z}(G) \neq \{1\}$, $|\mathcal{L}_A(G/\widehat{Z}(G))| < |\mathcal{L}_A(G)|$. Por hipóte de indução, $G/\widehat{Z}(G)$ é um BFC-grupo, pois $[G/\widehat{Z}(G), A] = G/\widehat{Z}(G)$. Pelo Teorema 3.15, $\widehat{Z}(G)C/\widehat{Z}(G)$ é normal em $G/\widehat{Z}(G)$. Portanto, $\widehat{Z}(G)C$ é normal em G.

Afirmação 6: G é FC-grupo.

Primeiro suponha que $G = \widehat{Z}(G)C$. Então, se $g \in G$, $g = zc$, com $z \in \widehat{Z}(G)$ e $c \in C$. Agora, se $\alpha \in A$, tem-se $g^{-1}g^{\alpha} = z^{-1}c^{-1}c^{\alpha}z^{\alpha} = z^{-1}z^{\alpha} \in \widehat{Z}(G)$. Daí, $[G, A] \leqslant \widehat{Z}(G)$ e, como $G = [G, A]$, deve-se ter $G = \widehat{Z}(G)$, ou seja, G é FC-grupo. Suponha, por absurdo, que $G \neq \widehat{Z}(G)C$. Uma vez que $C \leqslant \widehat{Z}(G)C$ e $\widehat{Z}(A)C \lhd G$, nenhum elemento de $G \setminus \widehat{Z}(G)C$ é conjugado de algum elemento de C. Logo, pela *Afirmação 3*, tem-se $\langle G \backslash \widehat{Z}(G)C \rangle \leqslant \widehat{Z}(G)$, isto é, $G = \widehat{Z}(G)C$, absurdo.

Portanto, pelo Teorema 3.15, o grupo G é um BFC-grupo. $\square$

3.2 Teorema B

Nesta seção, é assumido que G é um grupo abeliano, A um grupo abeliano de automorfismos de G que age por um número finito n de órbitas, $C = C_G(A)$ e $N_1, ..., N_s$ são todos os distintos subgrupos A-invariantes minimais não triviais de $[G, A]$. Além disso, o par (G, A) satisfaz a condição $(*)$. Esta seção é dedicada para enunciar e demonstrar o Teorema B, o qual descreve a estrutura de G sob as condições acima. Este teorema está dividido em dois lemas: no primeiro G é escrito como um produto direto de subgrupos A-invariantes de G e, no segundo, a natureza de G é ainda mais detalhada, como uma generalização do Teorema 2.13.

Definição 3.17. Um grupo G é dito A-*monolítico* se existe apenas um subgrupo A-invariante minimal não trivial em G.

Exemplo 3.18. Se $Q = \mathbb{Q}^{\times}$ e $B = \langle \imath \rangle$, com $\imath$ o automorfismo de Q que induz a inversão, então $\{1, -1\}$ é o único subgrupo B-invariante minimal não trivial de Q, ou seja, Q é B-monolítico. Observe que $\mathbb{Q}^{\times}_{>0}$ é um subgrupo próprio B-invariante de Q que não contém $\{1, -1\}$.

Lema 3.19. *Existem um inteiro positivo s e subgrupos A-invariantes $M_1, ..., M_s$ de $[G, A]$, tais que $G = C \times M_1 \times ... \times M_s$ e para cada $i \in \{1, ..., s\}$ o subgrupo M_i é maximal com respeito às propriedades:*

(i) $N_i \leqslant M_i$ *e*

(ii) M_i *é A-monolítico.*

Demonstração. Se $i \in \{1, ..., s\}$, então o conjunto $\mathcal{L}_i = \{M \leqslant [G, A]; N_i \leqslant M$ e M é A-monolítico $\}$ é não vazio, pois $N_i \in \mathcal{L}_i$. Seja agora $\{M_j\}_{j \in I}$ um subconjunto totalmente ordenado de $\mathcal{L}_i$. É fácil ver que $\bigcup_{j \in I} M_j \in \mathcal{L}_i$. Segue, pelo Lema de Zorn que M_i existe. Como G é abeliano, pela Proposição 3.9, tem-se $G = C \times [G, A]$. Claramente os M_i's, como nas hipóteses, são tais que $M_i \cap M_j = \{1\}$, se $i \neq j$. Falta, então, mostrar que $[G, A] = \langle M_1, ..., M_s \rangle$. Tal fato será mostrado por indução sobre o número s. No caso em que $s = 1$, tem-se $[G, A] = M_1$ e, daí, o resultado segue imediatamente. Suponha agora que $s > 1$. Logo, os únicos subgrupos A-invariantes minimais não triviais de $[G/M_s, A]$ são $N_1 M_s / M_s, ..., N_{s-1} M_s / M_s$. De fato, suponha que N/M_s é um subgrupo A-invariante minimal de $[G/M_s, A]$ diferente de cada $N_i Ms/Ms$, para $i = 1, ..., s$. Assim N contém N_s como seu único subgrupo A-invariante minimal e, como $M_s \leqslant N$, da maximalidade de M_s, obtém-se $M_s = N$, ou seja, $N/M_s = \{1\}$. Então, $[G/M_s, A]$ possui $s-1$ subgrupos A-invariantes minimais não triviais. Por hipótese de indução, $[G/M_s, A] = \langle M_1Ms/Ms, ..., M_{s-1}Ms/Ms\rangle$, de modo que $[G, A] = \langle M_1, ..., M_s\rangle$, como desejado. □

Lema 3.20. *Se G é abeliano e A-monolítico, então uma das seguintes afirmações ocorre:*

(a) G é de torção: neste caso, G é um p-grupo de expoente no máximo $p^{\ell_A(G)}$, para algum primo p;

(b) G é livre de torção: neste caso, G é divisível.

Demonstração. A prova será feita por indução sobre o número $\ell_A(G)$. Se $\ell_A(G) = 1$, então A é FPF. De fato, como G é A-monolítico, pela Proposicão 3.9, $C = \{1\}$ e, consequentemente, $\overline{\mathcal{L}}_G(A) = \{\{1\}, G\}$. Logo, o único subgrupo A-invariante minimal não trivial de G é o próprio G. Portanto, $C_G(\alpha) = \{1\}$, para todo $\alpha \in A\backslash\{Id_G\}$, isto é, A é FPF. Como A é abeliano, pelo Teorema 2.13, a base da indução fica demonstrada.

Suponha agora que $\ell(G) > 1$. Seja N o único subgrupo A-invariante minimal de G. Assim $\ell(N) = 1$ e, desta forma, N é infinito e $C_G(A) = \{1\}$, pois o par (G, A) satisfaz $(*)$. Considere o grupo quociente $\bar{G} = G/N$, o qual é infinito, pois $\ell(G) > 1$. Sejam $\bar{N}_1, ..., \bar{N}_r$ todos os subgrupos A-invariantes minimais de $\bar{G}$. Logo, pelo lema anterior, existem subgrupos A-invariantes $\bar{M}_1, ..., \bar{M}_r$ de $\bar{G}$, tais que $\bar{N}_1 \leqslant \bar{M}_1, ..., \bar{N}_r \leqslant \bar{M}_r$ e $\bar{G} = \bar{C} \times \bar{M}_1 \times ... \times \bar{M}_r$, com $\bar{C} = C_{\bar{G}}(A)$. Sejam $C, M_1, ..., M_r$ as imagens inversas, pelo epimorfismo canônico, de $\bar{C}, \bar{M}_1, ..., \bar{M}_r$ em G, respectivamente. Pelo Teorema da Correspondência, existe um subgrupo H de G contendo N tal que $\bar{C} = H/N$. É claro que $h^\alpha N = hN$, para todo $h \in H$ e todo $\alpha \in A$. Como $Im(T_\alpha|_H) = N$ para todo $\alpha \in A\backslash C_A(H)$, pelo Primeiro Teorema do Isomorfismo, tem-se que $H/Nuc(T_\alpha|_H) \simeq N$, para todo $\alpha \in A\backslash C_A(H)$. Em particular, pela Proposição 3.4, existe um automorfismo β em A livre de pontos fixos, com $Im(T_\beta|_H) = N$ e $H/Nuc(T_\beta|_H) \simeq N$. Mas $Nuc(T_\beta|_H) = C_H(\beta) = \{1\}$, ou seja, $H \simeq N$ e, portanto, $H = N$, pois N é o único subgrupo A-invariante minimal de G. Assim $\bar{G} = \bar{M}_1 \times ... \times \bar{M}_r$. Fixe agora $i \in \{1, ..., r\}$ e considere $M = M_i$. A demonstração é finalizada em quatro casos:

<u>*Caso 1*</u>: N e M/N possuem elementos livres de torção.

