Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Grupos metabelianos com os mesmos quocientes finitos

por

Felipe Batista da Silva

Brasília
2010

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Grupos metabelianos com os mesmos quocientes finitos

por

Felipe Batista da Silva*

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 26 de novembro de 2010.

Comissão Examinadora:

Profa. Dra. Aline G. S. Pinto - UnB (Orientadora)

Prof. Dr. Pavel A. Zalesskii - UnB (Membro)

Profa. Dra. Ana Cristina Vieira - UFMG (Membro)

*O autor foi bolsista do CNPq durante a elaboração deste trabalho.

A meus pais e avós !

AGRADECIMENTOS

Como em toda conquista obtida, agradeço primeiro a Deus.

Agradeço a meus pais, por todo apoio e amor dados durante toda minha vida.

À minha irmã Kelly e a todos meus familiares.

À minha orientadora, Aline Gomes da Silva Pinto, por me auxiliar com muita paciência e dedicação, e por todos ensinamentos durante o período de orientação.

A todos meus amigos, não citarei todos, mas agradeço a todos, em particular a meus amigos de graduação, João Marcelo, Marcos Mesquita, e/ou de pós-graduação, João Vítor, Henrique Zanata, Thiago Willians, Vinícius Facó, Igor Lima, Laura Cristina, Robson Nascimento, Adriana Bastos, os quais dentre outros participaram indireta ou diretamente comigo no processo de estudos para as disciplinas e/ou exames de qualificação de Mestrado, além de outros auxílios.

Aos professores do Departamento de Matemática, por possibilitarem o aumento de cultura e conhecimento. Em particular, agradeço a Aline Pinto, Hemar Godinho, Noraí Rocco, Rudolf Meier, Ana Gandulfo, Liliane Maia pelo apoio ao ingresso no programa de Mestrado.

Aos professores Ana Cristina e Pavel Zalesskii por integrarem à Banca Examinadora, e por todas sugestões e correções fornecidas.

À Tânia, Eveline, Manoel, Isabel por todo apoio técnico, o qual sempre foi desempenhado com eficiência.

Ao CNPq, pelo apoio financeiro durante todo programa de Mestrado.

RESUMO

Nesta dissertação, com base em [1], construímos uma quantidade infinita de grupos $G_M = M \rtimes A$ metabelianos finitamente apresentados não-isomorfos com os mesmos quocientes finitos, para tal utilizamos ferramentas da Teoria de Módulos. Outrossim, discutimos com base em [3] que, grupos metabelianos finitamente gerados satisfazem a condição maximal para subgrupos normais, denotada por max$-n$. Também apresentamos um exemplo dado por Baumslag, em [2], de um grupo finitamente apresentado que é metabeliano, e portanto satisfaz max$-n$. Tal grupo será útil na demonstração de que os grupos $G_M = M \rtimes A$ são finitamente apresentados.

ABSTRACT

In this work, based on [1], we construct infinitely many nonisomorphic finitely presented metabelian groups $G_M = M \rtimes A$ with the same finite quotients, for this goal we use Module Theory's tools. Futhermore, we discuss based on [3], that finitely generated metabelian groups satisfy the maximal condition on normal subgroups, denoted by $\max{-}n$. Besides we present an example given by Baumslag in [2] of a finitely presented group which is metabelian, hence holds $\max{-}n$, this group will be useful when we prove that the groups $G_M = M \rtimes A$ are finitely presented.

SUMÁRIO

INTRODUÇÃO

O objetivo central deste trabalho é mostrar que é possível obter uma quantidade infinita de grupos metabelianos não-isomorfos, mas que têm os mesmos quocientes finitos. Muitos exemplos de grupos não-isomorfos com os mesmos quocientes finitos já foram dados, como em [8], [9], [11], [12]. No entanto, em tais exemplos, há apenas uma quantidade finita de grupos não-isomorfos com os mesmos quocientes finitos, e além disso todos grupos nesses exemplos são policíclicos.

Encontramos certas condições que possibilitam fornecer uma quantidade infinita de grupos não-isomorfos com os mesmos quocientes finitos, para tal nos direcionamos aos grupos metabelianos, e escolhemos um anel noetheriano comutativo conveniente, o qual possibilitará definir grupos nas condições desejadas.

Este trabalho é dividido em três capítulos, no primeiro, são apresentados resultados preliminares, os quais são utilizados nos capítulos posteriores. No Capítulo 2, apresentamos definições e resultados acerca de Módulos, e mostramos que o conjunto formado pelas classes de isomorfismos de R-módulos projetivos de posto 1, munido com uma operação induzida pelo produto tensorial, forma um grupo abeliano, chamado Grupo de Picard de R. No Capítulo 3, primeiramente mostramos com base no artigo de Hall [3] que, grupos metabelianos finitamente gerados satisfazem a condição maximal sobre subgrupos normais, mais geralmente mostramos o teorema:

Teorema 3.2.10. *Um grupo finitamente gerado G que é uma extensão de um grupo abeliano por um grupo policíclico satisfaz a condição maximal sobre subgrupos normais.*

Posteriormente, com base no artigo de Pickel [1], mostramos o seguinte teorema principal:

Teorema 3.4.14. *Existe uma quantidade infinita de grupos metabelianos finitamente apresentados não-isomorfos com os mesmos quocientes finitos.*

Denotamos por $F(G)$, o conjunto das classes de isomorfismos de quocientes finitos do grupo G. Estendemos essa definição para módulos sobre um anel R comutativo com 1, isto é, denotamos por $F_R(M)$, como o conjunto das classes de R-isomorfismos de quocientes finitos de M. No Teorema 3.4.2 damos um critério que estabelece quando dois R-módulos M e N têm os mesmos quocientes finitos isomorfos como R-módulos, QFI_R:

Teorema 3.4.2. *Sejam R um anel noetheriano comutativo com 1, M e N, R-módulos finitamente gerados . Então M e N têm QFI_R se, e somente se, $M/\mathfrak{p}^k M$ é isomorfo a $N/\mathfrak{p}^k N$ para todo $k \in \mathbb{N}$ e para todos ideais maximais $\mathfrak{p}$ de índice finito em R.*

Depois mostramos que se A é um subgrupo das unidades do anel R que o gera como anel, então temos o seguinte resultado:

Lema 3.4.3. Sejam A um subgrupo do grupo das unidades $U(R)$ de R que gera R como um anel, considere que M e N sejam R-módulos finitamente gerados com QFI_R. Então, os grupos $G_M = M \rtimes A$ e $G_N = N \rtimes A$ têm os mesmos quocientes finitos.

Em particular, vamos nos restringir ao anel $R = \mathbb{Z}G[x, x^{-1}, (x+1)^{-1}]$, em que G é um grupo abeliano finito, cuja ordem não é livre de quadrados, esta condição sobre a ordem de G é necessária para garantir que o Grupo de Picard de R, $Pic(R)$, é infinito. Na Proposição 3.4.4, mostramos que quaisquer R-módulos projetivos de posto 1 têm QFI_R, de modo que se M e N são R-módulos projetivos de posto 1, então $G_M \cong G_N$, pelo Lema 3.4.3. Outrossim, mostramos na Proposição 3.4.8 que existem infinitos grupos G_M não isomorfos com os mesmos quocientes finitos e, por fim, na Proposição 3.4.13, mostramos que tais grupos G_M são finitamente apresentados, obtendo assim o teorema principal.

CAPÍTULO 1

PRELIMINARES

Neste capítulo, apresentaremos definições e resultados utilizados com frequência nos capítulos posteriores. Alguns resultados são clássicos, mas a fim de esclarecer notações e deixar as referências a esses claras, optamos por não omiti-los.

1.1 Anéis e Ideais

Por conveniência, apresentaremos a definição de anel.

Definição 1.1.1. *Um conjunto não-vazio R, com duas operações binárias adição "+" e multiplicação ".", é um anel quando são satisfeitas as seguintes propriedades:*

R_1. *$(R, +)$ é um grupo abeliano;*

R_2. *se $a, b, c \in R$, então $a(bc) = (ab)c$; e*

R_3. *se $a, b, c \in R$, então $a(b + c) = ab + ac$ e $(b + c)a = ba + ca$.*

Se além disso, R tem a propriedade

R_4. *se $a, b \in R$, então $ab = ba$;*

então R é chamado um anel comutativo, e se existe um elemento $1 \in R$ tal que $a.1 = 1.a = a, \forall a \in R$, dizemos que R é um anel comutativo com elemento identidade.

Observação: Nesta dissertação, todos os anéis serão comutativos com 1, exceto quando expresso o contrário. Embora, repetimos as condições de o anel ser comutativo ou de possuir 1, quando tais informações são essenciais na demonstração de um resultado. Deste modo, ao se dizer *anel*, *anel comutativo* ou *anel com 1*, subtende-se anel comutativo com 1.

Definição 1.1.2. *Um elemento x de um anel R é chamado um divisor de zero em R, quando existe $y \neq 0 \in R$, tal que $xy = 0$.*

Observação 1.1.3. *Pela Definição 1.1.2, segue que, se $R \neq \{0\}$, então 0 sempre é um divisor de zero. No caso de $R = \{0\}$, convencionemos que 0 seja ainda um divisor de zero.*

Definição 1.1.4. *Um subconjunto não-vazio I de um anel R é um ideal de R, quando I é um subgrupo de $(R, +)$, e $RI \subseteq I$.*

Exemplo 1.1.5. *Os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z}$, em que $n \in \mathbb{Z}$.*

Proposição 1.1.6. *Sejam R um anel comutativo não necessariamente com 1, e $a \in R$, então o menor ideal contendo a, denotado por (a), é formado pelo conjunto de todos elementos de R da forma $ra + na$, em que $r \in R$, e $n \in \mathbb{Z}$. No caso de $1 \in R$, temos que (a) coincide com o ideal principal gerado por a, ou seja, $(a) = Ra$.*

Demonstração: Defina $I = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$, temos que I é um ideal de R, uma vez que se $x = r_1a + n_1a$ e $y = r_2a + n_2a$ pertencem a I, então $x - y = (r_1 - r_2)a + (n_1 - n_2)a$ pertence a I, outrossim se $r \in R$, então $rx = r(r_1a + n_1a) = r(r_1a) + r(n_1a) = (rr_1)a + (rn_1)a = (rr_1 + rn_1)a = (rr_1 + rn_1)a + 0.a \in I$. Agora, seja J um ideal de R contendo a, então $na \in J$, para todo $n \in \mathbb{Z}$, mas como J é um ideal, $ra \in J$ para todo $r \in R$, logo $ra + na \in J$ para todo $r \in R$ e para todo $n \in \mathbb{Z}$, daí $I \subseteq J$. Portanto, I o qual denotamos por (a), é o menor ideal de R contendo a. No caso de $1 \in R$, segue que Ra é o menor ideal de R contendo a, pois $a = 1a \in Ra$, e se J é um ideal de R contendo a, segue pela definição de ideal que, $ra \in J$ para todo $r \in R$, logo $Ra = (a)$.

■

Definição 1.1.7. *Seja R um anel com 1, dizemos que $x \in R$ é uma unidade em R, quando existe $y \in R$ tal que $xy = 1$.*

Proposição 1.1.8. *Um elemento x de um anel R com 1 é uma unidade se, e somente se, o ideal principal gerado por x coincide com R.*

Demonstração: Se $x \in R$ é uma unidade, então existe $y \in R$ tal que $yx = 1$, de modo que, se $r \in R$, então $r = r1 = (ry)x \in Rx$, daí $Rx = R$. Reciprocamente, se $Rx = R$, então como $1 \in R$, segue que $1 \in Rx$, logo existe $y \in R$, tal que $yx = 1$, portanto x é uma unidade em R.

Definição 1.1.9. *Um elemento $x \in R$ é chamado nilpotente, quando $x^n = 0$ para algum $n > 0$.*

Proposição 1.1.10. *Se R é um anel não-nulo, então cada elemento nilpotente é um divisor de zero.*

Demonstração: Seja x um elemento nilpotente de R, então existe um inteiro $n > 0$ tal que $x^n = 0$, se $x = 0$, então x é um divisor de zero, suponha portanto $x \neq 0$, daí $n > 1$, e $xx^{n-1} = 0$, se x^{n-1} for não-nulo, então segue que x é um divisor de zero, caso contrário, temos que $x^{n-1} = 0$ com $n > 2$, pois $x \neq 0$. Logo $xx^{n-2} = 0$, assim se $x^{n-2} \neq 0$, segue que x é um divisor de zero, caso contrário temos $x^{n-2} = 0$ e $n > 3$, continuando com esse processo, segue que deve existir um inteiro positivo $k < n$, tal que $xx^{n-k} = 0$ com $x^{n-k} \neq 0$, pois caso contrário, teríamos no decorrer deste processo $x = x^{n-(n-1)} = 0$, que é uma contradição, logo existe $x^{n-k} \neq 0$ tal que $xx^{n-k} = 0$, portanto x é um divisor de zero.

■

Definição 1.1.11. *Um ideal $\mathfrak{m}$ de um anel R é chamado ideal maximal, quando $\mathfrak{m} \neq R$, e sempre que I é um ideal de R tal que $\mathfrak{m} \subseteq I \subseteq R$, tem-se $I = \mathfrak{m}$ ou $I = R$.*

Exemplo 1.1.12. *Os ideais maximais de $\mathbb{Z}$ são os ideais principais gerados por um número primo.*

Definição 1.1.13. *Um subconjunto C de um conjunto parcialmente ordenado S é uma cadeia, quando $x \leq y$ ou $y \leq x$ para cada par de elementos $x, y \in C$.*

Lema 1.1.14 (Zorn)**.** *Se cada cadeia C de um conjunto parcialmente ordenado S tem uma cota superior em S, então S tem ao menos um elemento maximal.*

Proposição 1.1.15. *Cada anel comutativo com 1, $R \neq (0)$ tem ao menos um ideal maximal.(No caso de $1 = 0$, temos que R é o anel nulo)*

Demonstração: Seja Σ o conjunto de todos ideais diferentes de R em R. Temos que $\Sigma \neq \emptyset$, pois o ideal (0) pertence a Σ. Ordene Σ pela inclusão. Seja $C = (\mathfrak{a}_\alpha)$ uma cadeia em Σ, assim podemos afirmar que $\bigcup_\alpha \mathfrak{a}_\alpha$ é um limitante superior de C em Σ. Com efeito, temos que $\bigcup_\alpha \mathfrak{a}_\alpha \neq R$, pois $1 \notin \mathfrak{a}_\alpha$, para todo α, daí $\mathfrak{a}_\alpha \neq R, \forall \alpha$, além disso $\bigcup_\alpha \mathfrak{a}_\alpha$ é um ideal de R, uma vez que, se $x, y \in \bigcup_\alpha \mathfrak{a}_\alpha$, então existem índices β e γ, tais que $\mathfrak{a}_\beta, \mathfrak{a}_\gamma \in \bigcup_\alpha \mathfrak{a}_\alpha$ com $x \in \mathfrak{a}_\beta$, e $y \in \mathfrak{a}_\gamma$, mas como C é uma cadeia, segue que $\mathfrak{a}_\beta \subseteq \mathfrak{a}_\gamma$ ou $\mathfrak{a}_\gamma \subseteq \mathfrak{a}_\beta$, de modo que $x \pm y \in \mathfrak{a}_\beta$ ou $x \pm y \in \mathfrak{a}_\gamma$, daí $x - y \in \bigcup_\alpha \mathfrak{a}_\alpha$. Outrossim, se $r \in R$, e $x \in \bigcup_\alpha \mathfrak{a}_\alpha$, então $x \in \mathfrak{a}_\alpha$ para algum índice α, mas como $\mathfrak{a}_\alpha$ é um ideal, segue que $rx \in \mathfrak{a}_\alpha$, daí $rx \in \bigcup_\alpha \mathfrak{a}_\alpha$. Logo $\bigcup_\alpha \mathfrak{a}_\alpha$ é um ideal, e é diferente de R. Portanto, $\bigcup_\alpha \mathfrak{a}_\alpha \in \Sigma$, e como temos que para todo $\mathfrak{a}_\beta \in C$, $\mathfrak{a}_\beta \preceq \bigcup_\alpha \mathfrak{a}_\alpha$, pois $\mathfrak{a}_\beta \subseteq \bigcup_\alpha \mathfrak{a}_\alpha$, segue que toda cadeia em Σ tem um limitante superior em Σ. Logo pelo Lema de Zorn, Σ tem um elemento maximal em R, daí R tem um ideal maximal.

■

Corolário 1.1.16. *Se $I \neq (1)$ é um ideal de R, então existe um ideal maximal de R contendo I.*

Demonstração: Considere o anel quociente R/I, o qual é comutativo com $\bar{1}$, logo pela Proposição 1.1.15, segue que R/I possui um ideal maximal $\mathfrak{m}/I$. Considere o homomorfismo canônico

$$\varphi : R \longrightarrow R/I,$$

temos pelo Teorema da Correspondência que, $\mathfrak{m}$ é o único ideal de R contendo I, tal que $\varphi(\mathfrak{m}) = \mathfrak{m}/I$. Mostremos que $\mathfrak{m}$ é um ideal maximal em R. De fato, suponha que $\mathfrak{m} \lneq J \leq R$, então $\mathfrak{m}/I \lneq J/I \leq R/I$, mas como $\mathfrak{m}/I$ é maximal, segue que $J/I = R/I$, logo pelo Teorema da Correspondência, temos que $J = R$, portanto $\mathfrak{m}$ é maximal em R.

■

Corolário 1.1.17. *Cada elemento de R que não é uma unidade está contido em um ideal maximal de R.*

Demonstração: Seja $x \in R$ uma não-unidade de R, então pela Proposição 1.1.8, $(x) \neq R$, logo pelo Corolário 1.1.16, R tem um ideal maximal $\mathfrak{a}$ contendo (x), logo x é um elemento do ideal maximal $\mathfrak{a}$ de R.

■

Proposição 1.1.18. *Seja R um anel comutativo com 1. Então $\mathfrak{m}$ é um ideal maximal de R se, e somente se, o anel quociente $R/\mathfrak{m}$ é um corpo.*

Demonstração:
($\Rightarrow$) Seja $r+\mathfrak{m}$ um elemento não-nulo em $R/\mathfrak{m}$, daí $r \notin \mathfrak{m}$. Considere o ideal $I = (r)+\mathfrak{m}$, note que I contém $\mathfrak{m}$ propriamente, mas como $\mathfrak{m}$ é um ideal maximal em R, segue que $I = R$, no entanto $1 \in R$, logo existem $rx \in (r)$, e $y \in \mathfrak{m}$, tais que $rx+y = 1$. Portanto $rx+y+\mathfrak{m} = 1+\mathfrak{m}$, mas $y+\mathfrak{m} = \mathfrak{m}$, pois $y \in \mathfrak{m}$. Logo $rx+\mathfrak{m} = 1+\mathfrak{m}$, daí $(r+\mathfrak{m})(x+\mathfrak{m}) = 1+\mathfrak{m} = \overline{1}$, deste modo $r+\mathfrak{m}$ é uma unidade em $R/\mathfrak{m}$, logo $R/\mathfrak{m}$ é um corpo.
($\Leftarrow$) Suponha que $R/\mathfrak{m}$ seja um corpo. Considere que I seja um ideal de R, tal que $\mathfrak{m} \lneq I \leq R$. Deste modo existe $x \in I$, tal que $x \notin \mathfrak{m}$, então $x+\mathfrak{m}$ não é nulo no corpo $R/\mathfrak{m}$, portanto é uma unidade. Logo existe $y+\mathfrak{m} \in R/\mathfrak{m}$, tal que $xy+\mathfrak{m} = 1+\mathfrak{m}$, de modo que $xy-1 \in \mathfrak{m}$. Assim existe $z \in \mathfrak{m}$, tal que $xy-1 = z$, daí $xy-z = 1$, mas como $xy \in I$, já que x pertence ao ideal I, e $z \in I$, pois $\mathfrak{m} \subset I$. Segue que $xy-z = 1 \in I$, logo $I = R$, e daí $\mathfrak{m}$ é um ideal maximal em R.

■

Definição 1.1.19. *Um anel R com exatamente um ideal maximal $\mathfrak{m}$ é chamado um anel local. E o corpo $R/\mathfrak{m}$ é chamado de corpo resíduo de R.*

Proposição 1.1.20. *i) Sejam R um anel comutativo com 1, e $\mathfrak{m} \neq R$ um ideal de R tal que cada $x \in R-\mathfrak{m}$ seja uma unidade em R. Então R é um anel local e $\mathfrak{m}$ é seu ideal maximal.*

ii) Sejam R um anel comutativo com 1, e $\mathfrak{m}$ um ideal maximal de R tal que cada elemento de $1+\mathfrak{m}$ seja uma unidade em R. Então, R é um anel local.

Demonstração:

(i) Por hipótese, temos que cada elemento de $R-\mathfrak{m}$ é uma unidade em R. Equivalentemente, se $x \in R$ não é uma unidade, então $x \in \mathfrak{m}$. Deste modo se $\mathfrak{q}$ é um ideal maximal em R, então $\mathfrak{q} \subseteq \mathfrak{m}$, uma vez que pela Proposição 1.1.8, $\mathfrak{q} \neq R$ não contém unidades, mas como $\mathfrak{m} \neq R$, e $\mathfrak{q}$ é maximal, segue que $\mathfrak{q} = \mathfrak{m}$. Portanto $\mathfrak{m}$ é um ideal maximal e é o único. Logo R é um anel local.

(ii) Seja $x \in R-\mathfrak{m}$, assim o ideal $\mathfrak{q}$ gerado por x e $\mathfrak{m}$, coincide com R, pois o ideal $\mathfrak{q}$ contém propriamente o ideal maximal $\mathfrak{m}$. Agora, como $1 \in \mathfrak{q}$, segue que existem $y \in R$

e $z \in \mathfrak{m}$, tais que $xy + z = 1$. Daí $xy = 1 - z \in 1 + \mathfrak{m}$, logo por hipótese segue que xy é uma unidade, daí x é uma unidade. Então por (i), segue que R é um anel local.

■

Definição 1.1.21. *Um domínio de integridade no qual cada ideal é principal é chamado de domínio de ideais principais.*

Definição 1.1.22. *Um ideal $\mathfrak{p}$ de um anel R é chamado primo, quando $\mathfrak{p} \neq R$, e sempre que $xy \in \mathfrak{p}$, tem se $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$.*

Proposição 1.1.23. *Seja R um anel comutativo com 1. Então $\mathfrak{p}$ é um ideal primo de R se, e somente se, $R/\mathfrak{p}$ é um domínio de integridade.*

Demonstração:
($\Rightarrow$) Suponha que $(x+\mathfrak{p})(y+\mathfrak{p}) = \mathfrak{p} = \bar{0}$ em $R/\mathfrak{p}$, daí $xy \in \mathfrak{p}$, deste modo se $\mathfrak{p}$ é primo, segue que $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$, de modo que $x + \mathfrak{p}$ ou $y + \mathfrak{p}$ é nulo em $R/\mathfrak{p}$. Logo $R/\mathfrak{p}$ é um domínio de integridade.
($\Leftarrow$) Seja $xy \in \mathfrak{p}$, então $(x+\mathfrak{p})(y+\mathfrak{p}) = \mathfrak{p} = \bar{0}$, mas como $R/\mathfrak{p}$ é um dominio de integridade, segue que $x + \mathfrak{p} = \mathfrak{p}$ ou $y + \mathfrak{p} = \mathfrak{p}$, daí $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Logo $\mathfrak{p}$ é um ideal primo.

■

Proposição 1.1.24. *Cada ideal maximal de um anel R comutativo com 1 é também um ideal primo.*

Demonstração: De fato, se $\mathfrak{m}$ é um ideal maximal em R, então $R/\mathfrak{m}$ é um corpo, com mais razão é um domínio de integridade, daí pela Proposição 1.1.23, segue que $\mathfrak{m}$ é um ideal primo.

■

Proposição 1.1.25. *Em um domínio de ideais principais, cada ideal primo não-nulo é maximal.*

Demonstração: Seja $\mathfrak{p}$ um ideal primo não-nulo em um domínio de ideais principais R, logo existe $x \in R$, tal que $\mathfrak{p} = (x)$. Seja (y) um ideal de R, tal que $(x) \subsetneq (y) \subseteq R$, deste modo $x \in (y)$, daí existe $z \in R$, tal que $x = yz$, logo $yz \in (x)$. No entanto $\mathfrak{p} = (x)$ é um

ideal primo, e $y \notin (x)$, pois $(x) \subsetneq (y)$, logo $z \in (x)$, portanto existe $t \in R$, tal que $z = tx$. Daí $x = yz = y(tx) = (yt)x$, logo $x = (yt)x$, mas como R é um domínio e $x \neq 0$, segue que $yt = 1$, assim y é uma unidade. Consequentemente $(y) = R$. Portanto, $\mathfrak{p} = (x)$ é um ideal maximal.

■

Proposição 1.1.26. *O conjunto $\mathfrak{N}$ de todos elementos nilpotentes em um anel R é um ideal, chamado nilradical de R. E o anel $R/\mathfrak{N}$ não tem elementos nilpotentes não-nulos.*

Demonstração: Sejam $x, y \in \mathfrak{N}$, então existem $m, n > 0$, tais que $x^m = y^n = 0$, mas como R é comutativo, vale o Teorema Binomial, daí $(x+y)^{m+n-1}$ é uma soma de múltiplos de produtos da forma $x^r y^s$, em que $r + s = m + n - 1$. No entanto não pode ocorrer, simultaneamente, $r < m$ e $s < n$, pois caso contrário, teríamos que $r+s \leq (m-1)+(n-1) = m+n-2 < m+m-1 = r+s$, que é uma contradição. Portanto $r \geq m$ ou $s \geq n$, decorre do primeiro caso que $x^r = 0$, que implica que $x^r y^s = 0$; do segundo, $y^s = 0$, e daí $x^r y^s = 0$, deste modo $(x+y)^{m+n-1} = 0$, logo $x + y \in \mathfrak{N}$. Agora, note que $-x \in \mathfrak{N}$, uma vez que $(-x)^m = (-1)^m x^m = 0$. Logo resta mostramos que $R\mathfrak{N} \subseteq \mathfrak{N}$, com efeito, se $r \in R$ e $x \in \mathfrak{N}$, então existe $n > 0$, tal que $x^n = 0$. Daí como R é comutativo $(rx)^n = r^n x^n = r^n 0 = 0$, portanto $rx \in \mathfrak{N}$. Logo $\mathfrak{N}$ é um ideal de R. Mostremos agora que o anel quociente $R/\mathfrak{N}$ não tem elemento nilpotente não-nulo. De fato se $\bar{x} \in R/\mathfrak{N}$ é nilpotente, então existe $n > 0$, tal que $\bar{x}^n = \bar{0}$, daí $\bar{x^n} = \bar{0}$. Logo $x^n \in \mathfrak{N}$, portanto existe $m > 0$, tal que $(x^n)^m = 0$, mas como $mn > 0$, segue que $x \in \mathfrak{N}$, daí $\bar{x} = \bar{0}$. Portanto, $\bar{0}$ é o único elemento nilpotente de $\mathfrak{N}$.