Como $\ell(N), \ell(M/N) < \ell(G)$, da hipótese de indução, segue que N e M/N são livres de torção e divisíveis. Pelo Teorema 1.14, existe um subgrupo K de M tal que $K \simeq M/N$ e $M = N \times K$. Desta forma, M é um produto direto de subgrupos livres de torção e divisíveis, portanto, é também livre de torção e divisível.

Caso 2: M/N é de torção e N possui elemento livre de torção.

Como no Caso 1, existe $K \leqslant M$ tal que $K \simeq M/N$ e $M = N \times K$. Sendo assim, K é o subgrupo de todos os elementos de torção de M, logo K é característico e, assim, K é A-invariante. Absurdo, pois N está contido em todo subgrupo A-invariante não trivial de M. Portanto, tal caso não ocorre.

Caso 3: N é de torção e M/N possui elemento livre de torção.

Por hipótese de indução, existe p primo tal que N é um p-grupo abeliano elementar e M/N é livre de torção e divisível. Pela Proposição 3.9, $M = [M, A] \times C_M(A)$; porém, $C_M(A) = \{1\}$, pois $|N| = \infty$, daí $M = [M, A]$. Logo, pela Proposição 3.6, existe $g \in M$ tal que g^A é A-regular. Se $C_M(\alpha) = \{1\}$, para todo $\alpha \in A$, g pode ser escolhido de tal forma que $g \notin N$ e, se existe $\alpha \in A$ tal que $N \leqslant C_M(\alpha)$, então $g \notin C_M(\alpha)$ e, assim, tem-se também $g \notin N$. Daí, gN é um elemento livre de torção em M/N. Em particular, g é livre de torção. Considere agora $x \in N\backslash\{1\}$. Existem um inteiro positivo s e $\alpha_1, ..., \alpha_s \in A$ tais que $x = g^{\alpha_1}...g^{\alpha_s}$, pois $N \leqslant \langle g^A \rangle$ e G é abeliano. Defina $\epsilon = \sum_{i=1}^{s} \alpha_i$; logo $\epsilon \in E(A) \leqslant End(M)$ e, daí, $(g^p)^\epsilon = x^p = 1$. Como $g^p \neq 1$ deve-se ter $N \leqslant Nuc(\epsilon) < M$, pois $g \notin Nuc(\epsilon)$. Uma vez que M/N é divisível, existe $hN \in M/N$ tal que $(hN)^p = gN$, logo $h^p = gy$, para algum $y \in N$ e, daí, $(h^p)^\epsilon = (gy)^\epsilon = g^\epsilon y^\epsilon = x \neq 1$. Desta forma, h^ϵ é um elemento de M de ordem p^2, contradizendo o fato de que o subgrupo de torção de M é N e N possui expoente p. Portanto, tal caso não ocorre.

Caso 4: N e M/N são subgrupos de torção.

Por hipótese de indução, existem números primos p e q tais que N é um p-grupo abeliano elementar e M/N é um q-grupo abeliano de expoente no máximo $q^{\ell(M)-1}$. Assim, claramente, M possui expoente no máximo $pq^{\ell(M)-1}$. Tome $y \in M$ tal que $|y| = q$. Como $\langle y^A \rangle$ é A-invariante e N é o único subgrupo A-invariante minimal de G, tem-se $N \leqslant \langle y^A \rangle$. Logo, para todo $n \in N\backslash\{1\}$ existem $\alpha_1, ..., \alpha_s \in A$ tais que $y^{\alpha_1}...y^{\alpha_s} = n$ e, assim, $n^q = 1$; mas $n^p = 1$, portanto, $q = p$. Com isso, M é um p-grupo abeliano de expoente no máximo $p^{\ell(G)}$.

Segue desses quatro fatos, que se N é um p-grupo, M é um p-grupo de expoente no máximo $p^{\ell(G)}$ e, se N é livre de torção e divisível, então M também é livre de torção e divisível. Como $G = \langle M_1, ..., M_r \rangle$, o resultado segue. $\square$

Segue dos Lemas 3.19 e 3.20 e usando indução junto com a Proposição 3.11 o

Teorema B. *Sejam G um grupo abeliano infinito e A um grupo abeliano de automorfismos de G, tal que G é uma união de um número finito de A-órbitas e A centraliza toda seção finita A-invariante de G. Então existem um inteiro positivo r, subgrupos $B_1, ..., B_r$ de A e subgrupos A-invariantes $G_1, ..., G_r$ de G tais que $B = B_1 \times ... \times B_r$ possui índice finito em A, $G = C_G(A) \times G_1 \times ... \times G_r$ e*

(a) B_i age trivialmente sobre G_j, para todo $i \neq j$, com $i, j = 1, ..., r$;

(b) G_i é um subgrupo B_i-monolítico de G, para todo $i = 1, ..., r$.

Além disso, cada G_i ou é um p-grupo de expoente no máximo $\ell(G_i)$, para algum primo p, ou é um grupo livre de torção e divisível.

3.3 Teorema A

Por fim a demonstração do *Teorema A*.

Teorema A. *Sejam G um grupo e A um subgrupo abeliano de $Aut(G)$ tais que G é uma união de um número finito de A-órbitas e o par (G, A) satisfaz a condição $(*)$. Então*

(a) G é abeliano-por-finito;

(b) Se G é livre de torção, então G é abeliano e divisível;

(c) O grupo A possui expoente infinito.

Demonstração. Como o par (G, A) satisfaz a condição $(*)$, pelo Teorema 3.16, $[G, A]$ é um BFC-grupo; desta forma, pelo Teorema 1.40, $[G, A]$ é finito-por-abeliano, ou seja, $[G, A]'$ é finito. Para provar o item (a) é suficiente mostrar que $[G, A]$ é abeliano, pois $[G, A] \lhd G$ e $|G : [G, A]| < \infty$. O raciocínio será feito por contradição. Como $[G, A] = [[G, A], A]$, pode-se supor, sem perda de generalidade, que $G = [G, A]$, assim $|G'|$ é finito. Suponha, também, que G não é abeliano e que minimiza o número $|G'| + |\mathcal{L}_A(G/G')|$. Denote o grupo quociente abeliano G/G' por $\bar{G}$. A demonstração, agora, seguirá em onze passos.

(1) $G' = C_G(A)$.

De fato, como $G = [G, A]$, então $\bar{G} = [\bar{G}, A]$. Uma vez que o par $(\bar{G}, A)$ também satisfaz a condição $(*)$, pela Proposição 3.9, $\bar{G} = [\bar{G}, A] \times C_{\bar{G}}(A)$ e, assim, $C_{\bar{G}}(A) = \{1\}$, daí $C_G(A) \leqslant G'$. Como G' é um subgrupo A-invariante finito e o par (G, A) satisfaz a condição $(*)$, da Proposição 3.3 item (b), segue que $G' \leqslant C_G(A)$. A afirmação segue.

(2) $Z(G) = G'$.