■

Proposição 1.1.27. *O nilradical $\mathfrak{N}$ de um anel R coincide com a interseção de todos ideais primos de R.*

Demonstração: Denote por $\mathfrak{N}_\circ$ a interseção de todos ideais primos de R. Seja x um elemento do nilradical $\mathfrak{N}$ de R, então x é um elemento nilpotente. Logo existe $n > 0$, tal que $x^n = 0$. Seja $\mathfrak{p}$ um ideal primo de R (recorde que sempre existe um ideal maximal no anel R comutativo com 1), então $0 = x^n \in \mathfrak{p}$, daí como $\mathfrak{p}$ é primo, segue que $x \in \mathfrak{p}$ ou $x^{n-1} \in \mathfrak{p}$. Se $x \in \mathfrak{p}$, então temos o que queremos. Suponha por absurdo que $x \notin \mathfrak{p}$, então $x^{n-1} \in \mathfrak{p}$. Aplicando o mesmo raciocínio, obteremos que $x^{n-2} \in \mathfrak{p}$. Procedendo deste modo, obtemos que $x = x^{n-(n-1)} \in \mathfrak{p}$, que é uma contradição. Deste modo, $x \in \mathfrak{p}$ para cada ideal primo

$\mathfrak{p}$, daí $\mathfrak{N} \subseteq \mathfrak{N}_o$. Reciprocamente, suponha que $x \notin \mathfrak{N}$. Defina Σ como sendo o conjunto de ideais I de R que têm a propriedade de que se $n > 0$, então $x^n \notin I$. Temos que $\Sigma \neq \emptyset$, pois $(0) \in \Sigma$, uma vez que $x^n \notin (0)$ para todo $n > 0$, haja vista que x não é um elemento nilpotente. Agora, ordene Σ pela inclusão, assim cada cadeia $C = (I_\lambda)$ de Σ tem uma cota superior, $\bigcup_{\lambda\in\Lambda} I_\lambda$, logo pelo Lema de Zorn, Σ tem um elemento maximal $\mathfrak{p}$. Mostremos que $\mathfrak{p}$ é um ideal primo e que $x \notin \mathfrak{p}$. De fato, sejam $y, z \notin \mathfrak{p}$ em R, então os ideais $(y) + \mathfrak{p}$ e $(z) + \mathfrak{p}$ contêm $\mathfrak{p}$ propriamente, logo existem inteiros $m, n > 0$, tais que $x^m \in (y) + \mathfrak{p}$, e $x^n \in (z) + \mathfrak{p}$. Deste modo $x^{m+n} \in (yz) + \mathfrak{p}$, pois se $x^m = ry + t$ e $x^n = sz + u$, em que $r, s \in R$ e $t, u \in \mathfrak{p}$, então $x^{n+m} = rysz + ryu + t(sz + u) \in (yz) + \mathfrak{p}$, logo existe $n + m > 0$, tal que $x^{n+m} \in (yz) + \mathfrak{p}$, e daí $(yz) + \mathfrak{p} \notin \Sigma$, e consequentemente $yz \notin \mathfrak{p}$, pois caso contrário, teríamos $(yz) + \mathfrak{p} = \mathfrak{p} \in \Sigma$, que é uma contradição. Em suma, temos que $y, z \notin \mathfrak{p}$ implica que $yz \notin \mathfrak{p}$, logo $\mathfrak{p}$ é um ideal primo de R. Agora, como $\mathfrak{p} \in \Sigma$ (elemento maximal em Σ para C), segue que $x \notin \mathfrak{p}$, logo $x \notin \mathfrak{N}_o$, assim temos que $x \notin \mathfrak{N}$ implica que $x \notin \mathfrak{N}_o$, equivalentemente, $\mathfrak{N}_o \subseteq \mathfrak{N}$. Portanto, $\mathfrak{N}_o = \mathfrak{N}$.

■

Proposição 1.1.28. *Considere que $\varphi : R \longrightarrow S$ seja um homomorfismo de anéis. Então, se $\mathfrak{q}$ é um ideal primo de S, então a imagem inversa $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ de $\mathfrak{q}$ por φ é um ideal primo de R.*

Demonstração: Seja $xy \in \mathfrak{p}$, então $\varphi(xy) \in \mathfrak{q}$, daí $\varphi(x)\varphi(y) \in \mathfrak{q}$, mas como $\mathfrak{q}$ é um ideal primo, segue que $\varphi(x) \in \mathfrak{q}$ ou $\varphi(y) \in \mathfrak{q}$, de modo que $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Portanto, $\mathfrak{p}$ é um ideal primo de R.

■

Definição 1.1.29. *O radical de Jacobson $\mathfrak{R}$ de um anel R é definido como sendo a interseção de todos ideais maximais de R.*

Proposição 1.1.30. *Seja R um anel comutativo com 1. Então $x \in \mathfrak{R}$ se, e somente se, $1 - xy$ é uma unidade em R para todo $y \in R$.*

Demonstração:
($\Rightarrow$) Considere que $x \in \mathfrak{R}$, e suponha, por absurdo, que $1 - xy$ não seja uma unidade em R, então pelo Corolário 1.1.17, existe um ideal maximal $\mathfrak{m}$ de R, tal que $1 - xy \in \mathfrak{m}$. No entanto $x \in \mathfrak{m}$, pois $\mathfrak{R}$ é a interseção de todos ideais maximais de R, logo $xy \in \mathfrak{m}$, mas como

$1 - xy \in \mathfrak{m}$, segue que $1 \in \mathfrak{m}$. Portanto $\mathfrak{m} = R$, que é uma contradição. Logo $1 - xy$ é uma unidade em R.
($\Leftarrow$) Suponha que $x \notin \mathfrak{R}$, daí existe um ideal maximal $\mathfrak{m}$ de R, tal que $x \notin \mathfrak{m}$, deste modo o ideal I gerado por $\mathfrak{m}$ e x contém o ideal maximal $\mathfrak{m}$ propriamente, portanto $I = R$. Mas como $1 \in R$, segue que existem $z \in \mathfrak{m}$, e $y \in R$, tais que $xy + z = 1$, daí $1 - xy = z \in \mathfrak{m}$, logo $1 - xy$ não é uma unidade em R.

■

1.1.1 Operações entre ideais

Nesta seção, discutiremos com mais detalhe as operações: soma, interseção e produto, que podem ser realizadas entre ideais em um anel R.

Proposição 1.1.31. *Se I e J são ideais em um anel R, então $I+J = \{x+y \mid x \in I, y \in J\}$ é o menor ideal de R contendo I e J.*

Demonstração: Sejam $a = x_1 + y_1 \in I + J$, e $b = x_2 + y_2 \in I + J$, em que $x_1, x_2 \in I$, e $y_1, y_2 \in J$, então $a - b = (x_1 - x_2) + (y_1 - y_2) \in I + J$. Agora se $r \in R, x \in I, y \in J$, então $r(x + y) = rx + ry \in I + J$, pois $rx \in I$, e $ry \in J$, já que I e J são ideais. Portanto, $I + J$ é um ideal que contém I e J, note que $x = x + 0 \in I + J$, e $y = 0 + y \in I + J$. Agora, seja L um ideal de R contendo I e J, então como L é ideal , segue que $x + y \in L$ para todo $x \in I$ e para todo $y \in J$, logo $I + J \subseteq L$.

■

Definição 1.1.32. *Definimos a soma de uma família $(\mathfrak{a}_\lambda)_{\lambda\in\Lambda}$ de ideais de R como sendo o conjunto formado pelos elementos da forma $\sum_{\lambda\in\Lambda} x_\lambda$, em que cada $x_\lambda \in \mathfrak{a}_\lambda$, e todos, exceto uma quantidade finita de elementos $\mathfrak{a}_\lambda$, são nulos. Denotemos por $\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$ tal soma.*

Proposição 1.1.33. $\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$ *é um ideal de R.*

Demonstração: Sejam $\sum_{\lambda\in\Lambda} x_\lambda$, $\sum_{\lambda\in\Lambda} y_\lambda$ elementos de $\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$, note que $\sum_{\lambda\in\Lambda} x_\lambda + \sum_{\lambda\in\Lambda} y_\lambda = \sum_{\lambda\in\Lambda}(x_\lambda + y_\lambda) \in \sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$, por outro lado, para cada $r \in R$, temos que $r\sum_{\lambda\in\Lambda} x_\lambda = \sum_{\lambda\in\Lambda} rx_\lambda \in \sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$. Portanto, $\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$ é um ideal de R.

■

Definição 1.1.34. *O produto de dois ideais I e J é definido como sendo o ideal IJ gerado por todos produtos xy, em que $x \in I$ e $y \in J$. Assim IJ consiste de todas somas finitas $\sum x_i y_i$, em que $x_i \in I$, e $y_i \in J$.*

Observação 1.1.35. *De modo análogo, definimos o produto de qualquer família finita de ideais de R. Em particular, denotemos por I^n, em que $n > 0$, como sendo o ideal gerado pelos produtos $x_1 x_2 \dots x_n$, em que cada fator $x_i \in I$. Convencionamos que $I^0 = R$. O produto de n ideais $I_1, \dots, I_n$ será denotado por $\prod_{j=i}^{n} I_j$.*

Proposição 1.1.36. *Se I, J, e L são ideais de R, então $I(J+L) = IJ + IL$.*

Demonstração: Note que $x(y+z) = xy + xz, \forall x \in I, \forall y \in J, \forall z \in L$, daí $I(J+L) \subseteq IJ + IL$. Por outro lado, se $u = xy + x_2 z \in IJ + IL$, com $x_2 \in I$, então como $y, z \in J + L$, segue que $xy, x_2 z \in I(J+L)$, consequentemente, $u \in I(J+L)$. Logo, $I(J+L) = IJ + IL$.

■

Proposição 1.1.37 (Lei Modular)**.** *Se I, J, e L são ideais de R, tais que $I \supseteq J$ ou $I \supseteq L$. Então, $I \cap (J+L) = (I \cap J) + (I \cap L)$.*

Demonstração: Suponha que $I \supseteq J$. Seja $x = y+z \in I \cap (J+L)$, em que $x \in I, y \in J, z \in L$, mas como I contém J, segue que $y \in I$, e daí $z = x - y \in I$. Logo $y \in I \cap J = J$, e $z \in I \cap L$, de modo que $x \in (I \cap J) + (I \cap L)$. Portanto $I \cap (J+L) \subseteq (I \cap J) + (I \cap L)$. Reciprocamente, seja $y + z \in (I \cap J) + (I \cap L)$ com $y \in I \cap J$, e $z \in I \cap L$, então $y, z \in I$ que implica que $y + z \in I$. Por outro lado, $y + z \in J + L$, portanto $y + z \in I \cap (J+L)$. O caso em que $I \supseteq L$ é análogo.

■

Lema 1.1.38. *Sejam I e J ideais de R, então $(I+J)(I \cap J) \subseteq IJ$.*

Demonstração: Seja $u \in (I+J)(I \cap J)$, então existem $x_i \in I, y_i \in J, z \in I \cap J, n \in \mathbb{N}$, tais que $u = \sum_{i=1}^{n} (x_i + y_i) z_i$, agora note que $u = \sum_{i=1}^{n} x_i z_i + \sum_{i=1}^{n} z_i y_i$, mas como cada $x_i y_i \in IJ$, e cada $z_i y_i \in IJ$, segue que $u \in IJ$. Portanto, $(I+J)(I \cap J) \subseteq IJ$.

■

Definição 1.1.39. *Dois ideais I e J de R são chamados comaximais(ou coprimos), quando $I + J = R$.*

Proposição 1.1.40. *Se I e J são ideais comaximais, então $IJ = I \cap J$.*

Demonstração: A inclusão $IJ \subseteq I \cap J$ é uma tautologia. Pelo Lema 1.1.38, temos que $(I+J)(I \cap J) \subseteq IJ$. No entanto, por hipótese, $I + J = R$, logo $R(I \cap J) \subseteq IJ$, daí como $1 \in R$ e $I \cap J$ é um ideal, segue que $I \cap J \subseteq IJ$. Portanto $IJ = I \cap J$.

■

Proposição 1.1.41. *I e J são ideais comaximais em R se, e somente se, existem $x \in I$ e $y \in J$, tais que $x + y = 1$.*

Demonstração: Se I e J são comaximais, então $I + J = R$, daí $1 \in I + J$, logo existem $x \in I$, $y \in J$, tais que $x + y = 1$. Reciprocamente, se existem $x \in I$, e $y \in J$, tais que $x + y = 1$, então $1 \in I + J$. Logo pela Proposição 1.1.8, $I + J = R$.

■

Proposição 1.1.42. *Sejam R um anel, e $I_1, \ldots, I_n$ ideais de R. Considere que*

$$\varphi : R \longrightarrow \prod_{k=1}^{n} R/I_k,$$

seja um homomorfismo definido por $\varphi(x) = (x + I_1, \ldots, x_n + I_n)$. Então,

(i) se I_i e I_j são comaximais sempre que $i \neq j$, então $\prod_{k=1}^{n} I_k = \bigcap_{k=1}^{n} I_k$;

(ii) ***(Teorema Chinês dos Restos)*** *O homomorfismo φ é sobrejetivo se, e somente se, I_i e I_j são comaximais sempre que $i \neq j$;*

(iii) φ é injetivo se, e somente se, $\bigcap_{k=1}^{n} I_k = (0)$.

Demonstração:

(i) Façamos indução sobre $n \geq 2$. Se $n = 2$, e $I_1 + I_2 = R$, então pela Proposição 1.1.40, $I_1 I_2 = I_1 \cap I_2$, daí $\prod_{k=1}^{2} I_k = \bigcap_{k=1}^{2} I_k$. Suponha que $n > 2$, e que (i) seja válida para todo $m < n$, assim $\prod_{k=1}^{n-1} I_k = \bigcap_{k=1}^{n-1} I_k$. Segue pela hipótese em (i) que, I_n e I_m, $1 \leq m \leq n-1$, são comaximais, pois $m \neq n$, portanto $I_m + I_n = R$, logo pela Proposição 1.1.41, obtemos

para cada $m \in \{1, \ldots, n-1\}$, elementos $x_m \in I_m$, $y_m \in I_n$, tais que $x_m + y_m = 1$, portanto $\prod_{k=1}^{n-1} x_k = \prod_{k=1}^{n-1}(1 - y_k)$.

Agora note que $\prod_{k=1}^{n-1}(1 - y_k) \equiv 1(mod\ I_n)$. De fato, temos $\prod_{k=1}^{n-1}(1 - y_k) = \prod_{k=2}^{n-1}(1 - y_k) - y_1 \prod_{k=2}^{n-1}(1 - y_k)$. Observe que ${y_1}' \stackrel{def}{=} y_1 \prod_{k=2}^{n-1}(1 - y_k) \in I_n$, uma vez que $y_1 \in I_n$. Deste modo, $\prod_{k=1}^{n-1}(1 - y_k) = \prod_{k=2}^{n-1}(1 - y_k) - {y_1}'$. Usando o mesmo raciocínio, obtemos $\prod_{k=1}^{n-1}(1 - y_k) = \prod_{k=3}^{n-1}(1 - y_k) - {y_2}' - {y_1}'$ em que ${y_2}' \stackrel{def}{=} y_2 \prod_{k=3}^{n-1}(1 - y_k)$ pertence a I_n, pois $y_2 \in I_n$. Procedendo desta maneira, obtemos $\prod_{k=1}^{n-1}(1 - y_k) = 1 - \sum_{k=1}^{n-1} {y_k}'$, em que ${y_k}' = y_k \prod_{i=k+1}^{n-1}(1 - y_i) \in I_n$. Logo $(\prod_{k=1}^{n-1} x_k) - 1 = -\sum_{k=1}^{n-1} {y_k}' \in I_n$, e portanto $\prod_{k=1}^{n-1} x_k \equiv 1(mod\ I_n)$. Mas já que $(\prod_{k=1}^{n-1} x_k) - 1 \in I_n$, existe $z \in I_n$, tal que $(\prod_{k=1}^{n-1} x_k) + z = 1$. Note que $\prod_{k=1}^{n-1} x_k \in \prod_{k=1}^{n-1} I_k$, portanto pela Proposição 1.1.41, segue que $\prod_{k=1}^{n-1} I_k$ e I_n são comaximais. Logo pela Proposição 1.1.40, $(\prod_{k=1}^{n-1} I_k)I_n = (\prod_{k=1}^{n-1} I_k) \cap I_n$, consequentemente, $\prod_{k=1}^{n} I_k = (\prod_{k=1}^{n-1} I_k)I_n = (\prod_{k=1}^{n-1} I_k) \cap I_n = (\bigcap_{k=1}^{n-1} I_k) \cap I_n = \bigcap_{k=1}^{n} I_k$. Portanto, pelo princípio de indução, segue o resultado.

(ii)

($\Rightarrow$) Suponha que $1 \leq i < j \leq n$, e que φ seja sobrejetivo. Então dado $(\bar{x_1}, \ldots, \bar{x_i}, \ldots, \bar{x_n}) \in \prod_{k=1}^{n} R/I_k$ definido por $\bar{x_i} = 1 + I_i$, $\bar{x_j} = I_j$, se $j \neq i$, existe $x \in R$ tal que $\varphi(x) = (I_1, I_2, \ldots, 1 + I_i, \ldots, I_j, \ldots, I_n)$. No entanto, $\varphi(x) = (x + I_1, x + I_2, \ldots, x + I_i, \ldots, x + I_j, \ldots, x + I_n)$, de modo que $x \equiv 1(mod\ I_i)$, e $x \equiv 0(mod\ I_j)$, portanto existem $1 - x \in I_i$, e $x \in I_j$, tais que $(1 - x) + x = 1 \in I_i + I_j$, logo pela Proposição 1.1.41, segue que I_i e I_j são comaximais.

($\Leftarrow$) Seja $z = (x_1 + I_1, \ldots, x_n + I_n) \in \prod_{k=1}^{n} R/I_k$, mostremos que existe $r \in R$, tal que $\varphi(r) = z$. Fixe $i \in \{1, \ldots, n\}$. Por hipótese, $I_i + I_j = R$, sempre que $i \neq j$, daí pela Proposição 1.1.41, existem $u_{ij} \in I_i$, $v_{ij} \in I_j$, tais que $u_{ij} + v_{ij} = 1$. Defina $r_i = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} v_{ij}$, então $r_i \equiv 0(mod\ I_j)$, e $r_i \equiv 1(mod\ I_i)$ (note que $r_i = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (1 - u_{ij})$ e use o mesmo raciocínio em (i)), daí $r_i x_i \equiv 0(mod\ I_j)$, e $r_i x_i \equiv x_i(mod\ I_i)$, de modo que $\varphi(r_i x_i) = (I_1, I_2, \ldots, x_i + I_i, I_{i+1}, \ldots, I_n)$, defina $r = \sum_{i=1}^{n} r_i x_i$, daí temos que $\varphi(r) = \sum_{i=1}^{n} \varphi(r_i x_i) = z$, logo φ é sobrejetivo.

(iii) Note que

$$\begin{aligned} Ker(\varphi) &= \{x \in R \mid (x + I_1, \ldots, x + I_n) = (I_1, \ldots, I_n)\} \\ &= \{x \in R \mid x \in I_k, k = 1, \ldots, n\} \\ &= \{x \in R \mid x \in \bigcap_{k=1}^{n} I_k\} \\ &= \bigcap_{k=1}^{n} I_k. \end{aligned}$$

Logo φ é injetivo se, e somente se, $\bigcap_{k=1}^{n} I_k = (0)$.

■

Observação 1.1.43. *Note, então que se I_i e I_j são comaximais sempre que $i \neq j$, então segue pelo primeiro Teorema do isomorfismo que,*

$$\prod_{k=1}^{n} R/I_k \cong R/\bigcap_{k=1}^{n} I_k = R/\prod_{k=1}^{n} I_k.$$

Exemplo 1.1.44. *Note que a Proposição 1.1.42 fornece um algoritmo para solucionar congruências múltiplas no caso em que há comaximalidade. Por exemplo, considere o seguinte sistema*

$$\begin{cases} r \equiv 3 \pmod{5\mathbb{Z}} \\ r \equiv 4 \pmod{3\mathbb{Z}} \\ r \equiv 6 \pmod{7\mathbb{Z}} \end{cases}$$

Considere as notações de acordo com a Proposição 1.1.42, ou seja,

$$R = \mathbb{Z}, I_1 = 5\mathbb{Z}, I_2 = 3\mathbb{Z}, I_3 = 7\mathbb{Z}, x_1 = 3, x_2 = 4, x_3 = 6$$

e defina $\varphi : \mathbb{Z} \longrightarrow \prod_{i=1}^{3} \mathbb{Z}/I_i$, note que existir solução para o sistema acima é equivalente a: dado $z = (3 + 5\mathbb{Z}, 4 + 3\mathbb{Z}, 6 + 7\mathbb{Z}) \in \prod_{i=1}^{3} \mathbb{Z}/I_i$, existir $r \in \mathbb{Z}$ tal que $\varphi(r) = z$. Como os ideais $3\mathbb{Z}, 5\mathbb{Z}, 7\mathbb{Z}$ são dois a dois comaximais, segue pela Proposição 1.1.42 que, φ é sobrejetivo, logo o sistema em questão tem solução. Usemos o procedimento na Proposição 1.1.42(ii):

Temos $5\mathbb{Z}+3\mathbb{Z} = \mathbb{Z}$, logo existem $u_{12} = 10, v_{12} = -9$, tais que $u_{12}+v_{12} = 1$, também temos $5\mathbb{Z}+7\mathbb{Z} = \mathbb{Z}$, consideremos $u_{13} = 15, v_{13} = -14$. Para $3\mathbb{Z}+5\mathbb{Z} = \mathbb{Z}$, e $3\mathbb{Z}+7\mathbb{Z} = \mathbb{Z}$, tomemos, respectivamente, $u_{21} = -9, v_{21} = 10$, e $u_{23} = 15, v_{23} = -14$, por fim, para $7\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$, e $7\mathbb{Z}+3\mathbb{Z} = \mathbb{Z}$, tomemos, respectivamente, $u_{31} = -14, v_{31} = 15$, e $u_{32} = -14, v_{32} = 15$. Assim,

com as mesmas notações anteriores, obtemos $r_1 = v_{12}v_{13} = -9(-14) = 126$, $r_2 = v_{21}v_{23} = 10(-14) = -140$, *e* $r_3 = v_{31}v_{32} = 15^2 = 225$. *Logo,* $r = \sum_{i=1}^{3} r_i x_i = 126.3 + (-140).4 + 225.6 = 1168$, *logo* $\varphi(1168) = z$. *De fato,*

$$\begin{cases} 1168 \equiv 3 \pmod{5\mathbb{Z}} \\ 1168 \equiv 4 \pmod{3\mathbb{Z}} \\ 1168 \equiv 6 \pmod{7\mathbb{Z}} \end{cases}$$

Observe que qualquer número da forma $1168 + 3.5.7k = 1168 + 105k, k \in \mathbb{Z}$, *é solução do sistema acima, em particular, a menor solução positiva é dada por* $1168 + 105(-11) = 13$, *note que:*

$$\begin{cases} 13 \equiv 3 \pmod{5\mathbb{Z}} \\ 13 \equiv 4 \pmod{3\mathbb{Z}} \\ 13 \equiv 6 \pmod{7\mathbb{Z}} \end{cases}$$

Proposição 1.1.45. *Considere que* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *sejam ideais primos, e que* $\mathfrak{a}$ *seja um ideal contido em* $\bigcup_{i=1}^{n} \mathfrak{p}_i$. *Então,* $\mathfrak{a} \subseteq \mathfrak{p}_i$ *para algum* i.

Demonstração: Mostremos o resultado equivalente: se $\mathfrak{a} \nsubseteq \mathfrak{p}_i$, para todo $i = 1, \ldots, n$, então $\mathfrak{a} \nsubseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. Façamos indução sobre $n \geq 1$. Se $n = 1$, temos trivialmente que $\mathfrak{a} \nsubseteq \mathfrak{p}_1$ implica que $\mathfrak{a} \nsubseteq \mathfrak{p}_1$. Suponha que o resultado seja verdadeiro para todo $k < n$, então se $\mathfrak{a} \nsubseteq \mathfrak{p}_i$, para todo i, segue pela hipótese de indução que, para cada $j \in \{1, \ldots, n\}$, $\mathfrak{a} \nsubseteq \bigcup_{\substack{1 \leq i \leq n \\ i \neq j}} \mathfrak{p}_i$, logo existe $x_j \in \mathfrak{a}$, tal que $x_j \notin \mathfrak{p}_i$, para todo $i \neq j$, ou seja, $x_j \notin \bigcup_{\substack{1 \leq i \leq n \\ i \neq j}} \mathfrak{p}_i$. Consideremos dois casos:

Caso I- Se $x_j \notin \mathfrak{p}_j$. Então, $x_j \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$, daí $\mathfrak{a} \nsubseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, logo pelo princípio de indução, segue o resultado;

Caso II- Se $x_j \in \mathfrak{p}_j$, para cada $j = 1, \ldots, n$ dado. Defina $x = \sum_{i=1}^{n} y_i$, em que $y_i = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} x_j$, note que $x \in \mathfrak{a}$, e que $y_i \in \mathfrak{p}_j$, para todo $j \neq i$, daí $y_i \in \bigcup_{\substack{1 \leq j \leq n \\ j \neq i}} \mathfrak{p}_j$. Observe que $y_i \notin \mathfrak{p}_i$, de fato, suponha por absurdo que, $y_i = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} x_j \in \mathfrak{p}_i$, então como $\mathfrak{p}_i$ é um ideal primo, segue que $x_j \in \mathfrak{p}_i$, para algum $j \neq i$, mas isso é uma contradição, pois $x_j \notin \bigcup_{\substack{1 \leq i \leq n \\ i \neq j}} \mathfrak{p}_i$.

Afirmamos que $x \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$, com efeito, se $x \in \bigcup_{i=1}^{n} \mathfrak{p}_i$, então $x \in \mathfrak{p}_j$ para algum j, daí $y_j = x - \sum_{i \neq j} y_i \in \mathfrak{p}_j$, uma vez que x e $\sum_{i \neq j} y_i$ pertencem a $\mathfrak{p}_j$, mas então $y_j \in \mathfrak{p}_{\mathfrak{j}}$, que é uma contradição. Logo, $x \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$, consequentemente $\mathfrak{a} \nsubseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. Portanto, pelo princípio de indução, temos o resultado.

■

Proposição 1.1.46. *Considere que $\mathfrak{a}_1, \ldots \mathfrak{a}_n$ sejam ideais, e que $\mathfrak{p}$ seja um ideal primo contendo $\bigcap_{i=1}^{n} \mathfrak{a}_{\mathfrak{i}}$. Então, $\mathfrak{p} \supseteq \mathfrak{a}_{\mathfrak{i}}$ para algum i. Se $\mathfrak{p} = \bigcap_{i=1}^{n} \mathfrak{a}_i$, então $\mathfrak{p} = \mathfrak{a}_{\mathfrak{i}}$ para algum i.*

Demonstração: Mostremos, equivalentemente que, se $\mathfrak{p} \not\supseteq \mathfrak{a}_i$, para todo $i = 1, \ldots, n$, então $\mathfrak{p} \not\supseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$. De fato, se $\mathfrak{p} \not\supseteq \mathfrak{a}_i$, para todo $i = 1, \ldots, n$, então para cada i, existe $x_i \in \mathfrak{a}_i$, tal que $x_i \notin \mathfrak{p}$, portanto como $\mathfrak{p}$ é um ideal primo, segue que $\prod_{i=1}^{n} x_i \notin \mathfrak{p}$. No entanto, $\prod_{i=1}^{n} x_i \in \prod_{i=1}^{n} \mathfrak{a}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$, deste modo $\prod_{i=1}^{n} x_i \in \bigcap_{i=1}^{n} \mathfrak{a}_i$, logo $\mathfrak{p} \not\supseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$. Agora, se $\mathfrak{p} = \bigcap_{i=1}^{n} \mathfrak{a}_i$, então já que $\mathfrak{p} \supseteq \mathfrak{a}_{\mathfrak{i}}$, para algum i, segue que $\mathfrak{a}_i \subseteq \mathfrak{p} = \bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{a}_i$, portanto $\mathfrak{p} = \mathfrak{a}_i$.

■

Definição 1.1.47. *Se I e J são ideais em um anel R, definimos o quociente entre ideais I e J por*

$$(I : J) = \{x \in R \mid xJ \subseteq I\}$$

Observação 1.1.48. *Em particular, quando $I = (0)$, chamamos $(0 : J)$ de anulador de J, o qual denotamos por $Ann(J)$. Por abuso de notação, denotemos $(I : (x))$ por $(I : x)$, para qualquer $x \in R$.*

Proposição 1.1.49. *$(I : J) = \{x \in R \mid xJ \subseteq I\}$ é um ideal de R.*

Demonstração: Com efeito, se $x, y \in (I : J)$, então $xJ \subseteq I$, e $yJ \subseteq I$, mas como I é um ideal, segue que $xJ - yJ \subseteq I$, mas $xJ - yJ = (x - y)J$, então $(x - y)J \subseteq I$. Logo $x - y \in (I : J)$. Agora, considere $r \in R$, e $x \in (I : J)$, temos que $xJ \subseteq I$, mas como I é um ideal, segue que $r(xJ) \subseteq I$, logo $rx \in (I : J)$. Portanto, $(I : J)$ é um ideal de R.

■

Definição 1.1.50. *Se I é um ideal de R, definimos o radical de I por*

$$r(I) = \{x \in R \mid x^n \in I, \text{ para algum inteiro } n > 0\}.$$

Proposição 1.1.51. *O radical de um ideal I de R é um ideal.*

Demonstração: Considere que

$$\varphi : R \longrightarrow R/I$$

seja o homomorfismo canônico. Mostremos que $r(I) = \varphi^{-1}(\mathfrak{N}_{R/I})$, em que $\mathfrak{N}_{R/I}$ é o nilradical de R/I. De fato,

$$\begin{aligned} \varphi^{-1}(\mathfrak{N}_{R/I}) &= \{x \in R \mid \varphi(x) \in \mathfrak{N}_{R/I}\} = \{x \in R \mid \bar{x} \in \mathfrak{N}_{R/I}\} \\ &= \{x \in R \mid \bar{x}^n = \bar{0}, \text{ para algum } n > 0\} \\ &= \{x \in R \mid x^n \in I, \text{ para algum } n > 0\} \\ &= r(I). \end{aligned}$$

Note que trivialmente $I \subseteq r(I)$, deste modo, segue pelo Teorema da Correspondência que, $r(I)$ é o único ideal de R contendo $ker(\varphi) = I$, tal que $r(I) = \varphi^{-1}(\mathfrak{N}_{R/I})$.

■

Proposição 1.1.52. *O radical de um ideal I é a interseção dos ideais primos de R que contêm I.*

Demonstração: Considere que

$$\varphi : R \longrightarrow R/I$$

seja o homomorfismo canônico. Segue pela Proposição 1.1.27 que, o nilradical de R/I coincide com a interseção dos ideais primos de R/I, logo temos que

$$r(I) = \varphi^{-1}(\mathfrak{N}_{R/I}) = \varphi^{-1}(\bigcap_{\substack{\mathfrak{q} \trianglelefteq R/I \\ primo}} \mathfrak{q}) = \bigcap_{\substack{\mathfrak{q} \trianglelefteq R/I \\ primo}} \varphi^{-1}(\mathfrak{q})$$

No entanto, pelo Teorema da Correspondência, segue que para cada ideal primo $\mathfrak{q}$ de R/I está associado univocamente um ideal $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ de R contendo I, que é primo pela Proposição 1.1.28. Portanto, $r(I)$ é igual a interseção dos ideias primos de R que contêm I.

■

Proposição 1.1.53. *Sejam I e J ideais de uma anel R comutativo com* 1. *Então:*

(i) $r(I) \supseteq I$;

(ii) $r(r(I)) = r(I)$

(iii) $r(IJ) = r(I \cap J) = r(I) \cap r(J)$;

(iv) $r(I) = R$ *se, e somente se,* $I = R$;

(v) $r(I) + r(J) \subseteq r(I + J)$;

(vi) $r(I + J) = r(r(I) + r(J))$; *e*

(vii) se $\mathfrak{p}$ *é um ideal primo de* R*, então* $r(\mathfrak{p}^n) = \mathfrak{p}$*, para todo* $n > 0$.

Demonstração:

(i) Se $x \in I$, então $x^1 \in I$, logo $x \in r(I)$. Portanto, $r(I) \supseteq I$;

(ii) Por (i), temos que $r(r(I)) \supseteq r(I)$. Seja $x \in r(r(I))$, então existe $n > 0$ tal que $x^n \in r(I)$, daí existe $m > 0$, tal que $(x^n)^m = x^{nm} \in I$, logo $x \in r(I)$. Portanto, $r(r(I)) \subseteq r(I)$.

(iii) Como $IJ \subseteq I \cap J$, segue que $r(IJ) \subseteq r(I \cap J)$. Seja $x \in r(I \cap J)$, então existe $n > 0$, tal que $x^n \in I \cap J$, daí $x^n \in I$ e $x^n \in J$, de modo que $x \in r(I)$, e $x \in r(J)$, logo $x \in r(I) \cap r(J)$. Em suma, $r(IJ) \subseteq r(I \cap J) \subseteq r(I) \cap r(J)$. Basta mostrarmos que $r(I) \cap r(J) \subseteq r(IJ)$, de fato, seja $y \in r(I) \cap r(J)$, então existem $m, n > 0$, tais que $y^m \in I$, e $y^n \in J$, mas então $y^m y^n = y^{m+n} \in IJ$, logo $y \in r(IJ)$.

(iv) Como $1 \in R$, e $R = r(I)$, segue que $1 \in r(I)$, logo existe $n > 0$ tal que $1^n = 1 \in I$, logo $R = I$. Reciprocamente, se $I = R$, então $r(I) = r(R) = R$.

(v) Seja $x \in r(I) + r(J)$, então existem $y \in r(I)$ e $z \in r(J)$, tais que $x = y + z$, e existem inteiros positivos m e n, tais que $y^m \in I$, e $z^n \in J$. Mas, como R é comutativo, vale o Teorema Binomial, logo x^{m+n-1} é uma soma de produtos, os quais possuem fatores da forma $y^i z^j$, em que $i + j = m + n - 1$, deste modo devemos ter pelo menos umas das desigualdades $i \geq m$ ou $j \geq n$, pois caso contrário teríamos, $i + j \leq (m-1) + (n-1) \leq m + m - 1 = i + j$. Portanto, cada parcela na expansão de x^{m+n-1} pertence a I ou J, dependendo, respectivamente se $i \geq m$ ou $j \geq n$, logo $x^{m+n-1} \in I + J$. Portanto, $x \in r(I + J)$.

(vi) Como $I + J \subseteq r(I) + r(J)$, segue que $r(I + J) \subseteq r(r(I)) + r(J))$. Agora, por (v), temos que $r(I) + r(J) \subseteq r(I + J)$, logo $r(r(I) + r(J)) \subseteq r(r(I + J))$, no entanto por (ii), temos que $r(I + J) = r(r(I + J))$, portanto, $r(r(I) + r(J)) \subseteq r(I + J)$.

(vii) Mostremos inicialmente que $r(\mathfrak{p}) = \mathfrak{p}$. De fato, se $x \in r(\mathfrak{p})$, então existe $n > 0$, tal que $x^n \in \mathfrak{p}$, mas como $\mathfrak{p}$ é primo, devemos ter $x \in \mathfrak{p}$, portanto $r(\mathfrak{p}) \subseteq \mathfrak{p}$. Logo $r(\mathfrak{p}) = \mathfrak{p}$. Agora, se $n > 0$, então por (iii), segue que $r(\mathfrak{p}^n) = r(\bigcap_{i=1}^{n} r(\mathfrak{p}))$, daí $r(\mathfrak{p}^n) = r(r(\mathfrak{p})) = \mathfrak{p}$.

■

Proposição 1.1.54. *Considere que I e J sejam ideais de R, tais que $r(I)$, $r(J)$ são comaximais. Então I e J são comaximais.*

Demonstração: Como $r(I)$ e $r(J)$ são comaximais, segue que $R = r(I) + r(J)$. No entanto pelo item (v) da Proposição 1.1.53, $R = r(I) + r(J) \subseteq r(I + J)$, logo $R = r(I + J)$. Portanto por (iv), temos que $I + J = R$, i.e. I e J são comaximais.

■

1.1.2 Anéis de frações

Faremos uma construção do anel de frações de um anel R com respeito a um subconjunto multiplicativamente fechado S. Depois apresentaremos um caso particular, o processo de localização de um anel R em um ideal primo $\mathfrak{p}$.

Definição 1.1.55. *Considere que R seja um anel. Dizemos que S é um subconjunto multiplicativamente fechado de R quando $1 \in S$, e S é fechado sob multiplicação.*

Proposição 1.1.56. *A relação $\equiv$ definida sobre $R \times S$ por $(x, s) \equiv (y, t) \Leftrightarrow (xt - ys)u = 0$ para algum $u \in S$, é uma relação de equivalência.*

Demonstração:

(Reflexiva) Seja $(x, s) \in R \times S$, como R é comutativo, temos que para todo $u \in S$, $(xs - sx)u = 0.u = 0$, logo $(x, s) \equiv (x, s)$.

(Simétrica) Suponha que $(x, s) \equiv (y, t)$, então existe $u \in S$, tal que $(xt - ys)u = 0$, mas daí $(ys - xt)(-u) = 0$, logo $(ys - xt)u = 0$. Portanto $(y, t) \equiv (x, s)$.

(Transitiva) Suponha que, $(x,s) \equiv (y,t)$ e $(y,t) \equiv (z,v)$, então existem $u_1, u_2 \in S$, tais que $(xt-ys)u_1 = 0$, e $(yv-zt)u_2 = 0$, mas então $(xt-ys)u_1u_2v = 0$, e $(yv-zt)u_2u_1s = 0$, logo $xv(tu_1u_2) - ysu_1u_2v = 0$, e $ysu_1u_2 - zs(tu_1u_2) = 0$. Somando-se estas duas equações, obtemos $(xv-zs)tu_1u_2 = 0$. Mas como $t, u_1, u_2 \in S$, segue que $tu_1u_2 \in S$, portanto $(x,s) \equiv (z,v)$.

■

Proposição 1.1.57. *O conjunto de todas classes de equivalências de $\equiv$, denotado por $S^{-1}R$, é um anel comutativo com unidade, se são definidas operações de adição e multiplicação em $S^{-1}R$, respectivamente, por*

$$(x/s) + (y/t) = (xt + ys)/st,$$

$$(x/s)(y/t) = xy/st$$

Demonstração: Mostremos que as operações de adição e multiplicação acima, estão bem definidas. Suponha que, $(x,s) \equiv (x_1,s_1)$ e $(y,t) \equiv (y_1,t_1)$, então existem $u, v \in S$, tais que $(xs_1 - x_1s)u = 0$, e $(yt_1 - y_1t)v = 0$. Queremos mostrar que, $(xt+ys, st) \equiv (x_1t_1 + y_1s_1, s_1t_1)$ e $(xy, st) \equiv (x_1y_1, s_1t_1)$. De fato, existe $uv \in S$, tal que $[(xt+ys)s_1t_1 - (x_1t_1 + y_1s_1)st]uv = [(xs_1 - x_1s)u]tt_1v + [(yt_1 - y_1t)v]ss_1u = 0 + 0 = 0$, daí $(xt + ys, st) \equiv (x_1t_1 + y_1s_1, s_1t_1)$. Outrossim, existe $uv \in S$, tal que $(xys_1t_1 - x_1y_1st)uv = (xs_1u)(yt_1v) - (x_1su)(y_1tv) = (x_1su)(y_1tv) - (x_1su)(y_1tv) = 0$, daí $(xy, st) \equiv (x_1y_1, s_1t_1)$. Agora, note que $x/s + 0/u = xu/su = x/s$ para todo $x/s \in S^{-1}R$, logo $0/u, \forall u \in S$ é elemento neutro com respeito à adição, também temos que $x/s + (-x)/s = 0/s$, de modo que cada elemento de $S^{-1}R$ tem elemento simétrico, por fim $1/1$ funciona como elemento neutro da multiplicação. Assim já que as operações acima são ambas associativas e comutativas, e a operação de multiplicação é distributiva em relação à adição, concluimos que $S^{-1}R$ é um anel comutativo com elemento identidade.

■

Definição 1.1.58. *O anel $S^{-1}R$ é chamado de anel de frações de R com respeito a S (subtende-se S multiplicativamente fechado).*

Observação 1.1.59. *Em particular, quando R é um domínio de integridade, temos que o anel de frações $S^{-1}R$, é um corpo, quando $S = R - \{0\}$, tal corpo é chamado de corpo de frações de R .*

Proposição 1.1.60. ***(Propriedade universal).*** *Considere que $g : R \longrightarrow T$ seja um homomorfismo de anéis, tal que $g(s)$ é uma unidade em T para todo s pertencente a um subconjunto multiplicativamente fechado S de R. Então, existe um único homomorfismo de anéis $h : S^{-1}R \longrightarrow T$ tal que $g = h \circ f$, em que $f : R \longrightarrow S^{-1}R$ é um homomorfismo de anéis definido por $f(x) = x/1$.*

Demonstração:

(Existência)

Defina $h : S^{-1}R \longrightarrow T$ por $h(x/s) = g(x)g(s)^{-1}$. Mostremos que h está bem definido. De fato, se $x/s = y/t$, então existe $u \in S$, tal que $(xt - ys)u = 0$. Daí $g(xt - ys)g(u) = 0$, mas como $g(u)$ é uma unidade em T, segue que $g(xt - ys)g(u)g(u)^{-1} = 0$. Logo $g(xt - ys) = 0$, daí $g(xt) = g(ys)$ que implica que $g(x)g(t) = g(y)g(s)$. Mas como $g(t)$ é uma unidade em T, temos que $g(x)(g(t)g(t)^{-1})g(s)^{-1} = g(y)(g(s)g(s)^{-1})g(t)^{-1}$, donde $g(x)g(s)^{-1} = g(y)g(t)^{-1}$. Portanto $h(x/s) = h(y/t)$. Note que h é um homomorfismo de anéis, com efeito $h(x/s + y/t) = h((xt + ys)/st) = g(xt + ys)g(st)^{-1} = (g(xt) + g(ys))g(st)^{-1} = g(xt)g(st)^{-1} + g(ys)g(st)^{-1} = h(xt/st) + h(ys/ts) = h(x/s) + h(y/t)$, também $h((x/s)(y/t)) = h(xy/st) = g(xy)g(st)^{-1} = (g(x)g(s)^{-1})(g(y)g(t)^{-1}) = h(x/s)h(y/t)$, por fim $h(1/1) = g(1)g(1)^{-1} = 1$. Portanto, h é um homomorfismo de anéis, e é tal que $h \circ f = g$, uma vez que para cada $x \in R$, $(h \circ f)(x) = h(f(x)) = h(x/1) = g(x)g(1)^{-1} = g(x)$.

(Unicidade)

Seja $h' : S^{-1}R \longrightarrow T$ um homomorfismo de anéis, tal que $h' \circ f = g$, então para cada $x/s \in S^{-1}R$, temos que $h'(x/s) = h'(x/1)h'(1/s) = h'(f(x))(h'(s/1))^{-1} = g(x)(h'(f(s))^{-1} = g(x)g(s)^{-1} = h(x/s)$, então $h = h'$.

■

Proposição 1.1.61. *Considere que $f : R \longrightarrow S^{-1}R$ seja um homomorfismo de anéis definido por $f(x) = x/1$. Então:*

(i) Se $s \in S$, então $f(s)$ é uma unidade em $S^{-1}R$;

(ii) $f(x) = 0$ implica que $xs = 0$ para algum $s \in S$; e

(iii) Cada elemento de $S^{-1}R$ é da forma $f(x)f(s)^{-1}$ para algum $x \in R$ e para algum $s \in S$.

Demonstração:

(i) Temos que $f(s) = s/1$, note que existe $1/s \in S^{-1}R$, tal que $(s/1)(1/s) = 1/1$, logo $f(s)$ é uma unidade em $S^{-1}R$;

(ii) Se $f(x) = 0$, então $x/1 = 0/1$, logo existe $s \in S$, tal que $(x.1 - 0.1)s = 0$, ou seja, $xs = 0$;

(iii) Seja $x/s \in S^{-1}R$, então $f(x)f(s)^{-1} = (x/1)(1/s) = x/s$.

■

A próxima proposição fornece condições que determinam $S^{-1}R$ a menos de isomorfismos.

Proposição 1.1.62. *Se $g : R \longrightarrow T$ é um homomorfismo de anéis tal que*

(i) $s \in S$ implica que $g(s)$ é uma unidade em T;

(ii) $g(r) = 0$ implica que $rs = 0$ para algum $s \in S$; e

(iii) Cada elemento de T é da forma $g(r)g(s)^{-1}$.

Então existe um único isomorfismo $h : S^{-1}R \longrightarrow T$ tal que $g = h \circ f$.

Demonstração: Se (i) ocorre, então pela Proposição 1.1.60, segue que existe um homomorfismo $h : S^{-1}R \longrightarrow T$, tal que $g = h \circ f$. Assim, basta mostrarmos que h é bijetor. Por (iii), temos que h é sobrejetor, uma vez que cada $y \in T$ é da forma $y = g(x)g(s)^{-1} = g(xs^{-1})$, logo existe $r = xs^{-1} \in R$, tal que $g(r) = y$. Por fim, h é injetor, pois se $x/s \in Ker(h)$, então $h(x/s) = 0$, daí $g(x) = h(f(x)) = h(x/1) = h(xs/1.s) = h(x/s)h(s/1) = 0.h(s/1) = 0$, logo $g(x) = 0$. Portanto por (ii), segue que existe $t \in S$, tal que $xt = 0$. Deste modo, $(x.1 - 0.s)t = 0$, de modo que $(x, s) \equiv (0, 1)$, ou seja, $x/s = 0$ em $S^{-1}R$.

■

Proposição 1.1.63. *Seja $\mathfrak{p}$ um ideal de R. Então, $S = R - \mathfrak{p}$ é multiplicativamente fechado se, e somente se, $\mathfrak{p}$ é um ideal primo.*

Demonstração: Seja $xy \in \mathfrak{p}$, então $xy \notin S$, mas como S é multiplicativamente fechado, segue que $x \notin S$ ou $y \notin S$, daí $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Portanto $\mathfrak{p}$ é um ideal primo de R. Reciprocamente, suponha que $\mathfrak{p}$ seja um ideal primo, então $1 \notin \mathfrak{p}$, daí $1 \in S$. Suponha que $x, y \in S$, então $x \notin \mathfrak{p}$ e $y \notin \mathfrak{p}$, mas como $\mathfrak{p}$ é primo, segue que $xy \notin \mathfrak{p}$, consequentemente $xy \in S$. Portanto S é multiplicativamente fechado.

■

Observação 1.1.64. *No caso de $S = R - \mathfrak{p}$, em que $\mathfrak{p}$ é um ideal primo de R, denotamos $S^{-1}R$ por $R_{\mathfrak{p}}$.*

Proposição 1.1.65. *O anel $R_{\mathfrak{p}}$ é local, cujo ideal maximal é $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}}$.*

Demonstração: Temos que $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}} = \{x/s \mid x \in \mathfrak{p}; s \in S = R - \mathfrak{p}\}$. Temos que se $x/s, y/t \in \mathfrak{m}$, então $x/s - y/t = (xt - ys)/st \in \mathfrak{m}$, uma vez que $xt - ys \in \mathfrak{p}$, pois $\mathfrak{p}$ é ideal, e $st \in S$, pois S é multiplicativamente fechado. Note que $0/1 \in \mathfrak{p}$ é elemento neutro em $\mathfrak{m}$ com respeito à adição, e que $-x/s$ é o simétrico de x/s. Agora, se $x/s \in R_{\mathfrak{p}}$, e $y/t \in \mathfrak{m}$, então $(x/s)(y/t) = xy/st$ pertence a $\mathfrak{m}$, uma vez que $xy \in \mathfrak{p}$, e $st \in S$, portanto $\mathfrak{m}$ é um ideal. Mostremos que $\mathfrak{m}$ é o único ideal maximal de $R_{\mathfrak{p}}$, mostrando que, se $\mathfrak{a}$ é um ideal de R, tal que $\mathfrak{a} \nsubseteq \mathfrak{m}$, então $\mathfrak{a} = R$. De fato, existe $r/s \in \mathfrak{a}$, tal que $r/s \notin \mathfrak{m}$, logo $r \notin \mathfrak{p}$, daí $r \in S$, deste modo r/s é uma unidade em $R_{\mathfrak{p}}$, portanto $\mathfrak{a}$ contém uma unidade, daí $\mathfrak{a} = R$. Portanto, $\mathfrak{m}$ é maximal (único) em R.

■

Definição 1.1.66. *O processo de passar de R a $R_{\mathfrak{p}}$ é chamado de localização de R em $\mathfrak{p}$.*

1.2 Grupos

Nesta seção, apresentaremos alguns resultados clássicos que são utilizados nos próximos capítulos, como por exemplo o Teorema de von Dyck, propriedades de comutadores de um grupo G, e de apresentação de grupos.

Definição 1.2.1. *Considere que G seja um grupo. O grupo derivado de G' de G é definido como o subgrupo gerado por todos comutadores $[g,h] = g^{-1}h^{-1}gh = g^{-1}g^h$.*

Proposição 1.2.2. *São válidas as seguintes propriedades de comutadores em um grupo G:*

(i) $[g,h]^t = [g^t, h^t]$;

(ii) $(gh)^t = g^t h^t$;

(iii) Seja $\varphi : G \longrightarrow H$ um homomorfismo de grupos. Então, se $g, t \in G$, então $\varphi(g^t) = \varphi(g)^{\varphi(t)}$;

(iv) Se $\varphi : G \longrightarrow K$ é um homomorfismo de grupos, então $\varphi([g,h]) = [\varphi(g), \varphi(h)]$, daí $\varphi(G') \subseteq \varphi(K')$.

Demonstração:

(i) De fato, $[g,h]^t = t^{-1}[g,h]t = t^{-1}g^{-1}h^{-1}ght = (t^{-1}g^{-1}t)(t^{-1}h^{-1}t)(t^{-1}gt)(t^{-1}ht) = (g^{-1})^t(h^{-1})^t g^t h^t = (g^t)^{-1}(h^t)^{-1}g^t h^t = [g^t, h^t]$;

(ii) $(gh)^t = t^{-1}ght = (t^{-1}gt)(t^{-1}ht) = g^t h^t$.

(iii) $\varphi(g^t) = \varphi(t^{-1}gt) = \varphi(t^{-1})\varphi(g)\varphi(t) = \varphi(t)^{-1}\varphi(g)\varphi(t) = \varphi(g)^{\varphi(t)}$.

(iv) Com efeito, $\varphi([g,h]) = \varphi(g^{-1}h^{-1}gh) = \varphi(g^{-1})\varphi(h^{-1})\varphi(g)\varphi(h) = \varphi(g)^{-1}\varphi(h)^{-1}\varphi(g)\varphi(h) = [\varphi(g), \varphi(h)] \in K'$. Logo como os geradores de G' são levados K', segue que $\varphi(G') \subseteq \varphi(K')$.

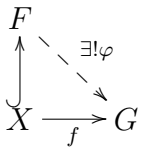
■

Proposição 1.2.3. *O grupo derivado é o menor subgrupo normal de G tal que G/G' é abeliano.*

Demonstração: Seja $h = \prod_{i=1}^{n} h_i \in G'$, em que $h_i = [h_{i1}, h_{i2}]$, então para cada $g \in G$, temos que $h^g = \prod_{i=1}^{n} {h_i}^g = \prod_{i=1}^{n} [{h_{i1}}^g, {h_{i2}}^g] \in G'$, logo $G' \trianglelefteq G$. Agora, suponha que $N \trianglelefteq G$, tal que G/N seja abeliano, então para cada $g, h \in G$, temos que $gNhN = hNgN$, daí $ghN = hgN$, logo $[g,h]N = N$, portanto $[g,h] \in N$, para cada g,h em G, logo $G' \subseteq N$.

■

Definição 1.2.4. *Seja X um subconjunto de um grupo F. Dizemos que F é um grupo livre com base X, quando dados qualquer grupo G e qualquer função $f : X \longrightarrow G$, existe um único homomorfismo $\varphi : F \longrightarrow G$ estendendo f, isto é, $f(x) = \varphi(x)$ para todo $x \in X$, conforme diagrama comutativo abaixo:*



Proposição 1.2.5. *Dado um conjunto X, existe um grupo livre com base X.*

Demonstração: Vide [15], p.344.

■

Definição 1.2.6. *Uma palavra sobre um conjunto X é uma sequência $w = (x_1, x_2, \ldots)$, em que $x_i \in X \cup X^{-1} \cup \{1\}$ para todo i, e tal que existe um inteiro $n \geq 0$ de modo que $a_i = 1$ para todo $i > n$.*

Definição 1.2.7. *A sequência constante sobre X, $(1, 1, \ldots)$ é chamada de palavra vazia e é denotada por 1.*

Observação 1.2.8. *Uma vez que dada uma palavra não vazia $w = (x_1, x_2, \ldots)$, nós temos uma quantidade finita de termos, n, antes de a sequência estagnar em 1. Podemos denotar a palavra w com outra notação:*

$$w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n},$$

em que $x_i \in X$, $\varepsilon_i = 1, -1$ ou 0 com $\varepsilon_n = \pm 1$.

Definição 1.2.9. *Sejam X um conjunto e Δ uma família de palavras sobre X. Dizemos que um grupo G tem geradores X e relações Δ, quando $G \cong F/R$, em que F é um grupo livre com base X, e R é o subgrupo normal de F gerado por Δ. Dizemos que o par $(X \mid \Delta)$ é uma apresentação para o grupo G.*

Observação 1.2.10. *Note que podemos dizer que um grupo G tem apresentação $(X \mid \Delta)$, quando existe um epimorfismo $\varphi : F \longrightarrow G$, em que F é o grupo livre com base X, e $Ker(\varphi) = \langle \Delta \rangle$. Deste modo, dizemos indistintamente que $\varphi : F \longrightarrow G$ ou $(X \mid \Delta)$ é uma apresentação para G.*

Definição 1.2.11. *Um grupo G é chamado finitamente apresentado, quando possui uma apresentação com uma quantidade finita de geradores e relações.*

Proposição 1.2.12. *Seja G um grupo finitamente gerado com apresentação $\varphi : F \longrightarrow G$. Então, se $Ker(\varphi)$ é finitamente gerado, então G é finitamente apresentado.*

Demonstração: Suponha que G tenha apresentação $(X \mid \Delta)$, então $Ker(\varphi) = \langle \Delta \rangle$. Mas como $Ker(\varphi)$ é finitamente gerado, segue que o conjunto de relações Δ é finito, logo o grupo finitamente gerado G é finitamente apresentado.

■

Proposição 1.2.13 (von Dyck). *Sejam G e $\overline{G}$ grupos com apresentações $\theta : F \longrightarrow G$ e $\phi : F \longrightarrow \overline{G}$ tais que toda relação de θ é uma relação de ϕ. Então, a função $\psi : G \longrightarrow \overline{G}$, dada por $\psi(\theta(x)) = \phi(x)$, é um epimorfismo.*

Demonstração: Temos que G e $\overline{G}$ têm, respectivamente, apresentações $(G \mid \Delta_1)$ e $(\overline{G} \mid \Delta_2)$, em que $Ker(\theta) = \langle \Delta_1 \rangle$, e $Ker(\phi) = \langle \Delta_2 \rangle$. Mas como toda relação de θ é uma relação de ϕ, segue que $Ker(\theta) \subseteq Ker(\phi)$. Logo, podemos definir um aplicação

$$\psi : G \longrightarrow \overline{G}$$

por $\theta(x) \mapsto \phi(x)$, a qual é um epimorfismo. Mostremos que ψ está bem definida. De fato, se $\theta(x) = \theta(y)$, então $\theta(xy^{-1}) = 1$, daí $xy^{-1} \in Ker(\theta)$, logo $xy^{-1} \in Ker(\phi)$, portanto $\phi(x) = \phi(y)$, daí $\psi(\theta(x)) = \psi(\theta(y))$. Agora, note que ψ é homomorfismo, pois ϕ e θ também são homomorfismos, e é epimorfismo, uma vez que $\overline{G} = \phi(F)$, logo dado $\phi(x) \in \overline{G}$, existe $\theta(x) \in G$, tal que $\psi(\theta(x)) = \phi(x)$.

■

CAPÍTULO 2

MÓDULOS

Neste capítulo, apresentaremos a definição de módulos livres, módulos projetivos, módulos noetherianos, módulos finitamente gerados sobre um anel comutativo R com 1. Também consideraremos o Grupo de Picard, i.e. o grupo (abeliano) formado pelas classes de isomorfismos de R-módulos projetivos de posto 1.

Definição 2.0.14. *Considere que R seja um anel comutativo com 1. Um R-módulo é um par (M, μ), em que M é um grupo aditivo abeliano, e μ é uma ação linear de R em M, dada por $\mu(r, m) = rm$, tal que $\forall r, s \in R$, e $\forall m, n \in M$:*

$$r(m+n) = rm + rn$$

$$(r+s)m = rm + sm$$

$$(rs)m = r(sm)$$

$$1m = m$$

Proposição 2.0.15. *M é um R-módulo se, e somente se, M é um grupo aditivo abeliano, e existe um homomorfismo de anéis $\varphi : R \longrightarrow End(M)$.*

Demonstração: Suponha que (M, μ) seja um R-módulo. Defina $\varphi : R \longrightarrow End(M)$ por $\varphi(r)(m) = \mu(r, m) = rm$, note que $\varphi(r) \stackrel{def}{=} \varphi_r \in End(M)$, e φ é um homomorfismo de anéis, pois

- $\varphi_{r+s} = \varphi_r + \varphi_s$:
  $\varphi_{r+s}(m) = (r+s)(m) = rm + sm = \varphi_r(m) + \varphi_s(m)$

- $\varphi_{rs} = \varphi_r \circ \varphi_s$:
  $\varphi_{rs}(m) = (rs)m = r(sm) = r\varphi_s(m) = \varphi_r(\varphi_s(m)) = (\varphi_r \circ \varphi_s)(m)$

- $\varphi_1 = 1_{End(M)}$:
  $\varphi_1(m) = 1.m = m = 1_{End(m)}(m)$.