Primeiramente, vale que $Z(G) \leqslant C_G(A)$. De fato, suponha, por absurdo, que $Z(G)$ não está contido em $C_G(A)$. Logo, $Z(G)$ é infinito e o par $(Z(G), A)$ satisfaz a condição $(*)$, pois $Z(G)$, sendo característico, é A-invariante. Assim, pela Proposição 3.9,

$$Z(G) = [Z(G), A] \times C_{Z(G)}(A).$$

Considere o grupo quociente $\tilde{G} = G/[Z(G), A]$. Como $Z(G)$ é infinito, $[Z(A), A]$ também o é, assim, $[Z(G), A]$ não está contido no subgrupo finito G' e, com isso, $|\tilde{G}'| + |\mathcal{L}_A(\tilde{G}/\tilde{G}')| < |G'| + |\mathcal{L}_A(G/G')|$. Daí, $\tilde{G}$ é abeliano por causa da escolha minimal de G. Desta forma, $G' \leqslant [Z(G), A]$ e, então, $G' = G' \cap [Z(G), A] = C_G(A) \cap [Z(G), A] = \{1\}$ e, consequentemente, G é abeliano, absurdo. Portanto, $Z(G) \leqslant C_G(A) \leqslant G'$. Por outro lado, pelo Teorema 3.15, o grupo G é nilpotente de classe no máximo 2 e, daí, $G' \leqslant Z(G)$. Fica demonstrada a afirmação.

(3) Cada subgrupo normal A-invariante não trivial de G contém G'.

Seja $\{1\} \neq N \lhd G$ um subgrupo A-invariante de G. Como G é nilpotente e $G' = Z(G)$ tem-se $G' \cap N \neq \{1\}$. Se $\hat{G} = G/N$, então $|\hat{G}'| = |G'/(G' \cap N)| < |G'|$ e, como $\hat{G}/\hat{G}' \simeq G/G'N$, tem-se que $|\mathcal{L}_A(\hat{G}/\hat{G}'| \leqslant |\mathcal{L}_A(G/G')|$, isto é, $|\hat{G}'| + |\mathcal{L}_A(\hat{G}/\hat{G}')| < |G'| + |\mathcal{L}_A(G/G')|$, donde $\hat{G}$ é abeliano. Assim, N contém G'.

(4) $\bar{G}$ não é um produto direto de dois subgrupos A-invariantes minimais não triviais.

Suponha que $\bar{G} = \bar{N}_1 \times \bar{N}_2$, com $\bar{N}_1$ e $\bar{N}_2$ subgrupos A-invariantes minimais. Se $\ell(\bar{N}_i) = 0$ para algum $i \in \{1, 2\}$, então $\bar{N}_i$ é finito. Logo, sendo N_j a imagem inversa de $\bar{N}_j$ em G, para $j \in \{1, 2\}$, tem-se que N_j também é finito, pois $\bar{N}_j = N_j/G'$ e G' é finito. Assim, $N_j \leqslant C_G(A) = G'$ o que implica $\bar{N}_j = \{1\}$, absurdo. Logo $\ell(\bar{N}_1), \ell(\bar{N}_2) > 0$. Pela Proposição 3.11, existe $B \leqslant A$, tal que $|A : B| < \infty$, $B = B_1 \times B_2$ e $B_1 = C_B(\bar{N}_2)$ e $B_2 = C_B(\bar{N}_1)$. Assim, B age sobre $\bar{N}_1$ como B_1 age. Como $\bar{N}_1$ é infinito, B_1 é abeliano e FPF sobre $\bar{N}_1$, pois $\bar{N}_1$ é minimal, e $\bar{N}_1$ é uma união de um número finito de B_1-órbitas, pelo Teorema 2.14, existe um corpo apropriado K tal que $\bar{N}_1 \simeq K^+$ e B_1 pode ser identificado com um subgrupo de índice finito de $K^\times$. Pela Proposição A.17 (veja Apêndice), existem $\alpha, \beta \in B_1$ tais que $\beta = 1 + \alpha$. Assim para cada $\bar{x} \in \bar{N}_1$ tem-se que $\bar{x}^\beta = \bar{x}\bar{x}^\alpha$. Logo, para cada $x \in N_1$ existe um $c_x \in G' = Z(G) = C_G(A)$ tal que $x^\beta = xx^\alpha c_x$. Tomando agora $x \in N_1$ e $y \in N_2$, existe $c \in G' = Z(G) = C_G(A)$ tal que $y^\beta = yc$, pois $\bar{y}^\beta = \bar{y}$. Daí,

$$[x, y] = [x, y]^\beta = [xx^\alpha c_x, yc] = [xx^\alpha, y] = [x, y]^{x^\alpha}[x^\alpha, y] = [x, y][x^\alpha, y],$$

donde $[x^\alpha, y] = 1$. Assim, tem-se que $[N_1, N_2] = \{1\}$. Agora, pela escolha minimal de G, deve-se ter N_1 e N_2 abelianos e, como $G = N_1N_2$, obtém-se que G é abeliano, absurdo. O resultado segue.

(5) $\bar{G}$ admite um único subgrupo A-invariante minimal não trivial $\bar{N}$.

Suponha, por absurdo, que $\bar{N}_1, ..., \bar{N}_r$ são subgrupos A-invariantes minimais não triviais de $\bar{G}$, com $r > 1$. Pelo Lema 3.19, $\bar{G} = \bar{M}_1 \times ... \times \bar{M}_r$, com $\bar{M}_i$ subgrupo de G A-monolítico contendo $\bar{N}_i$, para todo $i = 1, ..., r$. Seja M_i a imagem inversa de $\bar{M}_i$ em G, para cada $i = 1, ..., r$. Cada M_i é normal em G e, como $r > 1$, é também abeliano, pois $|M_i'| + |\mathcal{L}_A(M_i/M_i')| < |G'| + |\mathcal{L}_A(G/G')|$. Se $r > 2$, então cada M_iM_j é também abeliano, pelo mesmo argumento deste paragráfo, daí, $[M_i, M_j] = \{1\}$, para todos $i, j \in \{1, ..., r\}$. Logo, G é abeliano, absurdo. Se $r = 2$, suponha inicialmente que N_1 é um subgrupo próprio de M_1. Então N_1M_2 é um subgrupo próprio de G e $|G : N_1M_2|$ não é finito, pois $|M_1 : N_1|$ não é finito, logo $|(N_1M_2)'| + |\mathcal{L}_A(N_1M_2)/(N_1M_2)'| < |G'| + |\mathcal{L}_A(G/G')|$, ou seja, N_1M_2 é abeliano. Assim, se $g = m_1m_2 \in G$, com $m_1 \in M_1$ e $m_2 \in M_2$ e $n \in N_1$, então $ng = nm_1m_2 = m_1m_2n = gn$, isto é, $N_1 \leqslant Z(G) = G'$, donde $\bar{N}_1 = \{1\}$, absurdo. Logo, $M_1 = N_1$ e, analogamente, $M_2 = N_2$. Desta forma, $\bar{G} = \bar{N}_1 \times \bar{N}_2$, absurdo, pelo passo (4). Portanto, o resultado segue.

(6) $\mathcal{L}_A(\bar{G})$ é uma cadeia.