Reciprocamente, suponha que exista um homomorfismo de anéis $\varphi : R \longrightarrow End(M)$, então basta definir $\mu : R \times M \longrightarrow M$ por $\mu(r, m) = \varphi_r(m)$, assim já que $\varphi_r \in End(M)$, $\varphi_{r+s} = \varphi_r + \varphi_s$, $\varphi_{rs} = \varphi_r \circ \varphi_s$, e $\varphi_1 = 1_{End(M)}$, segue que μ é uma ação linear de R em M.

■

Definição 2.0.16. *Dizemos que N é um submódulo de M, quando N é um subgrupo de M e é fechado sob multiplicação de elementos de R.*

Exemplo 2.0.17. *(i) Um anel R é um R-módulo, quando se considera a ação como sendo a operação de multiplicação do anel;*

(ii) Os ideais de um anel R, são os submódulos de R, quando R é visto como módulo;

(iii) Os $\mathbb{Z}$-módulos são precisamente os grupos abelianos;

(iv) Módulos sobre um corpo R, são espaços vetoriais. Note que μ, neste caso, é uma transformação linear.

(v)

Definição 2.0.18. *Sejam R um anel com 1 não necessariamente comutativo, e G um grupo multiplicativo, definimos RG como o conjunto de todas as combinações lineares formais $\sum_{g \in G} r_g g$, em que $r_g \in R$, com $r_g = 0$ quase sempre.*

Podemos tornar RG num anel, o qual chamamos de anel de grupo de G sobre R, definindo operações de soma e multiplicação por:

(i) $\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g$; *e*

(ii) $\sum_{g \in G} r_g g . \sum_{h \in G} s_h h = \sum_{g \in G} \sum_{h \in G} r_g s_h gh = \sum_{x \in G} c_x x$, *em que* $c_x = \sum_{gh = x} r_g s_h$.

Podemos fornecer a RG uma estrutura de R-módulo (à esquerda), definindo uma multiplicação escalar para cada $\lambda \in R$ por

$$\lambda(\sum_{g\in G} r_g g) \stackrel{def}{=} \sum_{g\in G} (\lambda r_g)g.$$

Assim, RG é um R-módulo. Em particular, quando R é um anel comutativo, RG é uma álgebra sobre R, chamamos assim RG de álgebra de grupo de G sobre R. Como exemplo, temos o anel de grupo integral $\mathbb{Z}G$, que é uma álgebra de grupo.

Definição 2.0.19. *Considere que M e N sejam R-módulos. Uma aplicação $f : M \longrightarrow N$ é um homomorfismo de R-módulos quando,*

$$f(m+n) = f(m) + f(n),$$

$$f(rm) = rf(m), \forall r \in R, \forall m, n \in M$$

.

Definição 2.0.20. *Seja $f : M \longrightarrow N$ um homomorfismo de R-módulos, definimos por $ker(f) = \{m \in M \mid f(m) = 0\}$, e $Im(f) = \{f(m) \mid m \in M\}$, o núcleo e a imagem de f, respectivamente.*

Proposição 2.0.21. *Se $f : M \longrightarrow N$ é um homomorfismo de R-módulos, então $Ker(f)$ é um submódulo de M, e $Im(f)$ é um submódulo de N.*

Demonstração: Sejam $m, n \in Ker(f)$, então $f(m-n) = f(m) - f(n) = 0 - 0 = 0$, daí $m - n \in Ker(f)$, e se $r \in R$, então $f(rm) = rf(m) = r.0 = 0$, daí $rm \in Ker(f)$, portanto $Ker(f)$ é um R-submódulo de M. Como M é um R-módulo, temos que $m - n, rm \in M$, daí $f(m) - f(n) = f(m-n) \in Im(f)$, e $rf(m) = f(rm) \in Im(f)$, deste modo $Im(f)$ é um R-submódulo de N.

■

Proposição 2.0.22. *Se M' é um R-submódulo de M, então o grupo quociente M/M' é um R-módulo com multiplicação escalar(ação) dada por $r(m + M') \stackrel{def}{=} rm + M'$.*

Demonstração: Como M é um R-módulo, existe uma aplicação μ dada por $\mu(r, m) = rm$, a qual fornece uma ação linear de R em M, deste modo a aplicação induzida $\bar{\mu} : R \longrightarrow M/M'$ definida por $\bar{\mu}(r, m + M') = rm + M'$ descreve uma ação linear de R em M/M', logo M/M' é um R-módulo.

■

Definição 2.0.23. *O R-módulo M/M' é chamado de módulo quociente sobre R, ou R-módulo quociente.*

Teorema 2.0.24 (1º Teorema do Isomorfismo)**.** *Seja $f : M \longrightarrow N$ um homomorfismo de R-módulos, então*

$$M/Ker(f) \cong Im(f).$$

Demonstração: Defina $\bar{f} : M/ker(f) \longrightarrow Im(f)$ por $\bar{f}(m + Ker(f)) = f(m)$, temos que:

- $\bar{f}$ está bem definido e é injetivo:
  Temos que $m+Ker(f) = n+Ker(f)$ em $M/Ker(f)$ se, e somente se, $m-n \in Ker(f)$ se, e somente se, $f(m-n) = 0$ se, e somente se, $f(m) = f(n)$ se, e somente se, $\bar{f}(m + Ker(f)) = \bar{f}(n + Ker(f))$;

- $\bar{f}$ é um R-homomorfismo de módulos:
  De fato, $\bar{f}((m + Ker(f)) + (n + Ker(f))) = \bar{f}(m + n + Ker(f)) = f(m + n) = f(m)+f(n) = \bar{f}(m+Ker(f))+\bar{f}(n+Ker(f))$, e $\bar{f}(r(m+ker(f))) = \bar{f}(rm+Ker(f)) = f(rm) = rf(m) = r\bar{f}(m + Ker(f))$; e

- f é sobrejetor:
  Com efeito, se $y \in Im(f)$, então existe $m \in M$, tal que $f(m) = y$, logo existe $m + Ker(f) \in M/ker(f)$, tal que $\bar{f}(m + ker(f)) = f(m) = y$.

Portanto $\bar{f}$ é um R-isomorfismo de módulos, daí $M/Ker(f) \cong Im(f)$.

■

Teorema 2.0.25 (2º Teorema do Isomorfismo)**.** *Se $L \supseteq M \supseteq N$ são R-módulos, então*

$$(L/N)/(M/N) \cong L/M.$$

Demonstração: Defina $f : L/N \longrightarrow L/M$ por $f(x + N) = x + M$, temos que f está bem definido, pois se $x + N = y + N$, segue que $x - y \in N$, então já que $N \subseteq M$, segue que $x - y \in M$, daí $f(x + N) = f(y + N)$. Agora note que $Ker(f) = M/N$, e $Im(f) = L/M$, portanto pelo Teorema 2.0.24, obtemos que $(L/N)/(M/N) \cong L/M$.

■

Teorema 2.0.26 (3º Teorema do Isomorfismo)**.** *Sejam K e L submódulos de M, então*

$$(K+L)/K \cong L/(K \cap L).$$

Demonstração: Defina $f : L \longrightarrow (K+L)/K$ por $f(x) = x + K$, temos que f é um epimorfismo, cujo núcleo é $K \cap L$, logo pelo Teorema 2.0.24, segue que $(K+L)/K \cong L/(K \cap L)$.

■

Definição 2.0.27. *Sejam I um ideal de R, e M um R-módulo, definimos IM como sendo o conjunto formado por todas somas finitas da forma $\sum r_i m_i$, em que $r_i \in I$, e $m_i \in M$.*

Proposição 2.0.28. *IM é um R-submódulo de M.*

Demonstração: Sejam $x = \sum_{i=1}^{t} r_i m_i$, $y = \sum_{j=1}^{u} s_j m'_j \in IM$, definindo $s_j = -r_{t+j}$, e $m'_j = -m_{t+j}$, segue que $x - y = \sum_{i=1}^{t+u} r_i m_i \in IM$. Temos para cada $r \in R$ que, $rx = \sum_{i=1}^{t} r(r_i m_i) = \sum_{i=1}^{t} (rr_i)m_i$, como I é um ideal de R, segue que cada $rr_i \in I$, logo $rx \in IM$.

■

Observação 2.0.29. *A definição de IN pode ser estendida para quaisquer subconjuntos não-vazios I de R, e N de M, no entanto, podemos ter que IN não é submódulo de M. Agora, note que IN é um submódulo de M para o caso em que I é fechado sob subtração, e N é um submódulo de M.*

Definição 2.0.30. *Se N, P são submódulos de M, definimos $(N : P)$, como sendo o conjunto de todos elementos, $r \in R$, tais que $rP \subseteq N$.*

Proposição 2.0.31. *$(N : P)$ é um ideal de R.*

Demonstração: Sejam $s, t \in (N : P)$, e $r \in R$, então $sP, tP \subseteq N$, mas como N é um R-submódulo, segue que $(s-t)P \subseteq N$, e $rsP \subseteq N$, logo $s - t, rs \in (N : P)$, portanto $(N : P)$ é um ideal de R.

■

Definição 2.0.32. *$(0 : M) = Ann(M)$ é chamado de anulador de M.*

Proposição 2.0.33. *Se I é um ideal de R contido em $Ann(M)$, então M tem uma estrutura de R/I-módulo.*

Demonstração: Defina $\mu : R/I \times M \longrightarrow M$ por $\mu(r+I, m) = rm$, temos que μ é uma aplicação bem definida, pois se $r - s \in I$, então já que $I \subseteq Ann(M)$, segue que $(r-s)m = 0$, para todo $m \in M$. Daí $rm = sm$, para todo $m \in M$. Agora note, que R/I age linearmente em M, pois R também o age. Portanto, M é um R/I-módulo.

■

Definição 2.0.34. *Um R-módulo M é chamado fiel, quando $Ann(M) = 0$.*

Observação 2.0.35. *Se $Ann(M) = I$, então M é fiel como um R/I-módulo. De fato, $Ann_{R/I}(M) = I = \bar{0}$.*

Definição 2.0.36. *Um R-módulo M é chamado livre, quando é isomorfo a um R-módulo da forma $\bigoplus_{\lambda\in\Lambda} M_\lambda$, em que cada M_λ é isomorfo a R, como R-módulos.*

Definição 2.0.37. *Seja X um subconjunto de um R-módulo M. Definimos o submódulo de M gerado por X, denotado por $\langle X\rangle$, como sendo $\bigcap_{\lambda\in\Lambda} M_\lambda$, em que $\{M_\lambda \mid \lambda \in \Lambda\}$ é a família de todos submódulos de M que contêm X.*

Teorema 2.0.38. *Seja X um subconjunto de um módulo M. Se $X = \emptyset$, então $\langle X\rangle = 0$, caso contrário, $\langle X\rangle = \{\sum r_i x_i \mid r_i \in R, x_i \in X\}$.*

Demonstração: Se $X = \emptyset$, então já que (0) contém X, segue que $\langle X\rangle = \bigcap_{\lambda\in\Lambda} M_\lambda \subseteq (0)$, logo $\langle X\rangle = (0)$. Suponha $\langle X\rangle \neq \emptyset$, e defina $S = \{\sum r_i x_i \mid r_i \in R, x_i \in X\}$. Temos que $1 \in R$, logo $1.x = x \in S$, para todo $x \in X$, logo $X \subseteq S$, além disso, note que S é um submódulo de M, daí $\langle X\rangle \subseteq S$. Por outro lado, mostremos que se M' é um submódulo de M contendo X, então $S \subseteq M'$, de fato, como M' é um R-módulo, cada elemento da forma $\sum r_i x_i$ pertence a M', logo S está contido em todo submódulo de M que contém X, daí $S \subseteq \langle X\rangle$.

■

Definição 2.0.39. *Um R-módulo M é chamado finitamente gerado, quando é gerado por um subconjunto X finito de M. Em particular, quando existe $x \in M$, tal que $M = Rx$, chamamos M de R-módulo cíclico.*

Observação 2.0.40. *Se um R-módulo M é finitamente gerado, então pelo Teorema 2.0.38, segue que existe uma quantidade finita de elementos $x_1, \ldots, x_k$ em M, tais que $M = Rx_1 + \ldots + Rx_k$.*

Proposição 2.0.41. *Um módulo M é cíclico se, e somente se, $M \cong R/I$ para algum ideal I de R. Caso $M = \langle x \rangle$, então $I = \{r \in R \mid rx = 0\}$.*

Demonstração: Suponha que M seja cíclico, então existe $x \in M$, tal que $M = \langle x \rangle$, daí $M = Rx$, logo o R-homomorfismo $f : R \longrightarrow M$ dado por $f(r) = rx$ é um epimorfismo, e cujo núcleo é $I = Ker(f) = \{r \in R \mid rx = 0\} = Ann(M)$, portanto pelo 1º Teorema do Isomorfismo 2.0.24, segue que $M \cong R/I$. Reciprocamente, se $M \cong R/I$, então existe um isomorfismo $f : R/I \longrightarrow M$, já que R/I é cíclico gerado por $1 + I$, segue que M é cíclico gerado por $f(1 + I)$.

■

Notação: Denotamos por R^k, a soma direta de k cópias de R.

Proposição 2.0.42. *M é um R-módulo finitamente gerado se, e somente se, M é isomorfo a um quociente de R^k para algum $k \in \mathbb{N}$.*

Demonstração: Suponha que M seja um R-módulo finitamente gerado, então existe uma quantidade finita de elementos $x_1, \ldots, x_k$ de M, tais que $M = \sum_{i=1}^{k} Rx_i$, considere o R-homomorfismo $f : R^n \longrightarrow M$, dado por $f(r_1, \ldots, r_k) = \sum_{i=1}^{k} r_i x_i$, note que f é epimorfismo, daí $M \cong R^k/Ker(f)$. Reciprocamente, se $M \cong R^k/I$, então existe um epimorfismo f de R^k sobre M, com núcleo I, note que os vetores $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ com única coordenada não nula igual 1 na i-ésima coordenada, geram R^k, daí $\{f(e_i) \mid i = 1, \ldots, k\}$ gera M, logo M é finitamente gerado.

■

Teorema 2.0.43 (**Teorema Chinês dos Restos para Módulos.**). *Sejam M um R-módulo, e $I_1, \ldots, I_n$ ideais de R dois a dois comaximais. Então a aplicação $\varphi : M \longrightarrow \bigoplus_{i=1}^{n} M/I_iM$ definida por*

$$\varphi(m) = \{m + I_1M, \ldots, m + I_nM\}$$

é um epimorfismo, cujo núcleo é $\bigcap_{i=1}^{n} I_iM$.

Demonstração: Se $n = 1$, então temos o epimorfismo canônico $M \longrightarrow M/I_1M$. Suponha $n > 1$. Seja $y = (x_1 + I_1M, \ldots, x_n + I_nM) \in \bigoplus_{i=1}^{n} M/I_iM$, mostremos que existe $m \in M$, tal que $\varphi(m) = y$. Para cada $i = 1, \ldots, n$ fixo, defina $I_i' = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} I_j$, note que I_i e I_i' são comaximais, logo existem $u_i \in I_i$, e $v_i \in I_i'$, tais que $u_i + v_i = 1$, deste modo para cada $j \neq i$, temos que:

$$\begin{cases} v_i \equiv 1 \pmod{I_i} \\ v_i \equiv 0 \pmod{I_j} \end{cases}$$

uma vez que, pela Proposição 1.1.42 (i), temos que $I_i' = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} I_j = \bigcap_{\substack{1 \leq j \leq n \\ j \neq i}} I_j$, e daí v_i pertence a todo I_j, portanto

$$\begin{cases} v_i x_i \equiv x_i \pmod{I_i} \\ v_i x_i \equiv 0 \pmod{I_j} \end{cases}$$

de modo que $\varphi(\sum_{i=1}^{n} v_i x_i) = y$. Portanto, φ é um epimorfismo, cujo núcleo é

$$Ker(f) = \{m \in M \mid (m + I_1M, \ldots, m + I_nM) = (I_1M, \ldots, I_nM)\} = \bigcap_{i=1}^{n} I_iM.$$

■

2.1 Categorias e Funtores

Embora consideramos o anel R comutativo com 1, vamos fazer referências a módulos à direita e à esquerda, com intuito de apresentar as condições dos resultados em modo mais forte.

Definição 2.1.1. *Uma **categoria** $\mathfrak{C}$ consiste de uma classe de **objetos**, denotada por $obj\mathfrak{C}$; conjuntos dois a dois disjuntos, $Hom_{\mathfrak{C}}(A, B)$, de **morfismos** para cada par ordenado de objetos (A, B) ; e **composições** $Hom_{\mathfrak{C}}(A, B) \times Hom_{\mathfrak{C}}(B, C)$, definidas por $(f, g) \mapsto gf$, tais que:*

(i) para cada objeto A, existe um morfismo identidade $1_A \in Hom_{\mathfrak{C}}(A, A)$, tal que $f1_A = f$ para todo $f \in Hom_{\mathfrak{C}}(A, B)$, e $1_Ag = g$, para todo $g \in Hom_{\mathfrak{C}}(C, A)$; e

(ii) a associatividade de composições é satisfeita sempre que possível, ou seja, se $f \in Hom_{\mathfrak{C}}(A, B)$, $g \in Hom_{\mathfrak{C}}(B, C)$, e $h \in Hom_{\mathfrak{C}}(C, D)$, então $h(gf) = (hg)f$.

Exemplo 2.1.2. *(i)* $\mathfrak{C} = \boldsymbol{Conjuntos}$*, em que* $obj\mathfrak{C}$*, são conjuntos; os morfismos, são funções; e as composições, são composições usuais de funções;*

(ii) $\mathfrak{C} = {}_R\mathfrak{M}$*, em que* R *é um anel com* 1*, os objetos são os* R*-módulos à esquerda; os morfismos são* R*-homomorfismos; e as composições, são composições usuais de* R*-homomorfismos. Analogamente, definimos* $\mathfrak{C} = \mathfrak{M}_R$*, categoria dos* R*-módulos à direita.*

(iii) A categoria dos grupos abelianos, $\boldsymbol{Ab}$*, coincide com a categoria* ${}_{\mathbb{Z}}\mathfrak{M}$*, a qual coincide com* $\mathfrak{M}_{\mathbb{Z}}$*, uma vez que* $\mathbb{Z}$ *é um anel comutativo.*

Definição 2.1.3. *Sejam* $\mathfrak{C}$ *e* $\mathfrak{D}$ *categorias. Definimos um* ***functor*** *ou um* ***funtor covariante*** *como uma função*

$$F : \mathfrak{C} \longrightarrow \mathfrak{D},$$

tal que:

(i) se $A \in obj\mathfrak{C}$*, então* $FA \in obj\mathfrak{D}$*;*

(ii) se $f : A \longrightarrow B$ *é um morfismo em* $\mathfrak{C}$*, então* $Ff : FA \longrightarrow FB$ *é um morfismo em* $\mathfrak{D}$*;*

(iii) se $A \xrightarrow{f} B \xrightarrow{g} C$ *são morfismos em* $\mathfrak{C}$*, então*

$$F(gf) = FgFf;$$

(iv) para cada $A \in obj\mathfrak{C}$*,* $F(1_A) = 1_{FA}$*.*

Exemplo 2.1.4. *(i) O funtor* $F : \mathfrak{C} \longrightarrow \mathfrak{C}$ *definido por* $FA = A$*, e* $Ff = f$*, é chamado de* ***funtor identidade****;*

(ii) Os funtores $F = Hom_R(A, \bullet) : \mathfrak{C} \longrightarrow \boldsymbol{Conjuntos}$*, dados para cada* $A \in \mathfrak{C}$ *fixo, por* $FC = Hom(A, C)$*, e* $Ff : Hom(A, C) \longrightarrow Hom(A, C')$ *por* $g \mapsto fg$ *sempre que* $f : C \longrightarrow C'$ *é um morfismo em* $\mathfrak{C}$*, é chamado de* ***funtor Hom****. Denotamô-lo por* f_**. Note que, em particular, se* $\mathfrak{C} = {}_R\mathfrak{M}$*, então* f_* *tem imagem na categoria* $\boldsymbol{Ab}$*, o mesmo ocorre se* $\mathfrak{C} = \mathfrak{M}_R$*;*

(iii) Se $A \in \mathfrak{M}_R$*, a função* $F : {}_R\mathfrak{M} \longrightarrow \boldsymbol{Ab}$*, definida por*

$$FB = A \otimes_R B,$$

tal que $Ff = 1_A \otimes f$*, sempre que* $f : B \longrightarrow B'$ *é um* R*-homomorfismo de* R*-módulos à esquerda, é um funtor. Denotamô-lo por* $A\otimes_R$*. Analogamente para cada* $B \in {}_R\mathfrak{M}$*, definimos o funtor* $\otimes_R B : \mathfrak{M}_R \longrightarrow \boldsymbol{Ab}$*. (Vide a seção Produto Tensorial)*

Observação 2.1.5. *Denotamos por $f \otimes g$ a aplicação $A \otimes_R B \longrightarrow A' \otimes_R B'$, definida por $a \otimes b \mapsto fa \otimes gb$.*

*(iv) Seja $D \in obj\mathfrak{D}$ um objeto fixo. O funtor $|| : \mathfrak{C} \longrightarrow \mathfrak{D}$ dado por $|C| = D$ para cada $C \in \mathfrak{C}$, e por $|f| = 1_D$ para cada morfismo $f \in \mathfrak{C}$, é chamado de **funtor constante**.*

Definição 2.1.6. *Sejam $\mathfrak{C}$ e $\mathfrak{D}$ categorias. Definimos um **funtor contravariante** como uma função*

$$F : \mathfrak{C} \longrightarrow \mathfrak{D},$$

tal que:

(i) se $A \in obj\mathfrak{C}$, então $FA \in obj\mathfrak{D}$;

(ii) se $f : A \longrightarrow B$ é um morfismo em $\mathfrak{C}$, então $Ff : FB \longrightarrow FA$ é um morfismo em $\mathfrak{D}$;

(iii) se $A \xrightarrow{f} B \xrightarrow{g} C$ são morfismos em $\mathfrak{C}$, então

$$F(gf) = FfFg;$$

(iv) para cada $A \in obj\mathfrak{C}$, $F(1_A) = 1_{FA}$.

Exemplo 2.1.7. *Fixado um objeto $B \in \mathfrak{C}$, podemos definir um funtor*

$$F = Hom(\bullet, B) : \mathfrak{C} \longrightarrow \textbf{\textit{Conjuntos}},$$

por $FA = Hom(A, B)$, e $Ff : Hom(A', B) \longrightarrow Hom(A, B)$ por $g \mapsto gf$, sempre que $f : A \longrightarrow A'$ é um morfismo em $\mathfrak{C}$. Denotamô-lo por f^*.

Definição 2.1.8. *Duas aplicações*

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

são exatas em M, quando $Im(f) = Ker(g)$. Analogamente, dizemos que uma sequência de aplicações

$$\ldots \longrightarrow M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \longrightarrow \ldots$$

é exata, quando cada par adjacente de aplicações é exato.

Proposição 2.1.9. *Se*

$$0 \longrightarrow M' \xrightarrow{f} M$$

é exata, então f é uma aplicação injetora.

Demonstração: Temos que $Im(0 \longrightarrow M') = 0$, mas como a sequência é exata, segue que $Im(0 \longrightarrow M') = Ker(f)$, portanto $Ker(f) = 0$, daí f é uma aplicação injetora.

■

Proposição 2.1.10. *Se*

$$M \xrightarrow{g} M'' \longrightarrow 0$$

é exata, então g é sobrejetora.

Demonstração: Temos que $Ker(M'' \longrightarrow 0) = M''$, mas como a sequência é exata, temos que $Im(g) = Ker(M'' \longrightarrow 0)$, logo $Im(g) = M''$, portanto g é uma aplicação sobrejetora.

■

Corolário 2.1.11. *Se*

$$0 \longrightarrow M \xrightarrow{f} M' \longrightarrow 0$$

é exata, então f é bijetora.

Demonstração: Pelas proposições 2.1.9, e 2.1.10, segue que f é injetora e sobrejetora, respectivamente, logo f é bijetora.

■

Proposição 2.1.12. *Se*

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

é exata, então $M' \cong iM'$, e $M/iM' \cong M''$.

Demonstração: Pela Proposição 2.1.9, $Ker(i) = 0$, mas pelo 1º Teorema de Isomorfismos 2.0.24, $i(M') \cong M'/Ker(i) \cong M'/(0) \cong M'$, logo $i(M') \cong M'$. Agora, pela Proposição 2.1.10, $Im(p) = M''$, e como a sequência é exata, $Ker(p) = Im(i) = iM'$, mas pelo Teorema 2.0.24, $Im(p) \cong M/Ker(p)$, portanto $M'' \cong M/iM'$.

■

Definição 2.1.13. *Sequências exatas da forma*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

são chamadas sequências exatas curtas.

Definição 2.1.14. *Uma sequência exata curta*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

é chamada ***cindível****, quando existe uma aplicação* $h : C \longrightarrow B$*, tal que* $gh = 1_C$*.*

Definição 2.1.15. *Um funtor* F *é dito* ***exato à esquerda****, quando sempre que*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$$

é exata, tem-se que

$$0 \longrightarrow FA \xrightarrow{Ff} FB \xrightarrow{Fg} FC$$

é exata. Analogamente, um funtor F *é* ***exato à direita****, quando sempre que*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

é exata, tem-se que

$$FA \xrightarrow{Ff} FB \xrightarrow{Fg} C \longrightarrow 0$$

é exata.

Definição 2.1.16. *Um funtor é dito* ***exato****, quando é exato à direita e à esquerda.*

Proposição 2.1.17. *Funtores exatos à esquerda preservam monomorfismos, e funtores exatos à direita; epimorfismos.*

Demonstração: De fato, se F é um funtor exato à esquerda, então se $A \xrightarrow{f} B$ é injetiva, então $FA \xrightarrow{Ff} FB$ é injetiva, analogamente se F é exato à direita e $B \xrightarrow{g} C$ é sobrejetor, então $FB \xrightarrow{Fg} FC$ é sobrejetor.

■

Proposição 2.1.18. *O funtor* $\mathrm{Hom}(\mathrm{M}, \bullet)$ *é exato à esquerda para cada* R*-módulo* M*.*

Demonstração: Seja

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

uma sequência exata à esquerda, mostremos que a sequência

$$0 \longrightarrow Hom(M, A) \xrightarrow{F\alpha} Hom(M, B) \xrightarrow{F\beta} Hom(M, C)$$

é exata à esquerda. Basta mostrarmos que $F\alpha$ é injetiva, e que $Im(F\alpha) = Ker(F\beta)$.

- $F\alpha$ é injetivo:
  Seja $f \in Ker(F\alpha)$, então $F\alpha(f) = 0$, daí pela definição de F, segue que $\alpha \circ f = 0$, logo $\alpha(f(m)) = 0$, para todo $m \in M$, mas como α é injetor, temos que $f(m) = 0$, para todo $m \in M$, portanto $f = 0$.

- $Im(F\alpha) = Ker(F\beta)$:
  Seja $g \in Im(F\alpha)$, então existe $f \in Hom(M, A)$, tal que $F\alpha(f) = g$, daí $\alpha f = g$. Mas $Im(\alpha) = Ker(\beta)$, de modo que $\beta\alpha = 0$, assim $F\beta(g) = \beta g = \beta(\alpha f) = (\beta\alpha)f = 0$, portanto $F\beta(g) = 0$, logo $g \in Ker(\beta)$. Reciprocamente, suponha que $g \in Ker(\beta)$, então $\beta g = 0$, logo $\beta(g(m)) = 0$, para todo $m \in M$, de modo que $g(m) \in Ker(\beta)$ para todo $m \in M$, mas como $Ker(\beta) = Im(\alpha)$, segue que $g(m) \in Im(\alpha)$, logo existe $a \in A$, tal que $\alpha(a) = g(m)$, note que tal a é único, pois α é injetivo, assim podemos definir uma aplicação constante $f \in Hom(M, A)$ por $f(m) = a$, deste modo, $\alpha f(m) = \alpha(a) = g(m)$, para todo $m \in M$, logo $\alpha f = g$, ou seja, $(F\alpha)f = g$, consequentemente $g \in Im(F\alpha)$.