Sejam $K_1 = \bar{G}$ e $K_2 = \bar{G}/\bar{G}_1$, onde $\bar{G}_1 = \bar{N}$. Analogamente ao passo (5), mostra-se que K_2 possui um único subgrupo A-invariante minimal não trivial $\tilde{G}_2$. Seja $\bar{G}_2$ a imagem inversa de $\tilde{G}_2$ em $\bar{G}$ e coloque $K_3 = \bar{G}/\bar{G}_2$. Defina agora indutivamente para $i \geqslant 1$ o grupo quociente $K_{i+1} = \bar{G}/\bar{G}_i$, em que $\bar{G}_i$ é a imagem inversa do único subgrupo A-invariante minimal não trivial $\tilde{G}_i$ de K_i. Prova-se por indução, analogamente ao argumento do passo (5), que K_{i+1} possui único subgrupo A-invariante minimal não trivial $\tilde{G}_{i+1}$ e, que após uma quantidade finta $k-1$ de passos, com $k \geqslant 2$, tem-se que $\bar{G}/\bar{G}_{k-1}$ é o único minimal não trivial de K_k, ou seja, $\bar{G}_k = \bar{G}$. Seja $\mathcal{L}$ o conjunto dos subgrupos $\bar{G}_i$'s em $\bar{G}$. Observe que $\mathcal{L}$ é uma cadeia. Suponha, por absurdo, que existe $S \in \mathcal{L}_A(\bar{G})\backslash\{1\}$ tal que $S \notin \mathcal{L}$. Como $\bar{G}_1 \leqslant S$, pois $\bar{G}_1$ é o único subgrupo minimal não trivial de $\bar{G}$, então $S/\bar{G}_1$ contém $\tilde{G}_2$, ou seja, $\bar{G}_2 \leqslant S$. Se $\bar{G}_2 < S$, então $S/\bar{G}_2$ contém $\tilde{G}_3$, ou seja, $\bar{G}_3 \leqslant S$. Se $\bar{G}_3 < S$, então $S/\bar{G}_3$ contém $\tilde{G}_4$. Após uma quantidade finita de passos tem-se que $S = \bar{G}_{i+1}$, absurdo, pois $S \notin \mathcal{L}$. Então, $\mathcal{L} \cup \{1\} = \mathcal{L}_A(\bar{G})$. Assim, pode-se por $\mathcal{L}_A(\bar{G}) = \{\bar{G}_0, \bar{G}_1, ..., \bar{G}_k\}$, onde $\bar{G}_0 = \{1\} < \bar{G}_1 = \bar{N} < ... < \bar{G}_{k-1} < \bar{G}_k = \bar{G}$ e, se G_i é a imagem inversa de $\bar{G}_i$ e N a imagem inversa de $\bar{N}$ em G, então $\{1\} < G_0 = G' < G_1 = N < ... < G_{k-1} < G_k = G$.

(7) $C_A(\bar{N}) = C_A(\bar{G}/\bar{M})$, onde $M = G_{k-1}$. Além disso, existem um corpo K e $T \leqslant K^\times$, com $|K^\times : T| < \infty$, tais que $\bar{N} \simeq \bar{G}/\bar{M} \simeq K^+$, $A/C_A(\bar{N}) \simeq A/C_A(\bar{G}/\bar{M}) \simeq T$ e a ação de T sobre $\bar{N}$ e $\bar{G}/\bar{M}$ é a multiplicação de K.

Se $k = 1$, então $\bar{M} = \bar{G}_0 = \{1\}$ e, assim, $\bar{N} \simeq \bar{G}/\bar{M}$, logo $C_A(\bar{N}) = C_A(\bar{G}/\bar{M})$. Agora, se $k > 1$, então o grupo $\bar{G}/\bar{G}_{k-2}$ possui um único subgrupo A-invariante próprio e não trivial, a saber, $\bar{M}/\bar{G}_{k-2}$. Como $\bar{G}/\bar{G}_{k-2}$ é abeliano e o par $(\bar{G}/\bar{G}_{k-2}, A)$ satisfaz $(*)$, pela Proposição 3.10, tem-se que $C_A(\bar{M}/\bar{G}_{k-2}) = C_A((\bar{G}/\bar{G}_{k-2})/(\bar{M}/\bar{G}_{k-2})) = C_A(\bar{G}/\bar{M})$. Esse processo pode ser repetido na cadeia $\{1\} = \bar{G}_0 < N = \bar{G}_1 < ... < \bar{G}_{k-1} = \bar{M}$ para obter $C_A(\bar{G}_{k-2}/\bar{G}_{k-3}) = C_A(\bar{M}/\bar{G}_{k-3})$. Continuando, obtem-se $C_A(\bar{N}/\bar{G}_0) = C_A(\bar{G}_3/\bar{G}_2)$. Logo, $C_A(\bar{N}) = C_A(\bar{G}_3/\bar{G}_2) = ... = C_A(\bar{G}_{k-2}/\bar{G}_{k-3}) = C_A(\bar{G}/\bar{M})$, como desejado. Como $A/C_A(\bar{N})$ é FPF sobre $\bar{N}$ e $\bar{N}$ é uma união de um número finito de $A/C_A(\bar{N})$-órbitas, a segunda parte segue pelo Teorema 2.14.

(8) M é abeliano e $[M, N] = \{1\}$.

Tem-se que $|M'| + |\mathcal{L}_A(M/M')| < |G'| + |\mathcal{L}_A(G/G')|$, donde M é abeliano. Se $k = 1$, então $N = G$ e $M = G_0 = Z(G)$, logo $[M, N] = \{1\}$. Se $k > 1$, segue que $N \leqslant M$ e, como M é abeliano, $[M, N] = \{1\}$.

(9) Existem $\alpha, \beta \in A$ tais que, para cada $\bar{x} \in \bar{N}$ e cada $\bar{y} \in \bar{G}/\bar{M}$ tem-se que $\bar{x}^{\bar{\beta}} = \bar{x}\bar{x}^{\bar{\alpha}}$ e $\bar{y}^{\bar{\beta}} = \bar{y}\bar{y}^{\bar{\alpha}}$. Além disso, o automorfismo α pode ser escolhido de tal maneira que $\bar{\alpha}^3 \notin C_A(\bar{N})$.

A primeira parte segue direto da Proposição A.17. Agora, como cada corpo contém no máximo três elementos $\bar{\alpha}$ tais que $\bar{\alpha}^3 = 1$ e os pares $(\bar{\alpha}, \bar{\beta})$ existem em uma infinidade, tome $\bar{\alpha}$ de tal maneira que $\bar{\alpha}^3 \neq 1$, ou seja, tal que $\bar{\alpha}^3 \notin C_A(\bar{N})$.

(10) Se $x \in N$ e $y \in G$, então existe $\alpha \in A$ tal que $\bar{\alpha}^3 \notin C_A(\bar{N})$ e $[x^\alpha, y][x, y^\alpha][x, y] = 1$.

Se $\bar{x} \in \bar{N}$, então existem $\alpha, \beta \in A$ tais que $\bar{x}^{\bar{\beta}} = \bar{x}\bar{x}^{\bar{\alpha}}$ e, assim, para cada $x \in N$ existe um $c_x \in G' = Z(G)$ tal que $x^\beta = xx^\alpha c_x$. Analogamente, para cada $y \in G$ existe um $m_y \in M$ tal que $y^\beta = yy^\alpha y_y$. Pelo passo (8), $[n, m_y] = 1$, para qualquer n em N. Assim, e considerando que $G' = Z(G) = C_G(A)$, obtém-se

$$[x, y] = [x, y]^\beta = [x^\beta, y^\beta] = [xx^\alpha c_x, yy^\alpha m_y] = [xx^\alpha, yy^\beta m_y] = [xx^\alpha, m_y][xx^\alpha, yy^\alpha]^{m_y} =$$

$$= [xx^\alpha, yy^\alpha] = [x, yy^\alpha]^{x^\alpha}[x^\alpha, yy^\alpha] = [x, y^\alpha][x, y]^{y^\alpha}[x^\alpha, y^\alpha][x^\alpha, y]^{y^\alpha} = [x, y][x^\alpha, y][x, y^\alpha][x, y]$$

e, assim, tem-se a conclusão.

(11) $N \leqslant Z(G)$.

Dados $x \in N$ e $y \in G$, pelo passo (10), pode-se escolher $\alpha \in A$, com $\alpha^3 \notin C_A(\bar{N})$, tal que $[x^\alpha, y][x, y^\alpha] = [x, y]^{-1}$ e $[x^{\alpha^2}, y][x^\alpha, y^\alpha] = [x^\alpha, y]^{-1}$. Lembrando que $[x^\alpha, y^\alpha] = [x, y]$ e que $G' = Z(G)$, segue que $[x^{\alpha^2}, y][x^\alpha, y^\alpha][x, y^\alpha]^{-1} = [x^\alpha, y]^{-1}[x, y^\alpha]^{-1} = [x, y]$. Logo $[x^{\alpha^2}, y] = [x, y^\alpha]$ e, assim, $[x^{\alpha^3}, y] = [(x^\alpha)^{\alpha^2}, y] = [x^\alpha, y^\alpha] = [x, y]$, ou seja, $[x, y]^{-1}[x^{\alpha^3}, y] = 1$. Mas

$$[x, y]^{-1}[x^{\alpha^3}, y] = [y, x][x^{\alpha^3}, y] =$$

$$= y^{-1}x^{-1}yxx^{-\alpha^3}y^{-1}x^{\alpha^3}x^{-1}yy^{-1}xy = [x^{-1}x^{\alpha^3}, y]^{(x^{-1})^y} = [x^{-1}x^{\alpha^3}, y].$$

Então $[N, \alpha^3] \leqslant Z(G)$. Como $\alpha^3 \notin C_A(\bar{N})$, tem-se que $[\bar{N}, \bar{\alpha}^3] = \bar{N}$, isto é, $N = [N, \alpha^3]Z(G)$, donde $N \leqslant Z(G)$.