■

Definição 2.1.19. *Definimos o módulo dual de um R-módulo M como sendo o R-módulo $Hom(M, R)$, o qual indicaremos por M^*.*

Proposição 2.1.20. *Se R é um anel comutativo com 1, então $R^* = \mathrm{Hom}_R(R, R) \cong R$.*

Demonstração: De fato, a aplicação

$$\psi : R^* \longrightarrow R,$$

definida por $f \mapsto f(1)$ é um R-isomorfismo, cujo inverso é o homomorfismo

$$\varphi : R \longrightarrow R^*,$$

definido por $\varphi(r) : t \mapsto rt$.

■

Teorema 2.1.21. *Considere que M e $\{M_j : j \in J\}$ sejam módulos dados. Então $M \cong \bigoplus_{j\in J} M_j$ se, e somente se, existem aplicações $\lambda_j : M_j \longrightarrow M$, tais que, dado qualquer módulo X e quaisquer aplicações $f_j : M_j \longrightarrow X$, existe uma única aplicação $\varphi : M \longrightarrow X$ com $\varphi \circ \lambda_j = f_j$, para todo $j \in J$.*

Demonstração: [14], p.29.

■

Teorema 2.1.22. *Se λ_j é a j-ésima injeção $M_j \longrightarrow \bigoplus_{j\in J} M_j$, e N é um módulo, então a aplicação*

$$\theta : \mathrm{Hom}(\bigoplus_{j\in J} M_j, N) \longrightarrow \prod_{j\in J} \mathrm{Hom}(M_j, N)$$

dada por $\varphi \mapsto (\varphi\lambda_j)$ é um isomorfismo.

Demonstração: [14], p.30.

■

Observação 2.1.23. *Em particular, obtemos da Proposição 2.1.22 que,* $\mathrm{Hom}_R(M \oplus N, R) \cong \mathrm{Hom}_R(M, R) \oplus \mathrm{Hom}_R(N, R)$.

Proposição 2.1.24. *Sejam M um R-módulo à direita e $\{N_j : j \in J\}$ uma família de R-módulos à esquerda. Então, a aplicação $\theta : M \otimes_R \prod_{j\in J} N_j \longrightarrow \bigoplus_{j\in J}(M \otimes_R N_j)$, definida por $m \otimes (n_j) \mapsto (m \otimes n_j)$ é um isomorfismo. (Vide a seção Produto Tensorial)*

Demonstração: [14], p.33.

■

Observação 2.1.25. *Em particular, temos que $M \otimes (N \oplus P) \cong (M \otimes N) \oplus (M \otimes P)$.*

2.2 Produto tensorial

Definição 2.2.1. *Considere que R seja um anel com 1. Se A é um R-módulo à direita, B um R-módulo à esquerda, e G um grupo abeliano aditivo, então uma função R-biaditiva é uma função*

$$f : A \times B \longrightarrow G,$$

tal que para todos $a, a' \in A$, para todos $b, b' \in B$, $r \in R$.

(i) $f(a+a',b) = f(a,b) + f(a',b)$;

(ii) $f(a,b+b') = f(a,b) + f(a,b')$; *e*

(iii) $f(ar,b) = f(a,rb)$.

Observação 2.2.2. *Para R comutativo (nosso caso), chamamos f de função R-bilinear, quando f é R-biaditiva e $rf(a,b) = f(ra,b) = f(a,rb)$.*

Definição 2.2.3. *O produto tensorial entre $A \in \mathfrak{M}_R$, e $B \in {}_R\mathfrak{M}$ é um grupo abeliano $A \otimes B$ e uma função R-biaditiva h, tal que para cada grupo abeliano G e cada função R-biaditiva f, existe um único homomorfismo f' com $f = f' \circ h$, isto é, o diagrama abaixo comuta:*

$$\begin{array}{ccc} A \times B & \xrightarrow{h} & A \otimes B \\ & \searrow^{f} & \swarrow_{f'} \\ & G & \end{array}$$

Teorema 2.2.4. *O produto tensorial tensorial de um R-módulo à direita A e um R-módulo à esquerda B existe.*

Demonstração: Considere que F seja o grupo abeliano livre com base $A \times B$. Defina S como sendo o subgrupo de F gerado pelos elementos das seguintes formas: $(a+a',b)-(a,b)-(a',b)$, $(a,b+b')-(a,b)-(a,b')$, e $(ar,b)-(a,rb)$. Denote o grupo quociente F/S por $A \otimes_R B$, e cada elemento $(a,b)+S \in F/S$ por $a \otimes b$. Defina uma aplicação $h : A \times B \longrightarrow A \otimes_R B$ por $h((a,b)) = a \otimes b$, deste modo h é R-biaditiva, pois

$$\begin{cases} (a+a') \otimes b - a \otimes b - a' \otimes b = S = \bar{0} \\ a \otimes (b+b') - a \otimes b - a \otimes b' = S = \bar{0} \\ ar \otimes b - a \otimes rb = S = \bar{0} \end{cases}$$

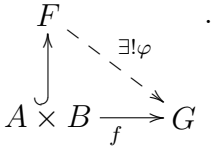
Logo,

$$\begin{cases} (a+a') \otimes b = a \otimes b + a' \otimes b \\ a \otimes (b+b') = a \otimes b + a \otimes b' \\ ar \otimes b = a \otimes rb \end{cases}$$

Daí,

$$\begin{cases} h(a+a',b) = h(a,b) + h(a',b) \\ h(a,b+b') = h(a,b) + h(a,b') \\ h(ar,b) = h(a,rb) \end{cases}$$

Agora seja G um grupo abeliano, e $f : A \times B \longrightarrow G$ uma função R-biaditiva. Já que F é livre com base $A \times B$, existe um único homomorfismo $\varphi : F \longrightarrow G$ estendendo f, isto é, $\varphi(a, b) = f(a, b)$, de acordo com o diagrama comutativo abaixo:

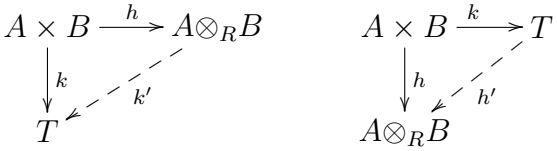


Note que cada gerador de S se anula por φ, pois f é R-biaditiva, assim $S \subseteq Ker(\varphi)$, daí segue que φ induz um homomorfismo $\overline{f} : A \otimes_R B \longrightarrow G$ dado por $\overline{f}(a \otimes b) = f(a, b)$, deste modo $\overline{f}(h(a, b)) = f(a, b)$ para todo $(a, b) \in A \times B$, logo $\overline{f} \circ h = f$. Temos que $\overline{f}$ é único com essa propriedade, de fato se $g : A \otimes_R B \longrightarrow G$ é um homomorfismo, tal que $g \circ h = f$, então para cada $(a, b) \in A \times B$, temos que $(g \circ h)(a, b) = f(a, b)$, logo $g(a \otimes b) = f(a, b) = \overline{f}(a \otimes b)$, portanto $g(a \otimes b) = \overline{f}(a \otimes b)$, como os elementos $a \otimes b$ geram $A \otimes_R B$, segue que $\overline{f} = g$.

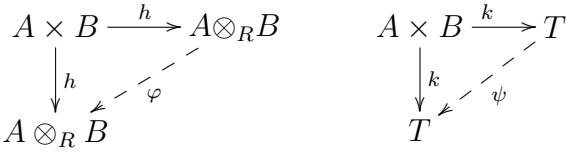
■

Proposição 2.2.5. *Quaisquer dois produtos tensoriais entre A e B são isomorfos.*

Demonstração: Considere que $A \otimes_R B$ e T sejam produtos tensoriais entre A e B, cujas funções R-biaditivas são $h : A \times B \longrightarrow A \otimes_R B$, e $k : A \times B \longrightarrow T$, respectivamente. Pela definição de produto tensorial, segue que existem homomorfismos k' e h', tais que os diagramas abaixo comutam:



Logo, $k = k'h$, e $h = h'k$, por outro lado, temos que existem φ e ψ, tais que os diagramas abaixo comutam:



Assim $h = \varphi h$, e $k = \psi k$, agora note que $h = h'k = (h'k')h$, e $k = k'h = (k'h')k$, logo pela unicidade de φ e ψ, segue que $h'k' = \varphi$, e $k'h' = \psi$, mas como $h = 1_{A \otimes_R B}h$, e $k = 1_T k$, temos novamente pela unicidade que, $h'k' = 1_{A \otimes_R B}$, e $k'h' = 1_T$, portanto k' é um isomorfismo, logo $A \otimes_R B \cong T$.

■

Teorema 2.2.6. *Se A é um R-módulo à direita, e B é um (RS)-bimódulo, então $A \otimes_R B$é um S-módulo à direita, em que*

$$(a \otimes b)s = a \otimes (bs).$$

Analogamente, se A é um (SR)-bimódulo, e B é um R-módulo à esquerda, então $A \otimes_R B$é um S-módulo à esquerda, em que

$$s(a \otimes b) = (sa) \otimes b.$$

Demonstração: Mostremos a primeira afirmação, a segunda é análoga. Para cada $s \in S$ fixado, temos que a função $\mu_s : B \longrightarrow B$ definida por $b \mapsto bs$ é um R-homomorfismo de módulos, uma vez que B é um RS-bimódulo. Agora, considere o funtor $F = A \otimes_R$, note que $F(\mu_s) : A \otimes_R B \longrightarrow A \otimes_R B$ é um homomorfismo de grupos, em que $F(\mu_s) = 1_A \otimes \mu_s : a \otimes b \mapsto a \otimes (bs)$. Logo das propriedades de homomorfismo, seguem os axiomas de S-módulo à direita para $A \otimes_R B$. Portanto, $A \otimes_R B$ é um S-módulo à direita.

■

Teorema 2.2.7. *Se R é um anel com 1, e B é um R-módulo à esquerda, então existe um R-isomorfismo $R \otimes_R B \xrightarrow{\sim} B$ com $r \otimes b \mapsto rb$.*

Demonstração: Como R é um $(R - R)$-bimódulo, e B é um R-módulo à esquerda, segue pelo Teorema 2.2.6 que $R \otimes_R B$ é um R-módulo à esquerda. Como B é um R-módulo, existe uma ação $f : R \times B \longrightarrow B$, dada por $f(r, b) = rb$, temos que f é R-biaditiva, logo pela definição de $R \otimes_R B$, existe um único homomorfismo $g : R \otimes_R B \longrightarrow B$, tal que $f = gh$, ou seja, o diagrama abaixo comuta:

$$\begin{array}{ccc} R \times B & \xrightarrow{h} & R \otimes_R B \\ & \searrow^{f} & \swarrow_{\exists! g} \\ & B & \end{array}$$

Deste modo, $gh(r, b) = f(r, b)$, daí $g(r \otimes b) = rb$. Mostremos que g é um isomorfismo, de fato a aplicação $g' : B \longrightarrow R \otimes_R B$ definida por $g'(b) = 1 \otimes b$ é um R-isomorfismo, cujo inverso é g. Portanto, $R \otimes_R B \cong B$ como R-módulos à esquerda, analogamente temos que $A \otimes_R R \cong A$ como R-módulos à direita.

■

Teorema 2.2.8. *Se R é um anel comutativo com 1, e A e B são R-módulos, então existe um R-isomorfismo $\varphi : A \otimes_R B \longrightarrow B \otimes_R A$, definido por $\varphi(a \otimes b) = b \otimes a$.*

Demonstração: Defina $f : A \times B \longrightarrow B \otimes_R A$, por $f(a,b) = b \otimes a$, deste modo f é R-biaditiva. Pela definição de $A \otimes_R B$, existe um único $\mathbb{Z}$-homomorfismo $f' : A \otimes_R B \longrightarrow B \otimes_R A$, tal que $f = f'h$,

$$\begin{array}{ccc} A \times B & \xrightarrow{h} & A \otimes_R B \\ \downarrow{\scriptstyle f} & \swarrow_{\exists! f'} & \\ B \otimes_R A & & \end{array}$$

Analogamente, para $g : B \times A \longrightarrow A \otimes_R B$ definida por $g(b,a) = a \otimes b$, temos que existe um único $\mathbb{Z}$-homomorfismo g', tal que $g = g'k$

$$\begin{array}{ccc} B \times A & \xrightarrow{k} & B \otimes_R A \\ \downarrow{\scriptstyle g} & \swarrow_{\exists! g'} & \\ A \otimes_R B & & \end{array}$$

Mostremos que $f'^{-1} = g'$, primeiramente note que $g(b,a) = g'k(b,a) = g'(b \otimes a)$, e $f(a,b) = f'h(a,b) = f'(a \otimes b)$, logo $g'f'(a \otimes b) = g'(f(a,b)) = g'(b \otimes a) = g(b,a) = a \otimes b$, e $f'g'(b \otimes a) = f'(g(b,a)) = f'(a \otimes b) = f(a,b) = b \otimes a$, portanto $f'^{-1} = g$, logo f' é um isomorfismo, daí $A \otimes_R B \cong B \otimes_R A$.

■

Corolário 2.2.9. *Se R é um anel comutativo com 1, então $A \otimes_R R \cong A$ como R-módulos, para cada R-módulo A.*

Demonstração: Temos que $A \otimes_R R \cong A$ como R-módulos à direita, e $R \otimes_R A \cong A$ como R-módulos à esquerda, mas como pelo Teorema 2.2.8, $A \otimes_R A \cong R \otimes_R A$, segue que $A \otimes_R R \cong A$ como R-módulos.

■

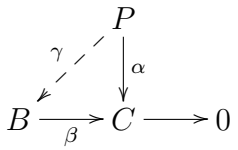
Proposição 2.2.10. *Considere que A, B, C sejam R-módulos. Então $(A \otimes_R B) \otimes_R C \cong A \otimes_R B \otimes_R C \cong A \otimes_R (B \otimes_R C)$.*

Demonstração: Construiremos homomorfismos $f : (A \otimes_R B) \otimes_R C \longrightarrow A \otimes_R B \otimes_R C$ e $g : A \otimes_R B \otimes_R C \longrightarrow (A \otimes_R B) \otimes_R C$ dados por $f((x \otimes y) \otimes z) = x \otimes y \otimes z$ e $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$, para todos $x \in A$, $y \in B$, $z \in C$. Inicialmente vamos construir f. Fixe um elemento $z \in C$. Deste modo, a aplicação $(x, y) \mapsto x \otimes y \otimes z$ é bilinear em $x \in A$ e $y \in B$, e induz um homomorfismo $f_z : A \otimes_R B \longrightarrow A \otimes_R B \otimes_R C$, tal que $f_z(x \otimes y) = x \otimes y \otimes z$. Agora, considere a aplicação $(t, z) \mapsto f_z(t)$ de $(A \otimes_R B) \times C$ em $A \otimes_R B \otimes_R C$. Note que tal aplicação é bilinear em t e z, logo pela propriedade universal na Definição 2.2.3, segue que existe um homomorfismo $f : (A \otimes_R B) \otimes_R C \longrightarrow A \otimes_R B \otimes_R C$, tal que $f((x \otimes y) \otimes z) = x \otimes y \otimes z$. Analogamente, construimos g considerando a aplicação bilinear $(x, y, z) \mapsto (x \otimes y) \otimes z$ de $A \times B \times C$ em $(A \otimes_R B) \otimes_R C$. Logo, existe um homomorfismo $g : A \otimes_R B \otimes_R C \longrightarrow (A \otimes_R B) \otimes_R C$, tal que $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$. Como $f \circ g$ e $g \circ f$ são identidades, segue que f e g são isomorfismos. Portanto, $(A \otimes_R B) \otimes_R C \cong A \otimes_R B \otimes_R C \cong A \otimes_R (B \otimes_R C)$.

■

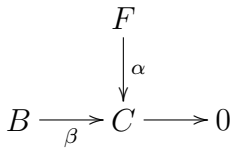
2.3 Módulos projetivos

Definição 2.3.1. *Um R-módulo P é chamado projetivo, quando dados qualquer R-epimorfismo de módulos $\beta : B \longrightarrow C$, e qualquer R-homomorfismo de módulos $\alpha : P \longrightarrow C$, existe um R-homomorfismo $\gamma : P \longrightarrow B$ com $\alpha = \beta\gamma$.*



Teorema 2.3.2. *Se F é um módulo livre, então F é um módulo projetivo.*

Demonstração: Seja F um módulo livre com base $X = \{x_i \mid i \in I\}$. Considere o diagrama



em que α é um homomorfismo, e β é um epimorfismo de módulos. Como β é sobrejetor, dado $\alpha(x_i) \in C$, existe $b_i \in B$, tal que $\beta(b_i) = \alpha(x_i)$. Agora, pelo axioma da escolha, existe

uma função $\psi : X \longrightarrow B$, tal que $\psi(x_i) = b_i$, para todo $i \in I$. No entanto, já que F é livre com base X, existe um único homomorfismo $\gamma : F \longrightarrow B$, tal que $\gamma(x_i) = \psi(x_i)$, para todo $i \in I$, ou seja o diagrama abaixo é comutativo:

$$\begin{array}{ccccc} X & \overset{i}{\hookrightarrow} & F & & \\ \downarrow{\scriptstyle \psi} & \swarrow{\scriptstyle \gamma} & \downarrow{\scriptstyle \alpha} & & \\ B & \underset{\beta}{\longrightarrow} & C & \longrightarrow & 0 \end{array}$$

Note que $\alpha = \beta\gamma$, pois para cada $x_i \in X$, temos que $\beta\gamma(x_i) = \beta\psi(x_i) = \beta(b_i) = \alpha(x_i)$. Portanto, já que existe um homomorfismo α tal que $\beta\gamma = \alpha$, segue que F é um módulo projetivo.

■

Teorema 2.3.3. *Um módulo P é projetivo se, e somente se, o funtor $F = Hom(P, \bullet)$ é exato.*

Demonstração:
($\Rightarrow$) Seja P um módulo projetivo. Pela Proposição 2.1.18, temos que o funtor $Hom(P, \bullet)$ é exato à esquerda, deste modo basta mostrarmos que $Hom(P, \bullet)$ é exato à direita, isto é, que preserva epimorfismos. Suponha que

$$B \xrightarrow{\beta} C \longrightarrow 0$$

seja uma sequência exata, queremos mostrar que

$$Hom(P, B) \overset{\beta_* = F\beta}{\longrightarrow} Hom(P, C) \longrightarrow 0$$

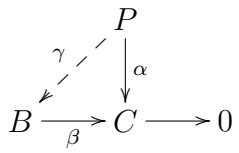
é exata, i.e, o homomorfismo $\beta_* : Hom(P, B) \longrightarrow Hom(P, C)$ definido por $\beta_*(f) = \beta f$ é sobrejetor. Com efeito, seja $g \in Hom(P, C)$, como β é um epimorfismo, e P é projetivo, segue que existe $f \in Hom(P, B)$ tal que $g = \beta f = \beta_*(f)$, logo β_* é sobrejetor.

$$\begin{array}{ccccc} & & P & & \\ & \swarrow{\scriptstyle f} & \downarrow{\scriptstyle g} & & \\ B & \underset{\beta}{\longrightarrow} & C & \longrightarrow & 0 \end{array}$$

($\Leftarrow$) Suponha que $Hom(P, \bullet)$ seja exato. Considere que $\beta : B \longrightarrow C$ seja um epimorfismo, e que $\alpha \in Hom(P, C)$. Por hipótese, temos que a sequência

$$Hom(P, B) \xrightarrow{\beta_*} Hom(P, C) \longrightarrow 0$$

é exata, logo $\beta_* : \gamma \mapsto \beta\gamma$ é epimorfismo, logo dado $\alpha \in Hom(P, C)$, existe $\gamma \in Hom(P, B)$, tal que $\beta_*(\gamma) = \alpha$, daí $\beta\gamma = \alpha$. Portanto, P é projetivo.



■

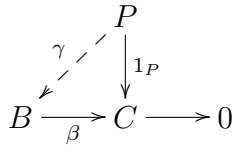
Lema 2.3.4. *Dados dois módulos A e B e um monomorfismo $i : A \longrightarrow B$. Então, A é um somando de B (ou seja, $B = iA \oplus C$ para algum submódulo C de B) se, e somente se, existe um homomorfismo de módulos $p : B \longrightarrow A$ com $pi = 1_A$.*

Demonstração: Suponha que A seja um somando de B, então existe C submódulo de B, tal que $B = iA \oplus C$, note que como i é injetor, podemos identificar A com iA. Defina $p : B \longrightarrow A$ por: $p(b) = b$, se $b \in A$, e $p(b) = 0$, caso contrário, i.e quando $b \in C$. Logo $p \circ i(a) = p(i(a)) = i(a) = 1_A(a) \in A$, portanto identificando A com iA, segue que $pi = 1_A$. Reciprocamente, suponha que exista um homomorfismo $p : B \longrightarrow A$, tal que $pi = 1_A$, seja $C = Ker(p)$, mostremos que $B = iA \oplus C$. De fato, se $b \in B$, então $b = i(p(b)) + [b - i(p(b)]$, note que $i(p(b)) \in i(A)$, e $b - i(p(b)) \in C = Ker(p)$, uma vez que $p(b - ip(b)) = p(b) - pi(p(b)) = p(b) - 1_A(p(b)) = 0$, logo $B = iA + C$. Por outro lado, $iA \cap C = 0$, pois se $x \in iA \cap C$, então $p(x) = 0$, mas como $x \in iA$, $x = i(a)$ para algum $a \in A$, deste modo $p(i(a)) = 0$, daí $1_A(a) = 0$, logo $a = 0$, consequentemente $i(a) = x = 0$. Portanto, $B = iA \oplus C$.

■

Teorema 2.3.5. *Se P é projetivo, e $\beta : B \longrightarrow P$ é um epimorfismo, então $B = Ker(\beta) \oplus P'$, em que $P' \cong P$.*

Demonstração: Como P é projetivo, existe um homomorfismo $\gamma \in Hom(P, B)$, tal que $1_P = \beta\gamma$:



note que γ é injetivo, pois se $\gamma(x) = \gamma(y)$, então $\beta\gamma(x) = \beta\gamma(y)$, daí $1_P(x) = 1_P(y)$, logo $x = y$. Portanto, como γ é injetivo, segue pelo Lema 2.3.4, que $B = \gamma(P) \oplus Ker(\beta)$, daí $B = P' \oplus Ker(\beta)$, em que $\gamma(P) = P' \cong P$.

■

Corolário 2.3.6. *Se A é um submódulo de B com B/A projetivo, então A é um somando direto de B. E cada sequência exata*

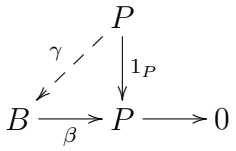
$$0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$$

com P projetivo, cinde.

Demonstração: Considere o epimorfismo canônico $\beta : B \longrightarrow B/A$, como $P = B/A$ é projetivo, segue pelo Teorema 2.3.5 que, $B = Ker(\beta) \oplus P'$, em que $P' \cong P$, no entanto $Ker(\beta) = A$, deste modo $B = A \oplus P'$, logo A é um somando direto de B. Agora, se

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} P \longrightarrow 0$$

é exata com P projetivo, então já que β é epimorfismo, segue que $B = Ker(\beta) \oplus P'$, em que $P \cong P'$, mas $A = Im(\alpha) = Ker(\beta)$, logo $B = A \oplus P'$, mas já que $\alpha : A \longrightarrow B$ é um monomorfismo, segue pelo Lema 2.3.4, que existe um homomorfismo $p : B \longrightarrow A$, tal que $pi = 1_A$, portanto a sequência dada cinde. Note também que existe um homomorfismo $\gamma : P \longrightarrow B$, tal que $\beta\gamma = 1_P$, pois P é projetivo:



■

Teorema 2.3.7. *Um módulo P é projetivo se, e somente se, é um somando direto de um módulo livre. Além disso, qualquer somando de um projetivo é projetivo.*

Demonstração: Suponha que P seja projetivo, temos que cada módulo é um quociente de um módulo livre , deste modo existe um epimorfismo $\beta : F \longrightarrow P$, em que F é livre, mas pelo Teorema 2.3.5, temos que P é um somando de F. Reciprocamente, mostremos que somandos de módulos projetivos são projetivos, deste modo se P é um somando de um livre, o qual é projetivo pelo Teorema 2.3.2, segue que P é projetivo. De fato, suponha que P seja somando de um módulo projetivo F, então pelo Lema 2.3.4, existe um morfismo $p : F \longrightarrow P$,

tal que $pi = 1_P$, em que i é a inclusão. Como F é projetivo, existe um homomorfismo de módulos $\gamma : F \longrightarrow B$, tal que $\beta\gamma = fp$, ou seja, o diagrama abaixo é comutativo:

$$\begin{array}{ccccc} F & \underset{i}{\overset{p}{\rightleftarrows}} & P & & \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle f} & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 \end{array}$$

Defina $g : P \longrightarrow B$ por $g = \gamma \circ i$, deste modo $\beta g = \beta\gamma i = fpi = f$, portanto $f = \beta g$. Logo P é projetivo.

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{g} & \downarrow{\scriptstyle f} & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 \end{array}$$

■

Exemplo 2.3.8. *Existem módulos projetivos que não são livres. Considere* $R = \mathbb{Z}/6\mathbb{Z}$*, então* $R \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$*, logo* $\mathbb{Z}/2\mathbb{Z}$ *é somando de um livre, daí é projetivo, no entanto,* $\mathbb{Z}/2\mathbb{Z}$ *não é livre, pois cada* R*-módulo livre não-nulo tem pelo menos* 6 *elementos. Mas, isso não ocorre com módulos projetivos finitamente gerados sobre um anel local, como no lema a seguir.*

Proposição 2.3.9. *Sejam* $P_1, \ldots, P_n$ *módulos sobre* R*. Então, a soma direta* $\bigoplus_{i=1}^{n} P_i$ *é um* R*-módulo projetivo se, e somente se, cada* P_i *é um* R*-módulo projetivo.*

Demonstração:

($\Leftarrow$) Inicialemente consideremos $n = 2$. Suponha que $P_1 = P$ e $P_2 = Q$ sejam R-módulos projetivos, sejam $\beta : B \longrightarrow C$ um R-epimorfismo, e $\alpha : P \oplus Q \longrightarrow C$ um R-homomorfismo. Mostremos que existe um homomorfismo γ tal que $\alpha = \beta\gamma$. Considere os homomorfismos $\alpha_p = \alpha \circ i_p : P \longrightarrow C$, e $\alpha_q = \alpha \circ i_q : Q \longrightarrow C$, em que $i_p : P \longrightarrow P \oplus Q$, e $i_q : Q \longrightarrow P \oplus Q$ são inclusões. Como P é um módulo projetivo, existe um homomorfismo $\gamma_p : P \longrightarrow B$, tal que $\alpha_p = \beta\gamma_p$, analogamente, como Q é projetivo, existe um homomorfismo $\gamma_q : Q \longrightarrow B$, tal que $\alpha_q = \beta\gamma_q$, como nos diagramas comutativos abaixo:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{\gamma_P} & \downarrow{\scriptstyle \alpha_p} & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 \end{array} \qquad \begin{array}{ccccc} & & Q & & \\ & \swarrow^{\gamma_q} & \downarrow{\scriptstyle \alpha_q} & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 \end{array}$$

Agora, pela propriedade universal de $P \oplus Q$, existe um único homomorfismo $\gamma : P \oplus Q \longrightarrow B$, tal que $\gamma_p = \gamma i_p$, e $\gamma_q = \gamma i_q$:

$$\begin{array}{ccc} P & \xrightarrow{i_p} & P \oplus Q \\ {\scriptstyle \gamma_p}\downarrow & \swarrow_{\gamma} & \\ B & & \end{array} \qquad \begin{array}{ccc} Q & \xrightarrow{i_q} & P \oplus Q \\ {\scriptstyle \gamma_q}\downarrow & \swarrow_{\gamma} & \\ B & & \end{array}$$

Mas, $(\beta\gamma)i_p = \beta(\gamma i_p)) = \beta\gamma_p = \alpha_p = \alpha i_p$, analogamente $(\beta\gamma)i_q = \alpha i_q$. Por outro lado, temos que $\alpha_p = \alpha i_p$, e $\alpha_q = \alpha i_q$:

$$\begin{array}{ccc} P & \xrightarrow{i_p} & P \oplus Q \\ {\scriptstyle \alpha_p}\downarrow & \swarrow_{\alpha} & \\ C & & \end{array} \qquad \begin{array}{ccc} Q & \xrightarrow{i_q} & P \oplus Q \\ {\scriptstyle \alpha_q}\downarrow & \swarrow_{\alpha} & \\ C & & \end{array}$$

Logo pela unicidade de α, segue que $\beta\gamma = \alpha$, logo $P \oplus Q$ é projetivo:

$$\begin{array}{ccccc} & & P \oplus Q & & \\ & \swarrow_{\gamma} & \downarrow{\scriptstyle \alpha} & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 \end{array}$$

Agora, suponha que para algum $n \in \mathbb{N}$, $\bigoplus_{i=1}^{n} P_i$ seja projetivo, então se P_{i+1} é um R-módulo projetivo, segue pelo argumento acima que $\bigoplus_{i=1}^{n} P_i \oplus P_{i+1}$ é projetivo, logo $\bigoplus_{i=1}^{n+1} P_i$ é projetivo, portanto pelo princípio de indução, segue que $\bigoplus_{i=1}^{n} P_i$ é projetivo para todo $n \in \mathbb{N}$.