Mas, isso contradiz o fato de que N é infinito enquanto $Z(G)$ não é. Portanto, $[G, A]$ é abeliano, provando o item (a).

Para provar o item (b), pelo Teorema 3.15, sabemos que o FC-grupo $\widehat{Z}(G)$ é BFC-grupo; logo $\widehat{Z}(G)'$ é finito e como $\widehat{Z}(G)$ é livre de torção, pois G é livre de torção, tem-se que $\widehat{Z}(G)' = \{1\}$, donde $\widehat{Z}(G)$ é abeliano. Daí, como $C_{\widehat{Z}(G)}(A) = \{1\}$, do Teorema B segue que $\widehat{Z}(G)$ é um produto direto de subgrupos divisíveis e, assim, $\widehat{Z}(G)$ é também divisível. Se $G = \widehat{Z}(G)$, já se tem o desejado. Suponha, por absurdo, que $G \neq \widehat{Z}(G)$. Do fato de $[G, A]$ ser abeliano segue que é BFC-grupo, logo $[G, A] \leqslant \widehat{Z}(G)$ e, então, $G/\widehat{Z}(G)$ é finito. Assim A centraliza $G/\widehat{Z}(G)$. Como $G \neq \widehat{Z}(G)$, existe $g \in G\backslash\widehat{Z}(G)$. Considere o subgrupo $H = \widehat{Z}(G)\langle g\rangle$, daí, $H/\widehat{Z}(G) \leqslant G/\widehat{Z}(G)$, H é A-invariante e existe um inteiro positivo m tal que $g^m \in \widehat{Z}(G)$. Como G é livre de torção, $g^m \neq 1$; consequentemente, $Z(H) \neq 1$, pois $g^m \in Z(H)$. Além disso, $Z(H) \leqslant \widehat{Z}(G)$, pois se $y \in Z(H)$, então $H \leqslant C_G(y)$, daí $|G : C_G(y)| < \infty$. Como $\widehat{Z}(G)$ é divisível, existe $h \in \widehat{Z}(G)$ tal que $g^m = h^m$. Agora, como $\widehat{Z}(G)/Z(H)$ é divisível, então pelo Teorema B, é livre de torção. Mas $h^m = g^m \in Z(H)$ e $h \in \widehat{Z}(G)$, daí $\bar{h} = 1$ em $\widehat{Z}(G)/Z(H)$ e, assim, $h \in Z(H)$. De $h \in \widehat{Z}(G)$ e $g \notin \widehat{Z}(G)$ vem que $gh^{-1} \neq 1$ e, como $h \in Z(H)$ e $g \in H$ tem-se que $(gh^{-1})^m = g^m h^{-m} = 1$. Mas isto contradiz a hipótese de G ser livre de torção. Logo, $G = \widehat{Z}(G)$ e, como $\widehat{Z}(G)$ é abeliano e divisível, o resultado segue.

Para o item (c) suponha que G é infinito. Seja H um subgrupo normal A-invariante minimal de $[G, A]$. Logo, $A/C_H(A)$ é FPF sobre H Pelo Teorema 2.14, existe um corpo apropriado K, de cardinalidade infinita, tal que $H \simeq K^+$ e $A/C_A(H)$ age sobre H como age a multiplicação de um subgrupo de índice finito de $K^\times$ sobre K. Pela Proposição A.14, o grupo $A/C_A(N)$ possui expoente infinito; daí, A possui expoente infinito. $\square$

Apêndice A

Apêndice ao Capítulo 3

1.1 O Teorema de Hales-Jewett

Nesta primeira parte do apêndice será apresentado um resultado de combinatória conhecido como *Teorema de Halles - Jewett*, o qual é um dos principais resultado da *Teoria de Ramsey*.

Definição A.1. Sejam n e t inteiros positivos e $A = \{a_1, ..., a_t\}$ um conjunto com t elementos. O *n-cubo* sobre A é o conjunto

$$C_t^n = \{(x_1, ..., x_n); x_i \in A, i = 1, ..., n\}.$$

Dados n e t inteiros positivos e conjuntos A_1 e A_2 tais que $|A_1| = |A_2| = t$, existe uma bijeção entre os n-cubos sobre A_1 e A_2 . Além disso, os resultados obtidos para um particular n-cubo sobre um conjunto com t elementos valem para todo $n-cubo$ definido sobre um conjunto com t elementos. Por isso, no restante deste texto, quando for mencionado o n-cubo C_t^n, será considerado, sem perda de generalidade, que o conjunto A sobre o qual C_t^n está definido é o conjunto $\{0, 1, ..., t-1\}$, ou seja, C_t^n será dado por

$$C_t^n = \{(x_1, ..., x_n); x_i \in \{0, 1, ..., t-1\}, i = 1, ..., n\}.$$

Definição A.2. Sejam n e t inteiros positivos. Uma *linha* em C_t^n é um subconjunto ordenado $L = \{x_0, x_1, ..., x_{t-1}\}$ com t elementos e $x_i = (x_{i1}, ..., x_{in})$, $i = 0, 1, ..., t-1$, tal que para cada j, $j = 1, ..., n$, ou

$$x_{0j} = ... = x_{(t-1)j}$$

ou

$$x_{ij} = i, \quad \text{para algum} \quad i = 0, 1, ..., t-1.$$

e a segunda condição ocorre para pelo menos um j.

Como exemplo de uma linha, se $n = 3$ e $t = 4$ o conjunto

$$L = \{(0, 2, 0), (1, 2, 1), (2, 2, 2), (3, 2, 3)\}$$

é uma linha em C_4^3.

Definição A.3. Sejam n e t inteiros positivos, $1 \leqslant k \leqslant n$ e $B_0, B_1, ..., B_k \subsetneqq \{1, ..., n\}$ tais que $\{1, ..., n\} = B_0 \biguplus B_1 \biguplus ... \biguplus B_k$, com $B_i \neq \emptyset$ para todo $i = 1, ..., n$. Considere uma aplicação $f : B_0 \to \{0, 1, ..., t-1\}$ e defina $\widehat{f} : C_t^k \to C_t^n$ dada por $(y_1, ..., y_k)\widehat{f} = (x_1, ..., x_n)$, com $x_i = (i)f$, se $i \in B_0$ e $x_i = y_j$, se $i \in B_j$, $1 \leqslant j \leqslant n$. O conjunto $Im(\widehat{f})$ é chamado de *subespaco k-dimensional de* C_t^n.

Para exemplificar, sejam $n = 7$, $t = 3$, $k = 2$, $B_0 = \{1, 2\}$, $B_1 = \{3, 4\}$, $B_2 = \{5, 6, 7\}$ e $f : B_0 \to \{0, ..., 6\}$ dada por $(1)f = 0$ e $(2)f = 2$. Assim $\widehat{f} : C_3^2 \to C_3^7$ é definida por $(x, y)\widehat{f} = (0, 2, x, x, y, y, y)$ e o subespaço k-dimensional com respeito a f é dado por $Im(\widehat{f}) = \{(0, 2, x, x, y, y, y); x, y \in \{0, 1, 2\}\}$.

Observação A.4. Seguindo as notações da Definição A.3 seguem as seguinte observações:

1. Se S é um subespaço k-dimensional com respeito à função f, então $\varphi : C_t^k \to S$ definida por $(y_1, ..., y_k)\varphi = (x_1, ..., x_n)$ em que $x_j = y_i$ se $j \in B_i$, com $i \neq 0$, e $x_j = (j)f$ se $j \in B_0$ é claramente uma bijeção entre C_t^k e S. Desta forma, S é considerado um k-cubo imerso no n-cubo C_t^n.

2. Seja $L = \{x_0, ..., x_{t-1}\}$ uma linha em C_t^n, como nas notações da Definição A.2. Defina $B_0 = \{j \in \{1, ..., n\}; x_{0j} = ... = x_{(t-1)j}\}$ e $B_1 = \{j \in \{1, ..., n\}; x_{ij} = i\}$. É claro que $\{1, ..., n\} = B_0 \biguplus B_1$ e $B_1 \neq \emptyset$, pela definição de L. Se $f : B_0 \to \{0, ..., t-1\}$ é dada por $(j)f = a_j$, em que $a_j = x_{0j}$, então $Im(\widehat{f}) = L$. Logo L é um subespaço 1-dimensional de C_t^n que pode ser escrito na forma:

$$L = \{(x, ..., x, a_{j_1}, x, ..., x, a_{j_l}, x, ..., x, a_{j_{|B_0|}}, x, ..., x) \in C_t^n; x = 0, 1, ..., t-1\},$$

com $j_l \in B_0$ para todo $l = 1, ..., |B_0|$ e $j_1 < j_2 < ... < j_{|B_0|}$.

As três definições a seguir dizem respeito aos conceitos de coloração, subconjunto monocromático e coloração por camadas.

Definição A.5. Sejam n, t e r inteiros positivos. Uma *r-coloração* de C_t^n é uma função $f : C_t^n \to \{1, ..., r\}$. Dada uma *$r$-coloração* f de C_t^n, diz-se que C_t^n é *r-colorido*.

Definição A.6. Sejam n, t e r inteiros positivos e f uma r-coloração de C_t^n. Se $C \subseteqq C_t^n$ é tal que existe $i \in \{1, ..., r\}$ com $(C)f = \{i\}$, então C é chamado de *i-colorido* ou *monocromático*.

Definição A.7. Sejam n, t e r inteiros positivos e f uma r-coloração de C_{t+1}^n. Para cada $i = 0, 1, ..., n$ defina $C_i = \{(x_1, ..., x_n) \in C_{t+1}^n ; x_j \neq t,$ se $1 \leqslant j \leqslant n - i$ e $x_j = t,$ se $n - i < j \leqslant n\}$. Então f é dita ser uma coloração *por camadas* se C_i é monocromático por f para todo $i = 0, 1, ..., n$.

Seguindo as notações da Definição A.2, um subespaço k-dimensional C de C_{t+1}^n é chamado *por camadas* se existe uma bijeção $\alpha : C_{t+1}^k \to C$ tal que a r-coloração $\alpha \circ f$ de C_{t+1}^k é por camadas. Assim, uma linha L de C_t^n é dita por camadas se existe uma bijeção $\alpha_L : C_{t+1}^1 \to L$ tal que a r-coloração $\alpha_L \circ f$ de C_{t+1}^1 leva os t "primeiros" pontos de C_{t+1}^1 em um único i, com $i \in \{1, ..., r\}$.

Exemplo A.8. Se $n = 4$, $t = 10$, então a linha $L = \{(x, 1, x, x); x \in \{0, 1, ..., 10\}\}$ de C_{11}^4 é por camadas se $(0, 1, 0, 0), ..., (9, 1, 9, 9)$ possuem a mesma cor por f. Agora, se o subespaço 2-dimensional $S = \{(x, 1, y, y); x, y \in \{0, 1, ..., 10\}\}$ de C_{11}^4 é por camadas, então $(1, 1, 1, 1)$ e $(2, 1, 2, 2)$ possuem a mesma cor por f e $(2, 1, 10, 10)$, $(3, 1, 10, 10)$ possuem a mesma cor por f.

Os três próximos resultados são, em essência, a demonstração do Teorema de Hales-Jewett, cujo enunciado é

Teorema A.9. (Hales-Jewet) *Para todos inteiros positivos r e t, existe $N' = HJ(r, t)$ tal que para todo $N \geqslant N'$ e toda r-coloração de C_t^N, existe uma linha monocromática em C_t^N.*

Esse teorema será demonstrado por indução. A base dessa demonstração é simples, mas para terminar a indução será necessário o Teorema A.10 junto com o Corolário A.12, os quais serão dados a seguir.

Teorema A.10. *Seja t um inteiro positivo e suponha que para cada inteiro positivo r exista $N' = N'(r,t)$ tal que, para todo $N \geqslant N'$ e toda r-coloração de C_t^N, existe uma linha monocromática em C_t^N. Então, dados inteiros positivos k e t, existe $M' = M'(r,t,k)$ satisfazendo o seguinte: para todo $M \geqslant M'$, se C_{t+1}^M é r-colorido, então existe um subespaço k-dimensional por camadas em C_{t+1}^M.*

Demonstração. A demonstração será feita por indução sobre k. Se $k = 1$, considere $M' = N'$ e $M \geqslant M'$ e f uma r-coloração de C_{t+1}^M. O subconjunto C de C_{t+1}^M dado por

$$C = \{(x_1, ..., x_M); x_i \in \{0, ..., t-1\}, i = 1, ..., M\}$$

pode ser identificado trivialmente com C_t^M. Logo $f|_C$ é uma r-coloração do M-cubo $C \approx C_t^M$. Por hipótese, existe uma linha $L = \{x_0, ..., x_{t-1}\}$ monocromática em C. Tomando B_0, B_1, como na Observação A.4, e $x_t = (x_{t0}, ..., x_{tM})$ tal que $x_{tj} = x_{0j}$ se $j \in B_0$ e $x_{tj} = t$ se $j \in B_1$, claramente $L \cup \{x_t\}$ é um subespaço 1-dimensional por camadas em C_{t+1}^M.

Suponha agora que $k \geqslant 1$ e que a existência de $N' = N'(r,t)$, para todo r, implica a existência de $M'(r,t,k)$, para todo inteiro $r \geqslant 1$. Sejam r um inteiro positivo e $m = M'(r,t,k)$. O número de r-colorações distintas de C_{t+1}^m é $s = r^{(t+1)^m}$. Escolha $m' = N'(s,t)$. Seja χ uma r-coloração de $C_{t+1}^{m'+m}$. O $(m'+m)$-cubo $C_{t+1}^{m'+m}$ pode ser visto, naturalmente, na forma $C_{t+1}^{m'+m} = C_{t+1}^{m'} \times C_{t+1}^m$. Logo um ponto $z \in C_{t+1}^{m'+m}$ pode ser escrito como $z = (x,y)$ com $x \in C_{t+1}^{m'}$ e $y \in C_{t+1}^m$.

Agora, considere o conjunto R de todas as r colorações de C_{t+1}^m. Logo, $|R| = s$. Seja

$$\varphi : C_{t+1}^{m'} \to R$$

$$x \mapsto \varphi_x$$

em que

$$\varphi_x : C_{t+1}^m \to \{1, ..., r\}$$

$$y \mapsto (y)\varphi_x = (x,y)\chi.$$

Escreva $C_{t+1}^{m'} = \{y_1, y_2, ..., y_{(t+1)^m}\}$ e defina uma s-coloração χ^* de $C_{t+1}^{m'}$ da seguinte forma: Para todo $x \in C_{t+1}^{m'}$, seja $\bar{x} = ((y_1)\varphi_x, (y_2)\varphi_x, ..., (y_{(t+1)^m})\varphi_x)$ e denote por $[x]$ o conjunto $\{x' \in C_{t+1}^{m'}; \overline{x'} = \overline{x}\}$. Coloque $W = \{[x]; x \in C_{t+1}^{m'}\}$ e sejam $w_1, w_2, ..., w_{|W|}$ elementos de $C_{t+1}^{m'}$

tais que $W = \{[w_1][w_2], ..., [w_{|W|}]\}$. Assim, dado $x \in C_{t+1}^{m'}$, existe um único $j \in \{1, ..., |W|\}$ tal que $[x] = [w_j]$. Defina $(x)\chi^* = j$. Como $|W| \leqslant s$, χ^* é uma s-coloração de $C_{t+1}^{m'}$. Além disso, tem-se que $(x)\chi^* = (x')\chi^*$ se, e somente se, $(x, y)\chi = (x', y)\chi$, para todo $y \in C_{t+1}^{m}$.