($\Rightarrow$) Suponha que $P \oplus Q$ seja um R-módulo projetivo. Sejam $\beta : B \longrightarrow C$ um R-epimorfismo, e $\alpha_p : P \longrightarrow C$ um R-homomorfismo. Considere o homomorfismo trivial $\alpha_q : Q \longrightarrow C$, daí $\alpha_q(x) = 0$, para todo $x \in Q$. Pela propriedade universal para soma direta, $P \oplus Q$, temos que existe um único homomorfismo $\alpha : P \oplus Q \longrightarrow C$, tal que $\alpha i_p = \alpha_p$, e $\alpha i_q = \alpha_q \equiv 0$:

$$\begin{array}{ccc} P & \xrightarrow{i_p} & P \oplus Q \\ {\scriptstyle \alpha_p}\downarrow & \swarrow_{\alpha} & \\ C & & \end{array} \qquad \begin{array}{ccc} Q & \xrightarrow{i_q} & P \oplus Q \\ {\scriptstyle \alpha_q}\downarrow & \swarrow_{\alpha} & \\ C & & \end{array}$$

Mas, por hipótese, $P \oplus Q$ é projetivo, logo existe um homomorfismo $\gamma : P \oplus Q \longrightarrow B$, tal que $\beta\gamma = \alpha$:

$$\begin{array}{ccccc} & & P \oplus Q & & \\ & \swarrow_{\gamma} & \downarrow{\scriptstyle \alpha} & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 \end{array}$$

Deste modo, $\beta(\gamma i_p) = (\beta\gamma)i_p = \alpha i_p = \alpha_p$. Portanto, $\gamma i_p : P \longrightarrow B$ é solução para o diagrama comutativo abaixo:

$$\begin{array}{ccccc} & & P & & \\ & \overset{\gamma i_p}{\swarrow} & \downarrow{\scriptstyle \alpha_p} & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 \end{array}$$

Logo, P é projetivo. Analogamente, mostramos que Q é projetivo. O caso geral segue por indução.

■

Proposição 2.3.10. *Se P e Q são R-módulos projetivos, então $P \otimes_R Q$ é um R-módulo projetivo.*

Demonstração: Sejam $\beta : B \longrightarrow C$ um R-epimorfismo, e $\alpha : P \otimes_R Q \longrightarrow C$ seja um R-homomorfismo, pela Proposição 2.3.9, temos que $P \oplus Q$ é projetivo, logo existe um homomorfismo $f : P \oplus Q \longrightarrow B$, tal que $\alpha h = \beta f$, em que $h : P \oplus Q \longrightarrow P \otimes_R Q$ é definida por $h(p, q) = p \otimes q$.

$$\begin{array}{ccccccc} P \oplus Q \cong P \times Q & \xrightarrow{h} & P \otimes_R Q & & & & \\ \downarrow{\scriptstyle f} & \overset{\gamma}{\swarrow} & \downarrow{\scriptstyle \alpha} & & & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 & & \end{array}$$

Agora, pela definição de $P \otimes_R Q$, existe um único $\mathbb{Z}$-homomorfismo $\gamma : P \otimes_R Q \longrightarrow B$, tal que $f = \gamma h$:

$$\begin{array}{ccc} P \times Q & \xrightarrow{h} & P \otimes_R Q \\ \downarrow{\scriptstyle f} & \overset{\gamma}{\swarrow} & \\ B & & \end{array}$$

Portanto, $\alpha h = \beta f = \beta(\gamma h) = (\beta\gamma)h$, mas h é sobrejetora, logo possui inversa à direita, h^{-1}, daí $\alpha h h^{-1} = (\beta\gamma h)h^{-1}$, logo $\alpha = \beta\gamma$, deste modo $P \otimes_R Q$ é projetivo:

$$\begin{array}{ccccc} & & P \otimes_R Q & & \\ & \overset{\gamma}{\swarrow} & \downarrow{\scriptstyle \alpha} & & \\ B & \xrightarrow[\beta]{} & C & \longrightarrow & 0 \end{array}$$

■

2.4 Módulos noetherianos

Proposição 2.4.1. *Considere que Σ seja um conjunto parcialmente ordenado de submódulos de um módulo M pela relação $\subseteq$. Então, são equivalentes:*

(i) ***(condição de cadeia ascendente)*** *Cada sequência crescente $M_1 \subseteq M_2 \subseteq \ldots$ em Σ é estacionária, i.e, existe $n \in \mathbb{N}$ tal que $M_i = M_n$ para todo $i \geq n$;*

(ii) ***(condição maximal)*** *Cada subconjunto não-vazio de Σ tem um elemento maximal.*

Demonstração: Veja num contexto mais geral a Proposição 3.1.12.

■

Definição 2.4.2. *Um R-módulo M é chamado* ***noetheriano****, quando M tem uma das condições equivalentes em 2.4.1.*

Proposição 2.4.3. *M é um R-módulo noetheriano se, e somente se, cada submódulo de M é finitamente gerado.*

Demonstração: Suponha que M seja noetheriano, e que N seja um submódulo de M. Defina Σ como sendo o conjunto de todos submódulos finitamente gerados de N. Portanto, já que $(0) \in \Sigma$, segue que Σ não é vazio. Logo como M é noetheriano, temos que Σ possui um elemento maximal, digamos N_0. Mostremos que $N_0 = N$, suponha por absurdo que $N_0 \neq N$, então existe $x \in N \backslash N_0$. Deste modo o submódulo $N_0 + Rx$ é finitamente gerado e contém N_0 propriamente, o que contradiz a maximalidade de N_0. Portanto $N = N_0$, e daí N é finitamente gerado. Reciprocamente, suponha que cada submódulo de M seja finitamente gerado. Seja $M_1 \subseteq M_2 \subseteq \ldots$ uma cadeia ascendente de submódulos de M, deste modo $N = \bigcup_{i=1}^{\infty} M_i$ é um submódulo de M e, por hipótese, é finitamente gerado, logo existem $x_1, \ldots, x_k \in N$, tais que $N = \sum_{i=1}^{m} Rx_i$. Agora, suponha que $x_i \in M_{n_i}$, e defina $n = max_{1 \leq i \leq k} n_i$, então cada x_i pertence a M_n, daí $N = M_n$, logo $M_i = N$ para todo $i \geq n$. Portanto a cadeia dada é estacionária, logo M é noetheriano.

■

Definição 2.4.4. *Um anel R é noetheriano, quando é noetheriano como um R-módulo.*

Proposição 2.4.5. *Seja M um módulo noetheriano, então cada submódulo de M é noetheriano.*

Demonstração: Seja N um submódulo de M. Considere que $N_1 \leq N_2 \leq \ldots$ seja um cadeia ascendente de submódulos de N, daí é um cadeia de submódulos de M, mas como M é noetheriano, tal cadeia é estacionária, portanto N é noetheriano.

■

Proposição 2.4.6. *Seja M um módulo noetheriano, então cada módulo quociente de M é noetheriano.*

Demonstração: Sejam M/N um módulo quociente de M e M'/N um submódulo de M/N. Como M é noetheriano, segue que M' é finitamente gerado, digamos por $x_1, \ldots, x_k$, mas daí $x_1 + M, \ldots, x_k + M$ geram M'/M como módulo, portanto M'/M é finitamente gerado, logo M/N é noetheriano.

■

Proposição 2.4.7. *Sejam M um módulo e N um submódulo de M. Então M é noetheriano se, e somente se, N e M/N são noetherianos.*

Demonstração: Se M é noetheriano, temos pelas Proposições 2.4.5 e 2.4.6, que N e M/N são noetherianos. Reciprocamente, suponha que N e M/N sejam módulos noetherianos. Seja $M_1 \leq M_2 \leq \ldots$ uma cadeia ascendente de submódulos de M, deste modo $M_1 \cap N \leq M_2 \cap N \leq \ldots$ e $(M_1+N)/N \leq (M_2+N)/N \leq \ldots$ são cadeias ascendentes em N e M/N, logo são estacionárias, pois M e M/N são noetherianos, portanto existem índices i e j, tais que $M_i \cap N = M_n \cap N$ e $(M_j + N)/N = (M_m + N)/N$ para todo $n \geq i$, e para todo $m \geq j$. Seja $k = max\{i, j\}$, então $M_k \cap N = M_n \cap N$ e $(M_k + N)/N = (M_n + N)/N$ para todo $n \geq k$, mas pelo Teorema da Correspondência, segue que $M_k + N = M_n + M$. Mostremos que $M_k = M_n$ para $n \geq k$ fixado, a inclusão $M_k \subseteq M_n$ é trivial, seja $x \in M_n$, então $x \in M_n + N$, logo $x \in M_k + N$, portanto existem $y \in M_k$ e $z \in N$, tais que $x = y + z$, logo $z = x - y \in M_n \cap N$, consequentemente $z \in M_k \cap N$, daí $z \in M_k$. Portanto, $x = y + z \in M_k$. Deste modo, $M_k = M_n$ para todo $n \geq k$, logo M é noetheriano.

■

Corolário 2.4.8. *Considere que* $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ *seja uma sequência exata de R-módulos. Então, M é noetheriano se, e somente se, M′ e M″ são noetherianos.*

Demonstração: Como a sequência dada é exata, segue que α é injetor e β é sobrejetor, logo M' pode ser visto como um submódulo de M, e M'', como um quociente de M. Segue pela Proposição 2.4.7, que M é noetheriano se, e somente se, M' e M'' são noetherianos.

■

Corolário 2.4.9. *Se* M_i, $i = 1, \ldots, n$ *são R-módulos noetherianos, então* $\bigoplus_{i=1}^{n} M_i$ *é um R-módulo noetheriano.*

Demonstração: Considere a sequência exata

$$0 \longrightarrow M_2 \xrightarrow{\alpha} M_1 \oplus M_2 \xrightarrow{\beta} M_1 \longrightarrow 0,$$

em que α é a inclusão, e β a projeção. Logo pelo Corolário 2.4.8, segue que $M_1 \oplus M_2$ é noetheriano. Agora, suponha que para algum $k \geq 2$, $M_1, \ldots, M_k$ e $\bigoplus_{i=1}^{k-1} M_i$ sejam noetherianos, então considerando a sequência exata

$$0 \longrightarrow M_k \xrightarrow{\alpha'} \bigoplus_{i=1}^{k} M_i \xrightarrow{\beta'} \bigoplus_{i=1}^{k-1} M_i \longrightarrow 0,$$

segue pelo Corolário 2.4.8, que $\bigoplus_{i=1}^{k} M_i$ é noetheriano, logo pelo Princípio de Indução segue o resultado.

■

Proposição 2.4.10. *Considere que R seja um anel noetheriano, e que M seja um R-módulo finitamente gerado. Então M é noetheriano.*

Demonstração: Como M é um R-módulo finitamente gerado, segue que M é isomorfo a um quociente de um R-módulo livre, logo existe $n \in \mathbb{N}$, e um R-homomorfismo $\varphi : R^n \longrightarrow M$. Deste modo $M \cong (\bigoplus_{i=1}^{n} M_i)/Ker(\varphi)$, em que M_i é isomorfo a R como R-módulos para cada i. Agora, pelo Corolário 2.4.9, $\bigoplus_{i=1}^{n} M_i$ é noetheriano, logo também é o quociente $\bigoplus_{i=1}^{n} M_i/Ker(\varphi)$. Portanto M é noetheriano.

■

Nas próxima seção, veremos a definição de módulo de frações, mas por comodidade apresentaremos aqui a seguinte proposição:

Proposição 2.4.11. *Se M é um módulo noetheriano sobre um anel R, então $S^{-1}M$ é um módulo noetheriano.*

■

2.5 Módulos de frações

Nestão seção, denotaremos a injeção canônica $x \mapsto x/1$ do anel R no anel de frações $S^{-1}R$ por i_R^S. Note que, se M é um $S^{-1}R$-módulo, podemos considerá-lo um R-módulo via i_R^S.

Agora apresentaremos uma proposição, a qual nos possibilita definir módulo de frações.

Proposição 2.5.1. *Sejam R um anel, S um subconjunto de R, M um R-módulo, $M' = M \otimes_R S^{-1}R$ módulo sobre R, e f o R-homomorfismo canônico $x \mapsto x \otimes 1$ de M a M'. Então:*

(i) Para todo $s \in S$, a homotetia $z \mapsto sz$ de M' é bijetiva;

(ii) Para cada R-módulo N, tal que para todo $s \in S$, a homotetia $y \mapsto sy$ de N é bijetiva, e para cada homomorfismo u de M em N, existe um único homomorfismo u' de M' em N, tal que $u = u' \circ f$.

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle u}\downarrow & \swarrow_{u'} & \\ N & & \end{array}$$

Demonstração: [7], p.60

■

Definição 2.5.2. *Sejam R um anel, S um subconjunto de R, $\overline{S}$ o subconjunto multiplicativamente fechado de R gerado por S, e M um R-módulo. Dizemos que o módulo de frações de M definido por S e denotado por $M[S^{-1}]$ ou $\overline{S}^{-1}M$ é qualquer $R[S^{-1}]$-módulo isomorfo a $M \otimes_R R[S^{-1}]$.*

Observação 2.5.3. *Coincidimos as notações $R[S^{-1}]$ e $S^{-1}R$ quando S é um subconjunto multiplicativamente fechado de R.*

Notação Indicaremos o homomorfismo canônico $m \mapsto m \otimes 1$ de M em $M[S^{-1}]$ por i_M^S.

Observação 2.5.4. *1. $M[\overline{S}^{-1}] = M[S^{-1}]$;*

2. *Para cada $m \in M$ e $s \in \overline{S}$, denotamos o elemento $m \otimes (1/s)$ de $M[S^{-1}]$ por m/s.*

3. *Cada elemento de $M[S^{-1}]$ é da forma $\sum_i m_i \otimes (a_i/s)$, em que $m_i \in M$, $a_i \in R$, $s \in S$. Note que*

$$m_i \otimes (a_i/s) = (a_i m_i) \otimes (1/s).$$

Logo

$$\sum_i m_i \otimes (a_i/s) = m \otimes (1/s), \text{ em que } m = \sum_i a_i m_i.$$

4. *Com a notação em (2), temos que*

$$(m/s) + (m'/s) = (s'm + sm')/ss'$$

$$(a/s)(m/s') = (am)/(ss'),$$

em que $m, m' \in M$, $a \in R$, e $s, s' \in S$.

5. *Se $S = R - \mathfrak{p}$, em que $\mathfrak{p}$ é um ideal primo de R, denotamos o múdulo de frações de M definido por S por $M_{\mathfrak{p}}$ em vez de $S^{-1}M$.*

Proposição 2.5.5. *Sejam S um subconjunto multiplicativamente fechado do anel R e M um R-módulo. Para $m/s = 0$, em que $m \in M$, $s \in S$, é necessário e suficiente que exista $s' \in S$, tal que $s'm = 0$.*

Demonstração: [7], p.62.

■

Corolário 2.5.6. *Para $m/s = m'/s$ em $S^{-1}M$, é necessário e suficiente que exista $t \in S$, tal que $t(s'm - sm') = 0$.*

Demonstração: De fato, $m/s = m'/s$, se e somente se, $(m/s) - (m'/s') = (1/ss')(s'm - sm')$. Note que $1/ss' \in S$.

■

Observação 2.5.7. *O módulo de frações poderia ser, equivalentemente, definido por meio de relações de equivalências definidas segundo o Corolário 2.5.6. Deste modo, obteríamos o isomorfismo* $S^{-1}M \cong S^{-1}R \otimes_R M$*, observando que a aplicação* $h : S^{-1}R \times M \longrightarrow S^{-1}M$ *definida por* $(a/s, m) \mapsto am/s$ *é* R*-bilinear, e induz um único homomorfismo*

$$\varphi : S^{-1}R \otimes_R M \longrightarrow S^{-1}M,$$

tal que $\varphi((a/s) \otimes m) = am/s$*. Verica-se facilmente que* φ *é bijetor.*

Proposição 2.5.8. *Se* M *e* N *são* R*-módulos, então existe um único isomorfismo de* $S^{-1}R$*-módulos*

$$\varphi : S^{-1}M \otimes_{S^{-1}R} S^{-1}N \longrightarrow S^{-1}(M \otimes_R N),$$

tal que $\varphi((m/s) \otimes (n/t)) = (m \otimes n)/st$*. Em particular, se* $\mathfrak{p}$ *é um ideal primo de* R*, então vale o isomorfismo de* $R_\mathfrak{p}$*-módulos*

$$M_\mathfrak{p} \otimes_{R_\mathfrak{p}} N_\mathfrak{p} \cong (M \otimes_R N)_\mathfrak{p}.$$

Demonstração: Considere $h : S^{-1}M \times S^{-1}N \longrightarrow S^{-1}M \otimes_{S^{-1}R} S^{-1}N$ a aplicação que define o produto tensorial $S^{-1}M \otimes_{S^{-1}R} S^{-1}N$. Defina $f : S^{-1}M \times S^{-1}N \longrightarrow S^{-1}(M \otimes N)$ por $f((m/s, n/t)) = (m \otimes n)/st$, deste modo f é uma aplicação R-biaditiva. Logo, pela propriedade universal que define $S^{-1}M \otimes_{S^{-1}R} S^{-1}N$, existe um único homomorfismo

$$\varphi : S^{-1}M \otimes_{S^{-1}R} S^{-1}N \longrightarrow S^{-1}(M \otimes_R N),$$

tal que $f = \varphi \circ h$, ou seja, o diagrama abaixo comuta:

$$\begin{array}{ccc} S^{-1}M \times S^{-1}N & \xrightarrow{\ h\ } & S^{-1}M \otimes_{S^{-1}R} S^{-1}N \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \varphi} & \\ S^{-1}(M \otimes N) & & \end{array}$$

Portanto, $(m \otimes n)/st = f((m/s, n/t)) = \varphi(h(m/s, n/t)) = \varphi((m/s) \otimes (n/t))$. Note que φ é um isomorfismo, daí o resultado. Apresentaremos uma outra demonstração, que apenas usa a associatividade do produto tensorial e os isomorfismos

$$S^{-1}M \cong S^{-1}R \otimes_R M; M \otimes_{S^{-1}R} S^{-1}R \cong M.$$

Demonstração: Temos que $S^{-1}M \otimes_{S^{-1}R} S^{-1}N \cong S^{-1}M \otimes_{S^{-1}R} (S^{-1}R \otimes N) \cong S^{-1}M \otimes_R N \cong (S^{-1}R \otimes_R M) \otimes_R N \cong (S^{-1}R) \otimes_R (M \otimes_R N) \cong S^{-1}(M \otimes_R N)$.

■

Proposição 2.5.9. *Sejam M e N R-submódulos, então $S^{-1}(M \oplus N) = S^{-1}M \oplus S^{-1}N$. Em particular, para cada ideal primo $\mathfrak{p}$ de R, temos que $(M \oplus N)_{\mathfrak{p}} = M_{\mathfrak{p}} \oplus N_{\mathfrak{p}}$.*

Demonstração: Seja $(m+n)/s \in S^{-1}(M \oplus N)$, note que $(m+n)/s = m/s + n/s \in S^{-1}M \oplus S^{-1}N$. Reciprocamente, se $m/s + n/t \in S^{-1}M \oplus S^{-1}N$, então $m/s + n/t = (tm+sn)/st \in S^{-1}(M \oplus N)$, pois $st \in S$, $tm \in M$, e $sn \in N$.

■

Observação 2.5.10 ([4], p.39)**.** *A operação S^{-1} é exata. Mais precisamente, se*

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

é exata, então

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0$$

é exata.

Proposição 2.5.11. *$S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.*

Demonstração: Considere a sequência exata

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0,$$

agora aplique S^{-1}, obtendo-se a sequência exata

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0.$$

Portanto $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

■

Proposição 2.5.12. *Seja $\varphi : M \longrightarrow N$ um R-homomorfismo. São equivalentes:*

(i) φ é injetivo (sobrejetivo);

(ii) $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ é injetivo (sobrejetivo) para cada ideal primo $\mathfrak{p}$ de R;

(iii) $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}$ é injetivo (sobrejetivo) para cada ideal maximal $\mathfrak{m}$ de R.

Demonstração:
$(i) \Rightarrow (ii)$ Se $0 \longrightarrow M \longrightarrow N$ é exata, então $0 \longrightarrow M_{\mathfrak{p}} \longrightarrow N_{\mathfrak{p}}$ é exata.
$(ii) \Rightarrow (iii)$ De fato, cada ideal maximal é primo.
$(iii) \Rightarrow (i)$ Seja $M' = \mathrm{Ker}(\varphi)$, então a sequência

$$0 \longrightarrow M' \longrightarrow M \longrightarrow N$$

é exata. Localizando obtemos a sequência exata

$$0 \longrightarrow (M')_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}}.$$

Portanto, $(M')_{\mathfrak{m}} \cong \mathrm{Ker}(\varphi_m)$, mas $\varphi_{\mathfrak{m}}$ é injetor, logo $(M')_{\mathfrak{m}} = 0$, daí $M' = 0$. Portanto, φ é injetor.
Para o outro caso, é suficiente reverter as flechas.

■

Proposição 2.5.13. *Sejam R um anel, $\mathfrak{m}$ um ideal maximal de R e M um R-módulo. Se existe um ideal $\mathfrak{a}$ de R tal que $\mathfrak{a}M = 0$, e $\mathfrak{m}$ é o único ideal maximal de R contendo $\mathfrak{a}$, então o homomorfismo canônico $M \longrightarrow M_{\mathfrak{m}}$ é bijetivo. Em particular, se existe um inteiro $k \geq 0$, tal que $\mathfrak{m}^k M = 0$, temos que $M \longrightarrow M_{\mathfrak{m}}$ é bijetivo.*

Demonstração: Como $\mathfrak{m}$ é o único ideal maximal que contém $\mathfrak{a}$, segue que o anel $R/\mathfrak{a}$ é local, cujo ideal maximal é $\mathfrak{m}/\mathfrak{a}$. Agora note que, como $\mathfrak{a}M = 0$, segue que $\mathfrak{a} \subseteq Ann(M)$, logo M pode ser considerado como um $R/\mathfrak{a}$-módulo. Deste modo, temos que para todo $s \in R - \mathfrak{m}$, a imagem canônica de s em $R/\mathfrak{m}$ é invertível. Logo, a homotetia $x \mapsto sx$ em M, dada como na Proposição 2.5.1 como solução do problema universal, é bijetiva. Consequentemente o homomorfismo canônico $x \mapsto x \otimes 1$ de M em $M_{\mathfrak{m}}$ é bijetivo.

■

Proposição 2.5.14. *Sejam R um anel, $\mathfrak{m}$ um ideal maximal de R, M um R-módulo e $k \geq 0$ um inteiro. Então o homomorfismo canônico $M \longrightarrow M_{\mathfrak{m}}/\mathfrak{m}^k M_{\mathfrak{m}}$ é sobrejetor e tem núcleo $\mathfrak{m}^k M$, daí define um isomorfismo de $M/\mathfrak{m}^k M$ sobre $M_{\mathfrak{m}}/\mathfrak{m}^k M_{\mathfrak{m}}$.*

Demonstração: Basta tomar, com as notações da Proposição 2.5.13, $\mathfrak{a} = \mathfrak{m}^k$, e notar que $\mathfrak{m}$ é o único ideal maximal que contém $\mathfrak{a}$, e que $\mathfrak{m}^k \subseteq Ann(M/\mathfrak{m}^k M)$, daí $\mathfrak{a}(M/\mathfrak{m}^k M) = 0$. Logo pela Proposição 2.5.13, $M/\mathfrak{m}^k M \cong (M/\mathfrak{m}^k M)_{\mathfrak{m}}$, mas pela Proposição 2.5.11, $(M/\mathfrak{m}^k M)_{\mathfrak{m}} \cong M_{\mathfrak{m}}/\mathfrak{m}^k M_{\mathfrak{m}}$, daí segue a proposição.

■

O resultado abaixo já foi demonstrado anteriormente, mas será reapresentado, pois é uma consequência do corolário acima.

Corolário 2.5.15. *Sejam R um anel, $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ distintos ideais maximais de R, M um R-módulo, e $k_1, \ldots, k_n$ inteiros não-negativos. Então o homomorfismo canônico de M em $\prod_{i=1}^{m} M_{\mathfrak{m}}/\mathfrak{m}_i^{k_i} M_{\mathfrak{m}}$ é sobrejetivo, cujo núcleo é $(\bigcap_{i=1}^{n} \mathfrak{m}_i^{k_i})M$.*

■

2.6 Anéis noetherianos

Mostramos algumas propriedades acerca de módulos noetherianos. Nesta seção, apresentaremos resultados sobre anéis noetherianos R, os quais podem ser vistos como R-módulos, de modo que os resultados válidos para R-módulos noetherianos, valem também para o anel R visto como R-módulo. Note também que os submódulos de R são precisamente seus ideais.

Uma característica notável dos anéis noetherianos é que estes sempre possuem uma decomposição primária, a qual será definida nesta seção.

Proposição 2.6.1. *Considere que Σ seja um conjunto de ideais de R parcialmente ordenado por uma relação $\subseteq$. Então, são equivalentes:*

(i) ***(condição de cadeia ascendente)*** *Cada sequência crescente $I_1 \subseteq I_2 \subseteq \ldots$ em Σ é estacionária, i.e, existe $n \in \mathbb{N}$ tal que $I_i = I_n$ para todo $i \geq n$;*

(ii) ***(condição maximal)*** *Cada subconjunto não-vazio de Σ tem um elemento maximal.*

Demonstração: Vide 3.1.12.

■

Definição 2.6.2. *Se um anel R satisfaz uma das condições equivalentes acima, chamamos R de anel noetheriano.*

Observação 2.6.3. *Note que essa definição é equivalente à fornecida em 2.4.4.*

Proposição 2.6.4. *Sejam R um anel e I um ideal de R. Então, R é noetheriano se, e somente se, I e o anel quociente R/I são noetherianos.*

Demonstração: R é um R-módulo, e seus submódulos são precisamente os seus ideais, logo pela Proposição 2.4.7, segue o resultado.

■

Proposição 2.6.5. *Se R é um anel noetheriano, e φ é um epimorfismo de anéis de R em S, então S é uma anel noetheriano.*

Demonstração: De fato, temos pelo 1º Teorema do isomorfismo que, $S \cong R/Ker(\varphi)$, logo S é um quociente de um anel noetheriano, logo é também noetheriano.

■

Proposição 2.6.6. *Considere que S seja um subanel de R. Se S é noetheriano, e R é finitamente gerado como um S-módulo, então R é um anel noetheriano.*

Demonstração: Temos que R é um módulo finitamente gerado sobre o anel noetheriano S, logo pela Proposição 2.4.10, R é um S-módulo noetheriano, logo é um R-módulo noetheriano. Portanto, R é um anel noetheriano.

■

Proposição 2.6.7. *Se R é um anel noetheriano, e S é um subconjunto multiplicativamente fechado de R, então o anel de frações $S^{-1}R$ é noetheriano.*

Demonstração: Temos que os ideais de R estão em correspondência $1-1$ com os ideias de $S^{-1}R$. Seja $S^{-1}\mathfrak{a}$ um ideal de $S^{-1}R$, o qual corresponde ao ideal $\mathfrak{a}$ de R. Por hipótese, R é noetheriano, logo $\mathfrak{a}$ é finitamentente gerado, digamos por $x_1, \ldots, x_n$. Logo $S^{-1}\mathfrak{a}$ é gerado por $x_1/1, \ldots, x_n/1$. Portanto, $S^{-1}\mathfrak{a}$ é finitamente gerado. Logo $S^{-1}R$ é noetheriano.

■

Corolário 2.6.8. *Se R é noetheriano, e $\mathfrak{p}$ é um ideal primo de R, então a localização $R_\mathfrak{p}$ de R em $\mathfrak{p}$ é um anel noetheriano.*

Demonstração: Basta notar que $S = R - \mathfrak{p}$ é multiplicativamente fechado, uma vez que $\mathfrak{p}$ é primo. Logo $S^{-1}R = R_\mathfrak{p}$ é noetheriano.