Pela escolha de m', existe uma linha $\{x_0, ..., x_t\}$ monocromática por χ^* em $C_{t+1}^{m'}$, daí, para todos $i, j \in \{0, 1, ..., t\}$ tem-se $(x_i)\chi^* = (x_j)\chi^*$ e, consequentemente, $(x_i, y)\chi = (x_j, y)\chi$, para todo $y \in C_{t+1}^{m}$. Defina agora uma r-coloração χ^{**} de C_{t+1}^{m} colocando $(y)\chi^{**} = (x_0, y)\chi$, para todo $y \in C_{t+1}^{m}$. Por hipótese de indução, existe um subespaço k-dimensional A por camadas, em relação a χ^{**}, em C_{t+1}^{m}. Sejam, como na Definição A.3 e Observação A.4, os subconjuntos $A_0, ..., A_k$ de A. Considere o subespaço $(k+1)$-dimensional $T = \{(x_i, a); 0 \leqslant i \leqslant t, a \in A\}$ de $C_{t+1}^{m'+m}$ e sejam $T_j = \{(x_i, a); 0 \leqslant i < t, a \in A_j\}$, $j = 0, 1, ..., k$ e $T_{(k+1)} = \{(x_t, y)\}$, com $y = (t, ..., t)$. Segue que T é por camadas, em relação a χ, em $C_{t+1}^{m'+m}$. De fato, se $(x_i, a), (x_{i'}, a') \in T_j$, com $0 \leqslant j \leqslant k$, então

$$(x_i, a)\chi = (x_0, a)\chi = (a)\chi^{**} = (a')\chi^{**} = (x_0, a')\chi = (x_{i'}, a')\chi.$$

Logo T é um subespaço $(k+1)$-dimensional por camadas, em relação a χ, em $C_{t+1}^{m'+m}$, o que completa a indução. □

Teorema A.11. *Seja χ uma r-coloração de C_{t+1}^{n}. Se existe um subespaço k-dimensional por camadas C de C_{t+1}^{n}, com $0 \leqslant k \leqslant n$, tal que $(C)\chi \subseteq \{i_1, ..., i_k\} \subseteq \{1, ..., r\}$, então existe uma linha monocromática, com relação a χ, em C.*

Demonstração. Em virtude da Observação A.4, é suficiente mostrar para C_{t+1}^{k}. Considere os $(k+1)$ elementos da forma $x_i = (x_{i1}, ..., x_{ik})$, com $x_{ij} = 0$, se $j \leqslant i$ e $x_{ij} = t$, se $j > i$, com $0 \leqslant i \leqslant k$. Uma vez que $|(C_{t+1}^{k})\chi| \leqslant k$, pelo *Princípio da Casa dos Pombos*, existem $m < n$ tais que x_m e x_n possuem a mesma cor . A linha $\{y_0, ..., y_t\}$ de C_{t+1}^{k} dada por $y_l = (y_{l1}, ..., y_{lk})$, com $y_{li} = 0$, se $i \leqslant m$, $y_{li} = l$, se $m < i \leqslant n$ e $y_{li} = t$, se $n < i$, com $l = 0, ..., t$, é tal que $y_t = x_m$ e $y_0 = x_n$. Note que $\{y_0, ..., y_{t-1}\} \subseteq C_{n-m}$ e, como C_{t+1}^{k} é por camadas e y_t tem a mesma cor de y_0, a linha $\{y_0, ..., y_t\}$ é monocromática em relação a χ, como desejado. □

Corolário A.12. *Suponha que dados inteiros positivos r, s e t exista $M' = M'(r, t, k)$ tal que para todo $M \geqslant M'$ e toda r-coloração de C_{t+1}^{M}, existe um subespaço k-dimensional por camadas de C_{t+1}^{M}. Então, existe $N' = N'(r, t+1)$ tal que, para todo $N \geqslant N'$, se C_{t+1}^{N} é r-colorido, existe uma linha monocromática em C_{t+1}^{N}.*

Demonstração. Escolha $k = r$, assim, por hipótese, existe $M' = M'(r,t,r)$ tal que para todo $M \geqslant M'$, se C_{t+1}^M é r-colorido, então C_{t+1}^M contém um subespaço r-dimensional por camadas. Pelo teorema anterior, C_{t+1}^M possui uma linha monocromática. Tome $N'(r,t+1) = M'(r,t,r)$ e o resultado segue. $\square$

Agora, a demonstração do teorema principal.

Demonstração. **(Teorema de Hales-Jewet)** A demonstração será feita por indução sobre t. Se $t = 1$, a afirmação é óbvia. Já para o caso em que $t = 2$, coloque $H(2,r) = N$ e considere os $N+1$ pontos

$$(0,0,...,0),(1,0,...,0),...,(1,1,...,1,0),(1,1,...,1)$$

de C_2^N. Como $N+1 > r$, pelo Princípio da Casa dos Pombos, dois desses pontos possuem a mesma cor, mas quaisquer dois desses pontos formam uma linha em C_2^N. Agora, se $k \geqslant 2$ a indução fica completa pelo Teorema A.10 e pelo Corolário A.12. $\square$

1.2 Alguns Fatos sobre Corpos Infinitos

Nesta seção são enunciados e demonstrados dois resultados sobre corpos infinitos. Se K é um corpo, são usados os símbolos K^+ e $K^\times$ para o grupo aditivo $(K,+)$ e o grupo multiplicativo $(K \setminus \{0\}, \times)$, respectivamente. O resultado a seguir é bem conhecido e será admitido sem demonstração (para uma demonstração detalhada confira [3]).

Teorema A.13. *([3], página 65) Sejam K um corpo e $p(x)$ um polinômio não nulo de grau n com coeficientes em K. Então $p(x)$ possui no máximo n raízes em K.*

A primeira proposição, em verdade uma consequência imediata do teorema anterior, é dada a seguir.

Proposição A.14. *([6]) Um subgrupo infinito do grupo multiplicativo de um corpo não pode ter expoente finito.*

Demonstração. Sejam K um corpo e um subgrupo infinito T de $K^{\times}$. Suponha que o expoente de T é finito, isto é, existe inteiro positivo n tal que $t^n = 1$ para todo t em T. Assim, a equação $t^n - 1 = 0$ admite infinitas soluções no corpo K, o que contradiz o Teorema A.13. Portanto, T não possui expoente finito. $\square$

Os dois próximos lemas serão usados para demonstrar o último fato relevante dessa seção.

Lema A.15. *([17]) Se R é um anel com divisão infinito e n um inteiro positivo, então existem $c_1, ..., c_n \in R$ tais que, para todo subconjunto não vazio J de $\{1, ..., n\}$, tem-se $\sum_{j\in J} c_j \neq 0$.*

Demonstração. A demonstração será feita por indução sobre n. Se $n = 1$ a afirmação é óbvia, pois $R \setminus \{0\}$ é infinito. Suponha que a afirmação é verdadeira para $n \geqslant 1$. Sejam, assim, $c_1, ..., c_n \in R$ tais que para todo subconjunto não vazio J de $\{1, ..., n\}$ tem-se $\sum_{j\in J} c_j \neq 0$. Suponha, por absurdo, que para todo $c_{n+1} \in R$ exista um subconjunto não vazio J' de $\{1, ..., n+1\}$ tal que $\sum_{j\in J'} c_j = 0$. Deve-se ter $n+1 \in J'$, assim, $c_{n+1} = \sum_{j\in J'\setminus\{n+1\}}(-c_j)$, isto é, para todo $c_{n+1} \in R$ existe $\emptyset \neq J'\setminus\{n+1\} \subset \{1, ..., n\}$ tal que $c_{n+1} = \sum_{j\in J'\setminus\{n+1\}}(-c_j)$. Mas, o conjunto das partes do conjunto $\{1, ..., n\}$ é finito, logo o próprio R é finito, absurdo. Segue o resultado. $\square$

Lema A.16. *([17]) Sejam R um anel com divisão infinito e S um subgrupo de $(R \setminus \{0\}, \times)$ de índice finito n. Então, para elementos arbitrários $x_1, ..., x_m \in R \setminus \{0\}$ existe $c \in R \setminus \{0\}$ tal que $1 + cx_s \in S$, para todo $s \in \{1, ..., m\}$.*

Demonstração. Sejam $r_1, ..., r_n \in R$ tais que $R = \biguplus_{i=1}^{n} Sr_i$. Considere $N = H(n+1, m+1)$ como no Teorema A.9 e o N-cubo C^N_{m+1}. Sejam $c_1, ..., c_N \in R$ tais que para todo subconjunto não vazio J de $\{1, ..., N\}$ tem-se $\sum_{j\in J} c_j \neq 0$, que existem em virtude do Lema A.15. Seja $x_0 = 0$ e defina uma $(n+1)$-coloração f de C^N_{m+1} colocando, para todo $(i_1, ..., i_N) \in C^N_{m+1}$

$$(i_1, ..., i_N)f = \begin{cases} l, \; se \; S(\sum_{j=1}^{N} c_j x_{i_j}) = Sr_l \\ 0, \quad se \quad \sum_{j=1}^{N} c_j x_{i_j} = 0. \end{cases}$$

Pelo Teorema A.9, existe uma linha $L = \{y_0, ..., y_m\}$ monocromática em relação a f. Logo, para algum $l' \in \{0, 1, ..., n\}$ tem-se que $(y_s)f = l'$, para todo $s \in \{0, ..., m\}$. Escrevendo

$y_s = (y_{s0}, ..., y_{sN})$, para cada $s \in \{0, ..., m\}$, pela Observação A.4, existem L_0, $L_1 \subseteq \{1, ..., N\}$ com $L_0 \cap L_1 = \emptyset$, $L_0 \cup L_1 = \{1, ..., N\}$, $L_1 \neq \emptyset$ e tais que a linha L pode ser escrita na forma

$$L = \{y_s = (s, ..., s, a_1, s, ..., s, a_k, s, ..., s, a_{|J_0|}, s, ..., s) \in C_{m+1}^N; s = 0, ..., m\},$$

com $a_k \in L_0$, para todo $k = 1, ..., |L_0|$ e $a_1 < ... < a_{|L_0|}$. De $(y_s)f = l$, para todo s, obtém-se

$$S(\sum_{j=1}^{N} c_j x_{y_{sj}}) = S(\sum_{j \in L_0} c_j x_{y_{sj}} + \sum_{j \in L_1} c_j x_{y_{sj}}) = S(\sum_{j \in L_0} c_j x_{a_j} + x_s \sum_{j \in L_1} c_j) = Sr_l,$$

para todo $y_s \in L$. Observe que $L_0 \neq \emptyset$, pois, caso contrário $x_s = 0$ para todo $s \in \{0, ..., m\}$, absurdo. Tomando $a = \sum_{j \in L_0} c_j x_{a_j}$ e $b = \sum_{j \in L_1} c_j$, segue, em particular, que para cada $s \in \{1, ..., m\}$ tem-se $Sa = S(a + bx_s)$, em virtude de $(y_0)f = (y_s)f$, para todo $s \in \{1, ..., m\}$. Note que $b \neq 0$, pela escolha dos c_i's e, assim, $a \neq 0$, pois, caso contrário, $\{0\} = Sbx_s \neq \{0\}$, absurdo. Daí, $1 + (a^{-1}b)x_s \in S$, para todo $s \in \{1, ..., m\}$. Pondo $c = a^{-1}b$ o resultado segue. □

Já foi visto que se T é um subgrupo do grupo multiplicativo $K^\times$ de um corpo K, então T induz um grupo $\mathcal{T}$ de automorfismo de K^+. Em verdade, $\mathcal{T}$ é, naturalmente, isomorfo a T. Por esse motivo, o subgrupo T é identificado com o grupo $\mathcal{T}$, assim, por vezes os elementos de T são vistos como automorfismos de K^+. Agora a terceira e última proposição desta seção.

Proposição A.17. *([6]) Sejam K um corpo infinito e T um subgrupo de $K^\times$ com índice finito n. Então, existem uma infinidade de pares $(\alpha, \beta) \in T \times T$ tais que $\beta = 1 + \alpha$.*

Demonstração. Suponha, por absurdo, que existam uma quantidade finita m de pares $(\alpha, \beta) \in T \times T$ tais que $\beta = 1 + \alpha$. Seja $\{k_1, ..., k_n\} \subseteq K^\times$ um transversal à direita de T em $K^\times$. Escolha elementos distintos $x_1, ..., x_{m+1}$ de T. Pelo Lema A.16, existe um elemento $c \in K^\times$ tal que $1 + cx_ik_j \in T$, para cada $i \in \{1, ..., m+1\}$ e cada $j \in \{1, ..., n\}$. Como a multiplicação de c permuta as classes laterais de T em $K^\times$, existe um índice apropriado j tal que $ck_j \in T$. Defina $d = ck_j$, $\alpha_i = dx_i$ e $\beta_i = 1 + \alpha_i$ e, assim, (α_i, β_i) são $m + 1$ pares em $T \times T$ com $\beta_i = 1 + \alpha_i$, contradizendo a quantidade máxima m de pares desta forma. Portanto, segue o resultado. □

Referências

[1] BURNSIDE, W., Theory of Groups of Finite Order, segunda edição, Cambridge University Press, Cambridge, (1911).

[2] DAVEY, B. A., PRIESLEY, H. A., Introduction to Lattices and Order, segunda edição, Cambridge University Press, Cambridge, (2002).

[3] GARCIA, A., LEQUAIN, Y., Elementos de álgebra, quarta edição, Projeto Euclides, Rio de Janeiro, (2006).

[4] GORENSTEIN, D., Finite Groups, segunda edição, Chelsea Publishing Company, Nova York, (1980).

[5] GRAHAM, R. L., ROTHSCHILD, B. L., SPENCER, J. H., Ramsey theory, second edition, John Wiley e Sons, New York, (1989).

[6] JABARA, E., Abelian automorphisms groups with a finite number of orbits, J. Algebra, **323**, (2010), 2798 - 2817.

[7] JABARA, E., Actions of abelian groups in groups, J. Group Theory, **10 (2)**, (2007), 185 - 194.

[8] JABARA, E., Sugli automorfismi uniformi e privi di coincidenze dei gruppi infiniti, B. Unione Mat. Ital., **10 (B)**, (2007), 501 - 510.

[9] NEUMANN, B. H., Groups covered by permutable subsets, J. London Mathematical Society, **1 - 29 (2)**, (1954), 236-284.

[10] NEUMANN, B. H., Groups with automorphisms that leave only neutral element fixed. Archiv der Math, **7**, (1956), 1-5.

[11] NEUMANN, B. H., Groups with finite classes de conjugate elements. Proc. Lond. Math., **1**, (1951), 178-187.

[12] NEUMANN, P. M., ROWLEY, P. J., Free actions of abelian groups in groups, Geometry and Cohomology in Groups Theory, **252**, (1998), 291 - 295.

[13] PETTET, M., Free actions of virtually FC-groups, Arch. Math., **86**, (2006), 23-30.

[14] ROBINSON, D. J. S., A Course in the theory of groups, second edition, Springer, New York, 1991.

[15] ROSE, J. S., A Course on group theory, Cambridge University Press, Cambridge, 1978.

[16] THOMPSON, J. G., Finite groups with fixed-point-free automorphisms of prime order, Proc. Nat. Acad. Sci., **45**, (1959), 578-581.

[17] TURNWALD, G., Multiplicative subgroups of finite index in a division ring, Proc. Amer. Math., **120 (2)**, (1994), 377-381.

[18] ZAPPA, G., Sugli automorfismi uniformi nei gruppi di Hirshi, Ric. Math., **7**, (1958), 3-13.

Índice