■

Proposição 2.6.9 (Teorema da Base de Hilbert)**.** *Se R é um anel noetheriano, então o anel de polinômios $R[x]$ é noetheriano.*

Demonstração: Seja $\mathfrak{a}$ um ideal de R. Mostremos que $\mathfrak{a}$ é finitamente gerado. Considere que I seja o ideal de R formado por 0 e pelos coeficientes líderes dos polinômios pertencentes a $\mathfrak{a}$. Por hipótese, R é noetheriano, logo I pode ser gerado por uma quantidade finita de elementos, $a_1, \ldots, a_n$. Para cada $i = 1, \ldots, n$, considere o polinômio $f_i \in R[x]$ da forma $f_i = a_i x^{r_i} + g_i$, em que g_i é um polinômio em $R[x]$ com termos de grau menor que r_i. Agora, defina $r = max_{i=1}^{n} r_i$, e considere o ideal $\mathfrak{a}'$ de $R[x]$ gerado pelos $f_i's$. Seja $f = ax^m + f' \in \mathfrak{a}$, em que f' é um polinômio de grau menor que m, note que $a \in I$, pois é um coeficiente líder de um polinômio em $\mathfrak{a}$.

Suponha $m \geq r$, e escreva $a = \sum_{i=1}^{n} u_i a_i$, em que $u_i \in R$. Então $f - \sum u_i f_i x^{m-r_i}$ pertence a $\mathfrak{a}$ e tem grau menor que m. Usando este método, podemos continuar subtraindo elementos de $\mathfrak{a}'$ de f até obtermos um polinômio g, cujo grau é menor que r, daí temos $f = g + h$ para algum $h \in \mathfrak{a}'$. Logo se M é o R-módulo gerado por $1, x, \ldots, x^{r-1}$, segue que $\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$. Temos que M é um módulo finitamente gerado sobre o anel noetheriano R, logo pela Proposição 2.4.10, segue que M é noetheriano. Logo o submódulo $\mathfrak{a} \cap M$ é finitamente gerado como um R-módulo. Suponha que $g_1, \ldots, g_m$ gerem $\mathfrak{a} \cap M$. Deste modo, os $f_i's$ e $g_j's$, $i = 1, \ldots, n$, $j = 1, \ldots, m$ geram $\mathfrak{a}$. Portanto $\mathfrak{a}$ é finitamente gerado. Logo $R[x]$ é noetheriano.

■

Proposição 2.6.10. *Se R é noetheriano, então $R[x_1, \ldots, x_n]$ é noetheriano.*

Demonstração: Pelo Teorema da Base de Hilbert, temos que $R[x_1]$ é noetheriano. Suponha que $S = R[x_1, \ldots, x_n]$ seja noetheriano para algum $n \geq 1$, então pelo Teorema 2.6.9, temos que o anel $S[x_{n+1}]$ é noetheriano. Logo, $R[x_1, \ldots, x_{n+1}]$ é noetheriano. Portanto, pelo Princípio de indução, segue que $R[x_1, \ldots, x_n]$ é noetheriano para todo número natural n.

■

Definição 2.6.11. *Um ideal $\mathfrak{q}$ de um anel R é chamado primário, quando $\mathfrak{q} \neq R$, e sempre que $xy \in \mathfrak{q}$, tem-se que $x \in \mathfrak{q}$ ou $y^n \in \mathfrak{q}$ para algum inteiro $n > 0$.*

Proposição 2.6.12. *Um ideal* $\mathfrak{q}$ *de* R *é primário se, somente se,* $R/\mathfrak{q} \neq 0$*, e cada divisor de zero em* $R/\mathfrak{q}$ *é nilpotente.*

Demonstração: Suponha que $\mathfrak{q}$ seja primário, então $\mathfrak{q} \neq R$, daí $R/\mathfrak{q} \neq 0 = \mathfrak{q}$, agora considere que $y+\mathfrak{q}$ seja um divisor de zero em $R/\mathfrak{q}$, logo existe $x+\mathfrak{q} \neq \mathfrak{q}$, tal que $(x+\mathfrak{q})(y+\mathfrak{q}) = \mathfrak{q}$, logo $xy \in \mathfrak{q}$, mas como $\mathfrak{q}$ é primário e $x \notin \mathfrak{q}$, segue que existe $n > 0$, tal que $y^n \in \mathfrak{q}$, logo $(y + \mathfrak{q})^n = \mathfrak{q}$, portanto $y + \mathfrak{q}$ é nilpotente em $R/\mathfrak{q}$. Reciprocamente, suponha que $xy \in \mathfrak{q}$, $x \notin \mathfrak{q}$, note que $(x + \mathfrak{q})(y + \mathfrak{q}) = \mathfrak{q}$, logo como $x \notin \mathfrak{q}$, segue que $y + \mathfrak{q}$ é um divisor de zero em $R/\mathfrak{q}$, assim é nilpotente, por hipótese. Portanto, $y^n \in \mathfrak{q}$. Logo, $\mathfrak{q}$ é primário.

■

Proposição 2.6.13. *Considere que* $\mathfrak{q}$ *seja um ideal primário em* R*. Então o radical* $r(\mathfrak{q}) = \{x \in R \mid x^n \in \mathfrak{q}$ *para algum* $n > 0\}$ *de* $\mathfrak{q}$ *é o menor ideal primo de* R *contendo* $\mathfrak{q}$*.*

Demonstração: Pela Proposição 1.1.51, temos que $r(\mathfrak{q})$ é um ideal, e claramente $r(\mathfrak{q})$ contém $\mathfrak{q}$. Mostremos que $r(\mathfrak{q})$ é primo. Seja $xy \in r(\mathfrak{q})$, então existe um inteiro $n > 0$, tal que $(xy)^n \in q$, portanto como $\mathfrak{q}$ é primário, segue que $x^n \in \mathfrak{q}$ ou existe $m > 0$, tal que $y^{nm} \in \mathfrak{q}$, deste modo $x \in r(\mathfrak{q})$ ou $y \in r(\mathfrak{q})$. Logo $r(\mathfrak{q})$ é primo. Agora, considere que $\mathfrak{p}$ seja um ideal primo contendo $\mathfrak{q}$. Seja $x \in r(\mathfrak{q})$, então existe $n > 0$, tal que $x^n \in \mathfrak{q}$, logo $x^n \in \mathfrak{p}$, daí $x \in r(\mathfrak{p})$. Mas $\mathfrak{p} = r(\mathfrak{p})$, pois $\mathfrak{p}$ é primo. Portanto, $x \in \mathfrak{p}$, logo $r(\mathfrak{q}) \subseteq \mathfrak{p}$.

■

Definição 2.6.14. *Quando* $\mathfrak{p} = r(\mathfrak{q})$*, dizemos que* $\mathfrak{q}$ *é chamado de* $\mathfrak{p}$*-primário.*

Proposição 2.6.15. *Se* $\mathfrak{q}_i$*,* $i = 1, \ldots, n$ *são ideais* $\mathfrak{p}$*-primários, então o ideal* $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *é* $\mathfrak{p}$*-primário.*

Demonstração: De fato, $r(\mathfrak{q}) = r(\bigcap_{i=1}^{n} \mathfrak{q}_i)) = \bigcap_{i=1}^{n} r(\mathfrak{q}_i) = \mathfrak{p}$

■

Definição 2.6.16. *Uma decomposição primária de um ideal* $\mathfrak{a}$ *de um anel* R *é uma interseção finita de ideais primários* $\mathfrak{q}_i$ *de* R*, isto é,*

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_\mathfrak{i}$$

.

Definição 2.6.17. *Um ideal que possui uma decomposição primária é chamado de um ideal decomponível.*

Definição 2.6.18. *Seja* $\mathfrak{a}$ *um ideal decomponível. Uma decomposição primária* $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *de* $\mathfrak{a}$ *em* R *é chamada minimal(ou reduzida, ou irredundante, ou normal), quando*

(i) Para todo $i \in \{1, \ldots, n\}$, $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$;

(ii) Os radicais $r(\mathfrak{q}_i)$ *são todos distintos.*

Os ideais primos $\mathfrak{p}_i = r(\mathfrak{q}_i)$ *são chamados ideais pertencentes a* $\mathfrak{a}$ *(ou associados a* $\mathfrak{a}$*).*

Proposição 2.6.19. *Se* $\mathfrak{a}$ *é um ideal decomponível, então* $\mathfrak{a}$ *possui uma decomposição primária minimal.*

Demonstração: Suponha que $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ seja uma decomposição primária do ideal $\mathfrak{a}$. Considere que $r(\mathfrak{q}_i) = \mathfrak{p}_i$. Se existem ideias primários $\mathfrak{q}_i$ e $\mathfrak{q}_j$ com mesmo ideal primo associado, então pela Proposição 2.6.15, o ideal $\mathfrak{q}_i \cap \mathfrak{q}_j$ é $\mathfrak{p}_i$-primário(ou $\mathfrak{p}_j$-primário), logo podemos substituir a interseção de todos ideais com mesmo ideal primo $\mathfrak{p}$ associado por um ideal $\mathfrak{p}$-primário, deste modo conseguimos obter a condição (ii) da definição acima. Agora, considerando o ideal $\mathfrak{a}$ já com a condição (ii), mostremos que se verifica a condição (i). Suponha por absurdo que, exista um índice i, tal que $\mathfrak{q}_i \supseteq \bigcap_{j \neq i} \mathfrak{q}_j$, então $r(\mathfrak{q}_i) \supseteq \bigcap_{j \neq i} r(\mathfrak{q}_j)$, daí $\mathfrak{p}_i \supseteq \bigcap_{j \neq i} \mathfrak{p}_j$, mas pela Proposição 1.1.46, segue que $\mathfrak{p}_i \supseteq \mathfrak{p}_j$, para algum $j \neq i$, que é um absurdo. Portanto, o ideal decomponível $\mathfrak{a}$ possui uma decomposição primária minimal.

■

Definição 2.6.20. *Um ideal* $\mathfrak{q}$ *de um anel* R *é chamado irredutível, quando* $\mathfrak{q} = \mathfrak{a} \cap \mathfrak{b}$ *implica que* $\mathfrak{q} = \mathfrak{a}$ *ou* $\mathfrak{q} = \mathfrak{b}$.

Proposição 2.6.21. *Seja* $\mathfrak{q}$ *um ideal de* R*. Então* $\mathfrak{q}$ *é irredutível se, e somente se,* $\mathfrak{q}$ *não é uma interseção finita de ideais que contêm* $\mathfrak{q}$ *propriamente.*

Demonstração: Considere que $\mathfrak{q}$ seja irredutível. Suponha, por absurdo, que $\mathfrak{q} = \mathfrak{a} \cap \mathfrak{b}$ seja uma interseção de ideais de R, com$\mathfrak{a} \supsetneq \mathfrak{q}$, e $\mathfrak{b} \supsetneq \mathfrak{q}$, então $\mathfrak{q} \neq \mathfrak{a}$ e $\mathfrak{q} \neq \mathfrak{b}$, contradizendo a hipótese de $\mathfrak{q}$ ser irredutível. Reciprocamente, se $\mathfrak{q}$ é uma interseção finita de ideais que contêm $\mathfrak{q}$ propriamente, então segue imediatamente da Definição 2.6.20, que $\mathfrak{q}$ não é irredutível.

■

Definição 2.6.22. *Um ideal $\mathfrak{a}$ é chamado redutível, quando não é irredutível.*

Lema 2.6.23. *Em um anel noetheriano R, cada ideal é uma interseção finita de ideais irredutíveis.*

Demonstração: Suponha, por absurdo, que exista um ideal de R que não seja uma interseção finita de ideais irredutíveis, deste modo o conjunto

$$S = \{\mathfrak{a} \trianglelefteq R \mid \mathfrak{a} \text{ não é interseção finita de ideais irredutíveis}\}$$

não é vazio, logo como R é noetheriano, segue que S possui um elemento maximal, digamos $\mathfrak{a}$, o qual não pode ser irredutível, pois caso contrário teríamos trivialmente que $\mathfrak{a}$ seria interseção finita de ideais irredutíveis, ou seja, $\mathfrak{a} = \mathfrak{a} \cap \mathfrak{a}$, o que contradiz a definição de um elemento de S. Logo, sendo $\mathfrak{a}$ redutível, segue pela Proposição 2.6.21, que existem ideais $\mathfrak{b}$, $\mathfrak{c}$ em R, tais que $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ com $\mathfrak{b} \supsetneq \mathfrak{a}$, e $\mathfrak{c} \supsetneq \mathfrak{a}$, logo pela maximalidade de $\mathfrak{a}$, segue que $\mathfrak{b}, \mathfrak{c} \notin S$, deste modo $\mathfrak{b}$ e $\mathfrak{c}$ são interseções finitas de ideais irredutíveis, mas já que $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, segue que $\mathfrak{a}$ também o é, o que implica $\mathfrak{a} \notin S$, que é uma contradição. Portanto, $S = \emptyset$, consequentemente cada ideal de R é uma interseção finita de ideais irredutíveis.

■

Lema 2.6.24. *Em um anel noetheriano R, cada ideal irredutível é primário.*

Demonstração: Seja $\mathfrak{q}$ um ideal irredutível em R, então 0 é um ideal irredutível em $R/\mathfrak{q}$. Note que $\mathfrak{q}$ ser um ideal primário em R é equivalente a 0 ser um ideal primário em $R/\mathfrak{q}$. Considere que $xy = (0)$ com $y \neq 0$. Mostremos que existe $n > 0$ tal que $x^n = 0$. Considere a cadeia ascendente de ideais $Ann(x) \subseteq Ann(x^2) \subseteq \ldots$. Por hipótese, R é noetheriano, logo a cadeia dada é estacionária. Portanto, existe um inteiro $n > 0$, tal que $Ann(x^n) = Ann(x^{n+1}) = \ldots$. Agora, mostremos que $(x^n) \cap (y) = (0)$. De fato, se $a \in (y)$, então existe $r \in R$, tal que $a = ry$, logo $ax = rxy = 0$. Por outro lado, se $a \in (x^n)$, então existe $s \in R$, tal que $a = sx^n$. Logo $0 = ax = sx^{n+1}$, portanto $s \in Ann(x^{n+1})$. Mas $Ann(x^{n+1}) = Ann(x^n)$, daí $sx^n = 0$, ou seja $a = 0$. Portanto $(x^n) \cap (y) = (0)$, mas como (0) é um ideal irredutível, e $y \neq 0$, segue pela definição de ideal irredutível que $(x^n) = (0)$. Logo $x^n = 0$, portanto (0) é um ideal primário.

■

Teorema 2.6.25. *Em um anel noetheriano R, cada ideal tem uma decomposição primária.*

Demonstração: Cada ideal é uma interseção finita de ideias irredutiveis, os quais são primários. Logo, cada ideal de R é uma interseção finita de ideais primários, possuindo assim um decomposição primária.

■

Proposição 2.6.26. *Em um anel noetheriano R, cada ideal contém uma potência de seu radical.*

Demonstração: Seja $\mathfrak{a}$ um ideal de R, logo como R é noetheriano, segue que o ideal $r(\mathfrak{a})$ é finitamente gerado. Logo existe uma quantidade finita de elementos $x_1, \ldots, x_k$ que gera $r(\mathfrak{a})$, como tais geradores pertencem ao radical de $\mathfrak{a}$, temos que existem inteiros positivos $n_1, \ldots, n_k$, tais que $x_i^{n_i} \in \mathfrak{a}$. Defina $m = 1 + \sum_{i=1}^{k} (n_i - 1)$. Deste modo, $r(\mathfrak{a})^m$ é gerado pelos produtos $\prod_{i=1}^{k} x_i^{r_i}$, em que $\sum_{i=1}^{k} r_i = m$. Agora note que existe um índice i, tal que $r_i \geq n_i$, pois caso contrário, teríamos que $r_i \leq n_i - 1$, daí $m = \sum_{i=1}^{k} r_i \leq \sum_{i=1}^{k} (n_i - 1) < m$. Logo, como $x_i^{r_i} \in \mathfrak{a}$, segue que $\prod_{i=1}^{k} x_i^{r_i} \in \mathfrak{a}$, logo como os geradores de $r(\mathfrak{a})^m$ pertence a $\mathfrak{a}$, concluimos que $r(\mathfrak{a})^m \subseteq \mathfrak{a}$.

■

2.7 Grupo de Picard

Nesta seção, mostraremos que o conjunto formado pelas classes de isomorfismos de módulos projetivos de posto 1 sobre um anel R comutativo com 1, munido de uma operação induzida pelo produto tensorial $\otimes$, é um grupo abeliano.

Proposição 2.7.1. *Se R é um anel local, então cada R-módulo projetivo finitamente gerado P é livre com $P \cong R^n$, em que $n = dim_{R/\mathfrak{m}}(P/\mathfrak{m}P)$, e $\mathfrak{m}$ é o ideal maximal de R.*

Demonstração: [16], p.8.

■

Definição 2.7.2 (**Posto de um módulo projetivo finitamente gerado**). *O posto* $n = \text{posto}_{\mathfrak{p}}(M)$ *de um* R*-módulo projetivo finitamente gerado* M *em um ideal primo* $\mathfrak{p}$ *de* R *é definido como sendo o posto do* $R_{\mathfrak{p}}$*-módulo livre* $M_{\mathfrak{p}}$*. Ou seja,* n *é tal que* $M_{\mathfrak{p}} \cong (R_{\mathfrak{p}})^n$*.*

Observação 2.7.3. *Note que pela Proposição 2.7.1,* $M_{\mathfrak{p}}$ *é livre, pois é um módulo projetivo sobre o anel local* $R_{\mathfrak{p}}$*.*

Proposição 2.7.4. *O posto* n *de um* R*-módulo projetivo finitamente gerado* M *em um ideal primo* $\mathfrak{p}$ *de* R *é dado por* $n = \text{posto}_{\mathfrak{p}}(M) = dim_{k(\mathfrak{p})}(M \otimes_R k(\mathfrak{p}))$*, em que* $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$*.*

Demonstração: Por definição de posto, $M_{\mathfrak{p}} \cong (R_{\mathfrak{p}})^n$, mas pela Proposição 2.7.1, temos que

$$n = dim_{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}(M_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}M_{\mathfrak{p}}),$$

note que $R_{\mathfrak{p}}M_{\mathfrak{p}} = M_{\mathfrak{p}}$, portanto $n = dim_{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}(M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}})$. Logo,

$$\begin{aligned} n &= dim_{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}(M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}) \\ &= dim_{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}(M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}) \\ &= dim_{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}(M \otimes_R R_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}) \\ &= dim_{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}(M \otimes_R R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}) \\ &= dim_{k(\mathfrak{p})}(M \otimes_R k(\mathfrak{p})) \end{aligned}$$

■

Observação 2.7.5. *A função* posto *de um* R*-módulo finitamente gerado* P *é definida por* $\mathfrak{p} \mapsto \text{posto}_{\mathfrak{p}}(P)$ *para cada ideal primo* $\mathfrak{p}$*. Tal função é localmente constante, quando* P *é projetivo finitamente gerado. Dizemos que um módulo finitamente gerado tem posto constante, quando a função* posto *é constante.*

Proposição 2.7.6. *Sejam* P, Q *módulos projetivos de postos constantes sobre* R*, então* $\text{posto}(P \otimes_R Q) = \text{posto}(P).\,\text{posto}(Q)$*.*

Demonstração: Temos pela Proposição 2.3.10 que $P \otimes_R Q$ é um R-módulo projetivo (finitamente gerado). Suponha que $m = \text{posto}(P)$ e $n = \text{posto}(Q)$, então para cada ideal primo $\mathfrak{p}$ de R, temos que $P_{\mathfrak{p}} \cong R_{\mathfrak{p}}^m$, $Q_{\mathfrak{p}} \cong R_{\mathfrak{p}}^n$. Portanto,

$$\begin{aligned}(P \otimes_R Q)_{\mathfrak{p}} &\cong P_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} Q_{\mathfrak{p}} \\ &\cong R_{\mathfrak{p}}^m \otimes_{R_{\mathfrak{p}}} R_{\mathfrak{p}}^n \\ &\cong \bigoplus_{i=1}^{n} (R_{\mathfrak{p}}^m \otimes_{R_{\mathfrak{p}}} R_{\mathfrak{p}}) \\ &\cong \bigoplus_{i=1}^{n} R_{\mathfrak{p}}^m \\ &\cong R_{\mathfrak{p}}^{mn}\end{aligned}$$

Logo, $\text{posto}(P \otimes_R Q) = mn = \text{posto}(P).\,\text{posto}(Q)$.

■

Proposição 2.7.7. *Sejam M e N dois R-módulos.*

(i) Se M é finitamente gerado, então o homomorfismo canônico

$$\varphi : S^{-1}\,\text{Hom}_R(M, N) \longrightarrow \text{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

é injetivo.

(ii) Se M é finitamente apresentado, então φ é bijetivo. Em particular, $\text{Hom}_R(M, N)_{\mathfrak{p}} \cong \text{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})$.

Demonstração: [7], p.76.

■

Na proposição abaixo, veremos que o módulo dual de um R-módulo projetivo de posto 1 é também projetivo de posto 1.

Proposição 2.7.8. *(Bourbaki) Sejam R um anel comutativo com* 1 *e M um R-módulo finitamente gerado.*

(i) Se existe um R-módulo N tal que $M \otimes_R N$ é isomorfo R, então o módulo M é projetivo de posto 1.

(ii) Reciprocamente, se M é projetivo de posto 1*, e M^* é seu dual, então o homomorfismo canônico*

$$u : M^* \otimes_R M \longrightarrow R$$

correspondente à forma bilinear canônica

$$(f, x) \mapsto f(x)$$

definida de $M^* \times M$ sobre R é bijetor.

Demonstração:

(i) Basta mostrarmos que $M_{\mathfrak{m}} \cong R_{\mathfrak{m}}$ para cada ideal maximal $\mathfrak{m}$ de R. Como $M \otimes_R N \cong M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{\mathfrak{m}}$, podemos substituir R por $R_{\mathfrak{m}}$, e daí supor que R é um anel local. Considere o corpo $k = R/\mathfrak{m}$ e um isomorfismo

$$v : M \otimes_R N \longrightarrow R.$$

Agora note que $R \otimes_R k \cong k$, e

$$(M \otimes_R N) \otimes_R k \cong (M \otimes_R k) \otimes_k (N \otimes_R k) \cong (M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N),$$

logo obtemos o isomorfismo

$$v \otimes 1_k : (M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N) \longrightarrow k.$$

Portanto, o posto de $(M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N)$ sobre k é 1, consequentemente, pela Proposição 2.7.6, segue que $M/\mathfrak{m}M$ e $N/\mathfrak{m}N$ têm posto 1. Logo, o módulo $M/\mathfrak{m}M$ é cíclico, mas como $\mathfrak{m}$ coincide com o radical de Jacobson do anel local R, segue que que M é cíclico, o que implica que $M \cong R/Ann(M)$. Mas $Ann(M) \subseteq Ann(M \otimes_R N) \cong Ann(R)$, mas $Ann(R) = 0$, pois se $x \in Ann(R)$, então $x.1 = 0$. Portanto, $M \cong R$.

(ii) Pela Proposição 2.5.12, segue que basta mostramos que $u_{\mathfrak{m}}$ é um isomorfismo. Temos que $M_{\mathfrak{m}}$ e $(M_{\mathfrak{m}})^*$ são $R_{\mathfrak{m}}$-livres de posto 1, daí o homomorfismo canônico

$$u_{\mathfrak{m}} : M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} (M_{\mathfrak{m}})^* \longrightarrow R_{\mathfrak{m}}$$

é bijetivo.

■

Proposição 2.7.9. *Sejam P e Q módulos projetivos finitamente gerados sobre um anel R noetheriano comutativo com 1, então* $\text{posto}(\text{Hom}_R(P, Q)) = \text{posto}(P).\,\text{posto}(Q)$. *Em particular,* $\text{posto}(P^*) = \text{posto}(P)$.

Demonstração: Suponha que $m = \text{posto}(P)$ e $n = \text{posto}(Q)$. Seja $\mathfrak{p}$ um ideal primo de R, então $P_{\mathfrak{p}} \cong R_{\mathfrak{p}}^m$ e $Q_{\mathfrak{p}} \cong R_{\mathfrak{p}}^n$. Portanto,

$$\begin{aligned}(\mathrm{Hom}_R(P,Q))_{\mathfrak{p}} &\cong \mathrm{Hom}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}^m, R_{\mathfrak{p}}^n)\\ &\cong \mathrm{Hom}_{R_{\mathfrak{p}}}(\textstyle\bigoplus_{i=1}^m R_{\mathfrak{p}}, R_{\mathfrak{p}}^n)\\ &\cong \textstyle\bigoplus_{i=1}^m \mathrm{Hom}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}, R_{\mathfrak{p}}^n)\\ &\cong \textstyle\bigoplus_{i=1}^m \bigoplus_{j=1}^n \mathrm{Hom}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}, R_{\mathfrak{p}})\\ &\cong \textstyle\bigoplus_{i=1}^m \bigoplus_{j=1}^n R_{\mathfrak{p}}\\ &\cong {R_{\mathfrak{p}}}^{mn}\end{aligned}$$

Portanto, $\mathrm{posto}(\mathrm{Hom}_R(P,Q)) = \mathrm{posto}(P).\,\mathrm{posto}(Q)$. Note que, em particular, $\mathrm{posto}(P^*) = \mathrm{posto}(P).\,\mathrm{posto}(R) = \mathrm{posto}(P)$.

■

Definição 2.7.10. *Definimos $Pic(R)$ como sendo o conjunto de todas as classes de isomorfismos $[P]$ dos módulos projetivos P de posto* 1 *sobre um anel comutativo com unidade R.*

Proposição 2.7.11. *A operação $[\otimes]$ dada por $[P][Q] = [P \otimes_R Q]$ está bem definida sobre $Pic(R)$.*

Demonstração: Com efeito, se $[P] = [P']$, e $[Q] = [Q']$, então $P \cong P'$, e $Q \cong Q'$. Logo, $P \otimes_R Q \cong P' \otimes_R Q'$. Daí $[P \otimes_R Q] = [P' \otimes_R Q']$. Note que pela Proposição 2.7.6, $P \otimes_R Q$ é de fato um R-módulo projetivo de posto 1.

■

Proposição 2.7.12. Pic(R) *munido da operação induzida pelo produto tensorial $\otimes$, definida acima, é um grupo abeliano.*

Demonstração: Pela Proposição 2.7.11, temos que a operação $[\otimes]$ está bem definida sobre Pic(R). Sejam A, B e C módulos projetivos de posto 1 sobre R. Temos:

Associatividade: Temos pela Proposição 2.2.10, que $(A \otimes_R B) \otimes_R C \cong A \otimes_R (B \otimes_R C)$.

Comutatividade: Temos pela Proposição 2.2.8, que $A \otimes_R B \cong B \otimes_R A$.

Elemento neutro: Temos pela Proposição 2.2.9, que $A \otimes_R R \cong A$.

Elemento inverso: Temos pela Proposição 2.7.8 item (ii), que $A \otimes_R A^* \cong R$.

Portanto, Pic(R) é um grupo abeliano.

■

Definição 2.7.13. *O grupo* Pic(R) *é chamado de* ***grupo de Picard do anel R****.*

CAPÍTULO 3

RESULTADOS PRINCIPAIS

Neste capítulo, mostraremos com base em [3], que extensões finitamente geradas de grupos abelianos por grupos policíclicos satisfazem a condição maximal sobre subgrupos normais, max-n. Deste modo, em particular, grupos metabelianos finitamente gerados satisfazem max-n. Apresentaremos também um exemplo, com base em [2], de um grupo metabeliano finitamente apresentado, o qual portanto tem max-n. Além disso, com base em [1], construíremos grupos metabelianos não-isomorfos que têm os mesmos quocientes finitos. Por conveniência, usaremos a notação $H < G$ para indicar que H é subgrupo próprio de G.

3.1 Condição maximal

Definição 3.1.1. *Um grupo com conjunto de operadores Ω à direita é uma tripla (G, Ω, α) consistindo de um grupo G, de um conjunto Ω, chamado domínio de operadores, e de uma função $\alpha : G \times \Omega \longrightarrow G$, tal que para cada $\omega \in \Omega$ fixado, $g \mapsto (g, \omega)\alpha$ é um endomorfismo de G . Analogamente, definimos grupo com operadores à esquerda. Chamamos G de $\Omega-$grupo.*

Notação: Denotemos $(g, \omega)\alpha$ por g^{ω}.
Deste modo, um $\Omega-$grupo G é um grupo com um conjunto de operadores que agem sobre G como endomorfismos, i.e, $(gh)^{\omega} = g^{\omega}h^{\omega}$ para cada $\omega \in \Omega$ e para todos $g, h \in G$

Definição 3.1.2. *Se G é um $\Omega-$grupo, definimos um $\Omega-$subgrupo H de G como um subgrupo de G que é $\Omega-$admissível, i.e, $h^{\omega} \in H$ sempre que $h \in H$ e $\omega \in \Omega$.*

Observação 3.1.3. *Note que cada $\Omega-$subgrupo H de um $\Omega-$grupo G é também um $\Omega-$grupo.*

Proposição 3.1.4. *A interseção de um conjunto de $\Omega-$subgrupos é um $\Omega-$subgrupo.*

Demonstração: Seja $\mathfrak{F} = \{H_\sigma\}$ uma família de $\Omega-$subgrupos de um Ω-grupo G. Tome $h \in \bigcap_\sigma H_\sigma$, então como cada H_σ é $\Omega-$admissível, segue que para cada σ, $h^\omega \in H_\sigma$, $\forall \omega \in \Omega, \forall h \in H$, daí $h^\omega \in \bigcap_\sigma H_\sigma$, $\forall \omega \in \Omega, \forall h \in H$.

■

Definição 3.1.5. *O $\Omega-$subgrupo gerado por um subconjunto não-vazio X é definido como sendo a interseção de todos os $\Omega-$subgrupos contendo X.*

Notação: X^Ω

Observação 3.1.6. *Temos que $X^\Omega = \{(x_1^{\xi_1})^{\omega_1} \dots (x_r^{\xi_r})^{\omega_r} \mid x_i \in X, \xi_i = \pm 1, r \geq 0\}$, em que (ω_i) é uma sequência de Ω aplicada sucessivamente.*

Observação 3.1.7. *Se N é um $\Omega-$subgrupo normal de um $\Omega-$grupo G, então podemos tornar G/N em um $\Omega-$grupo quociente, definindo $(Ng)^\omega = Ng^\omega$.*

Definição 3.1.8. *Um $\Omega-$homomorfismo $\alpha : G \longrightarrow H$ é um homomorfismo entre os $\Omega-$grupos G e H, tal que $(g^\omega)^\alpha = (g^\alpha)^\omega$, para todo $g \in G$ e para todo $\omega \in \Omega$. Denotamos o conjunto de todos $\Omega-$homomorfismos de G em H por $Hom_\Omega(G, H)$.*

Exemplo 3.1.9. *(i) Se $\Omega = R$ é um anel, e M é um R-módulo à direita, então M é um $R-$grupo com domínio de operadores à direita R. Deste modo, módulos são exemplos de grupos com operadores:*
Como M é um $R-$módulo à direita, existe uma ação linear $\alpha : M \times R \longrightarrow M$, denote por g^ω a imagem $(g, \omega)\alpha$, deste modo, temos que $(gh)^\omega = g^\omega h^\omega$, uma vez que $\Omega = R$ age linearmente em M;

(ii) Sejam G um grupo, e $\Omega = End(G)$. Então, G é um $\Omega-$grupo se os endomorfismos de G operarem sobre G de forma natural, i.e, $g^\omega = (g)\omega$, imagem de $g \in G$ por $\omega \in End(G)$. Note que, deste modo, um $\Omega-$subgrupo de G é um subgrupo completamente invariante.

(iii) Um grupo G é um grupo com operadores $\Omega = Aut(G)$, grupo dos automorfismos de G. Daí, os $\Omega-$subgrupos de G são os subgrupos característicos de G.

(iv) Um grupo G é um grupo com operadores com respeito a $\Omega = Inn(G)$, grupo dos automorfismos internos de G, deste modo, os $\Omega-$subgrupos de G são os subgrupos normais de G. Note que, os $\Omega-$endomorfismos de G são precisamente estes endormorfismos (chamados de normais) que comutam com cada automorfismo interno de G, ou seja, se $\alpha : G \longrightarrow G$ é um $\Omega-$endomorfismo, então $(g^{\omega})^{\alpha} = (g^{\alpha})^{\omega}$, para todo $g \in G$, e para todo $\omega \in \Omega = Inn(G)$. Note também que, X^{Ω} coincide com o fecho normal X^{G}, uma vez que, X^{Ω} é a interseção de todos $Inn(G)-$subgrupos de G que contém X, mas os $Inn(G)-$subgrupos de G são precisamente os subgrupos normais de G que contêm X, portanto $X^{\Omega} = X^{G}$.

Definição 3.1.10. *Considere que Λ seja um conjunto parcialmente ordenado. Dizemos que Λ satisfaz a condição maximal, quando cada subconjunto não-vazio Λ_0 de Λ contém pelo menos um elemento maximal.*

Definição 3.1.11. *Um conjunto parcialmente ordenado Λ satisfaz a condição de cadeia ascendente, quando não existe uma cadeia ascendente propriamente infinita $\lambda_1 < \lambda_2 < \ldots$ em Λ.*

Proposição 3.1.12. *Um conjunto parcialmente ordenado Λ satisfaz a condição maximal se, e somente se, satisfaz a condição de cadeia ascendente.*

Demonstração: Suponha que Λ não satisfaça a condição maximal, então existe um subconjunto não-vazio Λ_0 de Λ que não possui elemento maximal, logo dado qualquer elemento $\lambda_i \in \Lambda$, temos que este não é maximal, portanto existe $\lambda_{i+1} \in \Lambda$ tal que $\lambda_i < \lambda_{i+1}$, de modo que obtemos uma cadeia ascendente infinita $\lambda_1 < \lambda_2 < \ldots$ em Λ, portanto Λ não satisfaz a condição ascendente. Reciprocamente, suponha que exista uma cadeia ascendente infinita $\lambda_1 < \lambda_2 < \ldots$ em Λ, então o subconjunto $\Lambda_0 = \{\lambda_i \mid \ i \in \mathbb{N}\}$ de Λ não tem elemento maximal, logo Λ não satisfaz a condição maximal.

■

Notação: Denotemos por $\mathsf{F}(G)$, o conjunto de todos $\Omega-$subgrupos do $\Omega-$grupo G. Note que $\mathsf{F}(G)$ é parcialmente ordenado pela inclusão.

Definição 3.1.13. *Um $\Omega-$grupo satisfaz a condição maximal, quando $\mathsf{F}(G)$ satisfaz a condição maximal. Denotemos tal condição por max$-\Omega$, em outros termos, a condição maximal sobre $\Omega-$subgrupos de G.*

Observação 3.1.14. *Se $\Omega = Inn(G)$, então max−Ω será denotado por max−n, a condição maximal sobre subgrupos normais. Equivalentemente, temos que max−G representa a mesma condição.*

Observação 3.1.15. *Se $\Omega = \emptyset$, indiquemos por max, a condição maximal sobre subgrupos.*

Proposição 3.1.16. *Um $\Omega-$grupo G satisfaz max−Ω se, e somente se, cada $\Omega-$subgrupo de G é finitamente gerado como um $\Omega-$grupo.*

Demonstração:
($\Leftarrow$) Considere que G seja um $\Omega-$grupo que tem max−Ω, e que H seja um $\Omega-$subgrupo de G. Suponha, por absurdo, que H não seja finitamente gerado como $\Omega-$grupo, i.e, não existe um conjunto finito $\{h_1 \dots h_n\}$ de elementos de H, tal que $H = \langle h_1, \dots, h_n\rangle^{\Omega}$. Deste modo, dado $h_1 \in H$, segue que $H_1 = \langle h_1\rangle^{\Omega} \neq H$, logo existe $h_2 \in H\backslash H_1$, de modo que $H_1 < H_2 = \langle h_1, h_2\rangle^{\Omega} \neq H$, analogamente, existe $h_3 \in H\backslash H_2$, tal que $H_1 < H_2 < H_3 = \langle h_1, h_2, h_3\rangle^{\Omega} \neq H$, como H não é finitamente gerado como $\Omega-$grupo, segue que esse processo é infinito, de modo que $H_n < H, \forall n \in \mathbb{N}$, assim $H_1 < H_2 < \dots$ é uma cadeia infinita de $\Omega-$subgrupos de G, o que contradiz a condição max−Ω.
($\Rightarrow$) Considere que cada Ω-subgrupo de G seja finitamente gerado como Ω-grupo. Suponha, por absurdo, que G não tenha max−Ω, logo existe uma cadeia ascendente propriamente infinita $H_1 < H_2 < \dots$ de $\Omega-$subgrupos de G. Defina $H = \bigcup_{i=1}^{\infty} H_i$, deste modo, como temos $H_i < H_{i+1}$, segue que H é um $\Omega-$subgrupo, portanto por hipótese, segue que H é finitamente gerado como $\Omega-$grupo, daí existe um conjunto finito $\{h_1, \dots, h_n\}$ de elementos de H tal que $H = \langle h_1, \dots, h_n\rangle^{\Omega}$. Agora, para n suficientemente grande, segue que cada $h_i \in H_n$, deste modo, $H_n = H$, que é uma contradição, pois a cadeia $H_1 < H_2 < \dots$ é propriamente infinita.

■

Lema 3.1.17. *Se $H \leq K \leq G$, e $N \trianglelefteq G$. Então, as equações $HN = KN$ e $H \cap N = K \cap N$ implicam que $H = K$.*

Demonstração: Por hipótese, $H \leq K$. Mostremos que $K \subseteq H$. Seja $k \in K$, então $k = k.1 \in KN = HN$ (note que KN e HN são grupos, pois $N \trianglelefteq G$), logo existem $h \in H$, e $n \in N$, tais que $k = hn$. Logo $kh^{-1} = n \in K \cap N$, mas $K \cap N = H \cap N$, portanto $kh^{-1} \in H \cap N$. Daí, $kh^{-1} \in H$, consequentemente $k \in H$.

■

Proposição 3.1.18. *A propriedade max−Ω é fechada com respeito à formação de extensões. Mais precisamente, se $N \trianglelefteq G$, e N e G/N têm max−Ω, então o Ω−grupo G tem max−Ω.*

Demonstração: Considere que N e G/N tenham max−Ω. Suponha, por absurdo, que G não tenha max−Ω, logo existe uma cadeia ascendente propriamente infinita $H_1 \leq H_2 \leq \ldots$ de Ω−subgrupos de G, da qual obtemos as cadeias ascendentes

$$H_1 \cap N \leq H_2 \cap N \leq \ldots$$
$$\frac{H_1 N}{N} \leq \frac{H_2 N}{N} \leq \ldots.$$

Agora, já que exitem infinitos índices i, tais que $H_i < H_{i+1}$, usando a contrapositiva do Lema 3.1.17, segue que $H_i N < H_{i+1} N$ ou $H_i \cap N < H_{i+1} \cap N$, de modo que pelo menos uma dentre estas duas últimas cadeias é propriamente infinita, portanto, N ou G/N não tem max−Ω, que é uma contradição.

■

Corolário 3.1.19. *A propriedade max-n, condição maximal para subgrupos normais, é uma propriedade fechada para extensões*

Demonstração: Basta toma $\Omega = Inn(G)$ na Proposição 3.1.18.

■

Proposição 3.1.20. *Sejam G um grupo, e $H \trianglelefteq G$. Então, se H e G/H são finitamente apresentados, então G é finitamente apresentado.*

Demonstração: Suponha que $H = \langle a_1, \ldots, a_r \mid h_1(a) = \ldots = h_\rho(a) = 1 \rangle$, $G/H = \langle b_1 H, \ldots, b_s H \mid k_1(bH) = \ldots = k_\sigma(bH) = H \rangle$ sejam apresentações de H e G/H. Escolha para cada classe $b_i H$ o representante b_i. Então, podemos encontrar relações $k_\alpha(b) = f_\alpha(a)$, $\alpha = 1, \ldots, \sigma$, e como $H \trianglelefteq G$, temos as relações $b_i^{-1} a_j b_i = g_{ij}(a)$, $i = 1, \ldots, s; j = 1, \ldots r$, em que f_α e g_{ij} são funções-palavra escolhidas convenientemente. Portanto, temos que G tem apresentação $G = \langle a_1, \ldots, a_r, b_1, \ldots b_s \mid k_\alpha(b) = f_\alpha(a), h_1(a) = \ldots = h_\rho(a) = 1, b_i^{-1} a_j b_i = g_{ij}(a), \alpha = 1, \ldots, \sigma, i = 1, \ldots, s; j = 1, \ldots r \rangle$. Logo, G é finitamente gerado com $r + s$ geradores e $\sigma + \rho + rs$ relações.

■

3.2 Grupos abelianos finitamente gerados por policíclicos

Definição 3.2.1. *Um grupo G é chamado solúvel, quando possui uma série (ou cadeia) subnormal de subgrupos de G*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_i \trianglelefteq G_{i+1} \trianglelefteq \ldots \trianglelefteq G_n = G,$$

tal que cada fator G_{i+1}/G_i é abeliano. Tal série é chamada série solúvel.

Definição 3.2.2. *Um grupo G é chamado policíclico, quando possui uma cadeia de subgrupos de G*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_i \trianglelefteq G_{i+1} \trianglelefteq \ldots \trianglelefteq G_n = G,$$

tal que cada fator G_{i+1}/G_i é cíclico. Tal série é chamada série cíclica.

Observação 3.2.3. *Note que grupos policíclicos são solúveis.*

Proposição 3.2.4. *Um grupo é policíclico se, e somente se, é solúvel e satisfaz a condição maximal, max.*

Demonstração:
($\Rightarrow$) Suponha que G seja um grupo policíclico, logo existe uma série subnormal

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_i \trianglelefteq G_{i+1} \trianglelefteq \ldots \trianglelefteq G_n = G,$$

tal que cada fator G_{i+1}/G_i é cíclico, logo G é solúvel. Temos que $G_0 = 1$ e G_1/G_0 são cíclicos, logo têm max, daí como a propriedade max é fechada para extensões, segue que G_1 tem max, com o mesmo argumento segue que G_2 também tem max, procedendo assim, obtemos que $G_n = G$ tem max.
($\Leftarrow$) Seja G um grupo solúvel que tenha max, então existe $n \in \mathbb{N}$ tal que $G^{(n)} = 1$, ou seja, temos uma série derivada de comprimento finito, digamos $G \geq G' \geq G'' \geq \ldots \geq G^{(n-1)} \geq G^{(n)} = 1$, temos que cada fator $G^{(i)}/G^{(i+1)}$ é abeliano, assim como G tem max, segue que os grupos G^i são finitamente gerados, logo os fatores $G^{(i)}/G^{(i+1)}$ são grupos abelianos finitamente gerados, deste modo, podemos refinar a série derivada de G, obtendo todos fatores desta nova série cíclicos, portanto G é policíclico.

Proposição 3.2.5. *Se G é um grupo policíclico, então G é finitamente apresentado.*

Demonstração: Seja G um grupo policíclico, então G possui uma série cíclica

$$G_0 = 1 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G,$$

temos que G_0 e G_1/G_0 são cíclicos, portanto são finitamente apresentados, logo G_1 é finitamente apresentado, pois tal propriedade é fechada para extensões (Proposição 3.1.20). Prosseguindo desta mesma forma, concluímos que $G_n = G$ é finitamente apresentado.

■

Proposição 3.2.6. *(Mal'cev) Considere que H seja um subgrupo de um grupo policíclico G. Então, H é igual a interseção de todos subgrupos normais de índice finito em G que contêm H.*

Corolário 3.2.7. *Grupos policíclicos são residualmente finitos. Mais precisamente, se G é um grupo policíclico, então a interseção de todos subgrupos normais de G de índice finito em G é trivial.*

Demonstração: Basta tomar $H = 1$ na Proposição 3.2.6.

■

Proposição 3.2.8. *Sejam G um grupo com subgrupo normal H, e R um anel comutativo com 1. Considere que G/H seja finito ou cíclico infinito. Suponha que M seja um $RG-$módulo, e que N seja um $RH-$submódulo. Se N gera M como um $RG-$módulo, e N é $RH-$noetheriano, então M é $RG-$noetheriano.*

Demonstração:

(i) Considere que G/H seja finito, e que $T = \{t_1, \ldots, t_k\}$ seja um transversal de H em G. Por hipótese, temos que N gera M como $RG-$módulo, logo $M = (N)RG$. No entanto, $G = \bigcup_{i=1}^{k} Ht_i$, e como N é um $RH-$módulo, segue que $M = Nt_1 + \ldots + Nt_k$. Agora note que cada Nt_i é um $RH-$submódulo de N, uma vez que, se $n_1t_i, n_2t_i \in Nt_i$, então $n_1t_i \pm n_2t_i = (n_1 \pm n_2)t_i \in Nt_i$, e se $n \in N$, $x = \sum_{j=1}^{l} r_jh_j \in RH$, temos que $nt_ix = nt_i\sum_{j=1}^{l} r_jh_j = \sum_{j=1}^{l} nt_ir_jh_j = \sum_{j=1}^{l}(nr_j)t_ih_j = \sum_{j=1}^{l} n_jt_ih_j = \sum_{j=1}^{l} n_jt_ih_jt_i^{-1}t_i = \sum_{j=1}^{l} n_jh_j^{t_i^{-1}}t_i$, em que $n_j = nr_j$ é um elemento de N. Mas como $H \trianglelefteq G$, segue que $h_j^{t_i^{-1}} \in H$, daí $n_jh_j^{t_i^{-1}} \in N$, pois N é RH-módulo, e $1 \in R$. Deste modo, para cada j temos que $n_jh_j^{t_i^{-1}}t_i \in Nt_i$, logo $nt_ix = \sum_{j=1}^{l} n_jh_j^{t_i^{-1}}t_i \in Nt_i$. Portanto Nt_i é um

$RH-$submódulo de N para cada $i = 1, \ldots, k$. Mostremos agora que, se N_0 é um $RH-$submódulo de N, então a aplicação $\psi_i : N_0 \longrightarrow N_0 t_i$, definida por $\psi_i(n) = nt_i$ é um $R-$isomorfismo para cada i entre RH-submódulos de N e de Nt_i. Com efeito, para $n_1, n_2 \in N_0$, e $r \in R$, temos que $\psi_i(n_1 \pm n_2) = (n_1 \pm n_2)t_i = n_1 t_i \pm n_2 t_i = \psi_i(n_1) \pm \psi_i(n_2)$, e $\psi_i(nr) = (nr)t_i = nt_i r = \psi_i(n)r$. Por hipótese, N é $RH-$noetheriano, daí os $RH-$submódulos de N têm max$-RH$, logo via ψ_i segue que os $RH-$submódulos de Nt_i têm max$-RH$, mas como pela Proposição 3.1.18 a condição max$-RH$ é fechada para extensões, segue que M tem max$-RH$, i.e, M é $RH-$noetheriano. No entanto, $RG = \sum_{i=1}^{k} RHt_i$, logo o $RG-$submódulo M é $RG-$noetheriano.

(ii) Considere que G/H seja cíclico infinito, e suponhamos que G/H seja gerado por Ht, deste modo, cada elemento $a \in M$ pode ser escrito, não necessariamente de forma única, como $a = \sum_{i=r}^{s} b_i t_i$, em que $b_i \in N$, $r \leq s$, note que r pode ser negativo; no caso de $b_s \neq 0$, denominemos $b_s t^s$ e b_s, por termo líder e coeficiente líder de a, respectivamente. Seja M_0 um $RG-$submódulo de M não-nulo, mostremos que M_0 é finitamente gerado, e daí M é $RG-$noetheriano. Com efeito, definamos N_0, como sendo o conjunto consistindo de 0 e de todos coeficientes líderes dos elementos do $RG-$módulo M_0, temos que N_0 é um $RH-$submódulo de N. De fato, suponha que b_r e b_s sejam elementos de N_0 com respectivos termos líderes $b_t t^r$ e $b_s t^s$ provenientes dos elementos a e a' de M_0. Suponha sem perda de generalidade que $r \leq s$, assim temos que $a \pm a' t^{r-s}$ é um elemento de M_0, cujo coeficiente líder é $b_r \pm b_s$, exceto se este for nulo, mas em todo caso, temos que $b_r \pm b_s \in N_0$. Agora, tome $x \in RH$, então $a(t^{-s} x t^s) \in M_0$ e possui termo líder $(b_s x)t^s$, exceto se este for nulo, então em todo caso, temos que o coeficiente $b_s x \in N_0$, portanto N_0 é um $RH-$módulo. Temos, por hipótese, que N tem max$-RH$, logo como N_0 é um $RH-$submódulo de N, segue que existe um conjunto finito $\{b_1, \ldots, b_k\}$ de elementos não-nulos que geram N_0 como $RH-$módulo. Deste modo, como cada $b_i \in N_0$, segue que existem elementos $a_i \in M_0$, cujos coeficientes líderes são b_i, alteremos se necessário os termos líderes de a_i multiplicando-os por potências de t com o intuito de obter termos líderes com o mesmo grau positivo m, em suma, $b_i t^m$. Suponhamos sem perda de generalidade que, $a_1, \ldots, a_k$ sejam os elementos de M_0 após essa alteração. Definamos M_1 como sendo o $RG-$submódulo de M_0 gerado por $a_1, \ldots, a_k$, e definamos N_1 por $N_1 = M_0 \cap (N + Nt + \ldots Nt^{m-1})$, assim como no caso (i), segue que $N + Nt + \ldots + Nt^{m-1}$ tem max$-RH$. Logo como N_1 é um

$RH-$submódulo deste, segue que N_1 tem max$-RH$, logo o $RG-$módulo $M_2 = M_1 + (N_1)RG$ é finitamente gerado como $RG-$módulo. Mostremos que $M_2 = M_0$, concluindo assim a prova. Temos que $M_0 \leq M_2$, suponha por absurdo que, exista $a \in M_0 \backslash M_2$, e suponha sem perda de generalidade que a não possua potências negativas de t e que dentre todos elementos de M_0 nessas condições a seja escolhido de tal modo que ct^p seja o seu termo líder, cuja potência de t é a menor possível, isto é, p é a menor potência de t dentre todos elementos de $M_0 \leq M_2$. Se $p \leq m$, então $a \in M_0 \cap (N + Nt + \ldots + Nt^{m-1}) = N_1 < M_2$, daí $a \in M_2$, que é uma contradição. Então, $p \geq m$, como c é coeficiente líder de a, segue que $c \in N_0$, logo podemos escrever c como $c = \sum_{i=1}^{k} b_i x_i$, em que $x_i \in RH$, assim o elemento $a' = \sum_{i=1}^{k} a_i(t^{-m} x_i t^p)$ pertence a M_2, não possui potências negativas de t e possui termo líder $(\sum_{i=i}^{k} b_i x_i)t^p = ct^p$, de modo que $a - a'$ tem o mesmo termo líder, daí $a - a' \in M_0 \backslash M_2$ e não envolve potências de t maiores que $p-1$, o que contradiz a minimalidade de p na escolha de $a \in M_0 \backslash M_2$. Logo $M_0 = M_2$, e portanto M_0 é finitamente gerado como $RG-$módulo.

■

Proposição 3.2.9. *Sejam G uma extensão finita de um grupo policíclico, e R um anel noetheriano à direita com* 1*. Então, o anel de grupo RG é noetheriano à direita.*

Demonstração: Temos que G é policíclico-por-finito, logo G possui umas série subnormal $1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G$, cujos fatores são finitos ou cíclicos infinitos. Mostremos que RG é noetheriano à direita, fazendo indução sobre $n \geq 0$. Se $n = 0$, então $G_0 = G = 1$, daí $RG = R$. Portanto RG é noetheriano à direita, pois R o é. Suponha que para todo $k < n$ o resultado seja válido, isto é, qualquer grupo nas condições acima tem seu anel de grupo sobre R noeheriano à direita. Deste modo, para $H = G_{n-1}$, segue pela hipótese de indução que RH é um anel noetheriano à direita, daí como RH-módulo tem max$-RH$. Assim considerando $M = RG$, $N = RH$, e notando que $H \trianglelefteq G$, G/H é finito ou cíclico infinito, e que M e N são trivialmente RG e $RH-$módulos, respectivamente, $M = RG$ gera $N = RH$ como $RG-$módulo, e $N = RH$ é $RH-$noetheriano à direita, temos portanto as hipóteses da Proposição 3.2.8. Portanto $M = RG$ é noetheriano à direita, logo pelo Princípio de Indução segue que o resultado é válido para todo $n \geq 0$. Em suma, RG é noetheriano à direita para qualquer G policíclico-por-finito.

■

Teorema 3.2.10. *Um grupo finitamente gerado G que é uma extensão de um grupo abeliano por um grupo policíclico satisfaz a condição maximal sobre subgrupos normais.*

Demonstração: Temos que G possui um subgrupo normal abeliano A, tal que $H = G/A$ é policíclico. Podemos considerar A como um $\mathbb{Z}H-$módulo via conjugação. Por hipótese, G é finitamente gerado, e temos que H é finitamente apresentado, pois é policílico, logo A é finitamente gerado como $\mathbb{Z}H-$módulo. Assim considerando A em notação aditiva, segue que A é uma soma de uma quantidade finita de $\mathbb{Z}H-$módulos cíclicos. No entanto um $\mathbb{Z}H-$módulo cíclico tem max$-\mathbb{Z}H$, já que é uma imagem do anel $\mathbb{Z}H$, o qual é noetheriano à direita pela Proposição 3.2.9. Portanto A tem max$-\mathbb{Z}H$, daí tem max$-G$, que é equivalente a max$-n$.

■

Definição 3.2.11. *Um grupo G é **metabeliano** quando possui um subgrupo normal abeliano A, tal que G/A é abeliano.*

Agora note que se G é um grupo metabeliano finitamente gerado, então G é uma extensão de um grupo abeliano A por um grupo abeliano finitamente gerado G/A, o qual é solúvel e tem *max*, sendo portanto policíclico. Deste modo, um grupo metabeliano finitamente gerado é uma extensão finitamente gerada de um grupo abeliano por um grupo policíclico. Obtemos deste modo o seguinte resultado:

Corolário 3.2.12. *Grupos metabelianos finitamente gerados tem max$-n$.*

■

Corolário 3.2.13. *Se G é um grupo metabeliano finitamente apresentado, então todo quociente de G é finitamente apresentado.*

Demonstração: Considere que $\varphi : F \longrightarrow G$ seja uma apresentação para G, e que

$$\pi : G \longrightarrow G/N$$

seja o epimorfismo canônico. Então $\pi \circ \varphi$ é uma apresentação para G/N, cujo núcleo é $\varphi^{-1}(N)$, mas como G tem *max*-n , segue que N é finitamente gerado, logo $\mathrm{Ker}(\pi \circ \varphi)$ é finitamente gerado, portanto G/N é finitamente apresentado.

3.3 Exemplo de Baumslag

Daremos agora um exemplo, que será utilizado no capítulo posterior, de um grupo metabeliano finitamente apresentado, construído por Baumslag em [2].

Exemplo 3.3.1. *O grupo com apresentação dada por*

$$K = \langle t, s, y_1, \ldots, y_m \mid [t,s] = 1, y_i^s = y_i y_i^t, [y_i, y_j] = [y_i, y_j^t] = 1, 1 \leq i, j \leq m \rangle.$$

é metabeliano.

Consideremos o caso com 3 geradores e 3 relações, ou seja,

$$K_0 = \langle t, s, y \mid [t,s] = 1, y^s = yy^t, [y, y^t] = 1 \rangle.$$

Mostremos que K_0' é abeliano, deste modo como K_0/K_0' é abeliano, segue que K_0 é metabeliano.

Afirmação 1: O grupo derivado K_0' é gerado pelos conjugados $y^{t^i s^j}$, $i, j \in \mathbb{Z}$.

Demonstração: Seja K_1 o grupo gerado pelos conjugados $y^{t^i s^j}$, $i, j \in \mathbb{Z}$. Note que $K_1 \trianglelefteq K_0$, uma vez que $(y^{t^i s^j})^u \in K_1$ para $u \in \{t, s, y\}$. Além disso, K_0/K_1 é abeliano, pois dois elementos xK_1, yK_1 pertencentes ao grupo K_0/K_1 comutam se, e somente se, $xK_1yK_1 = yK_1xK_1 \Leftrightarrow xyK_1 = yxK_1 \Leftrightarrow [x,y] \in K_1$, e temos que os comutadores aplicados nos geradores $[t,s] = 1, [t,y] = (y^t)^{-1}y, [y,s] = y^{-1}y^s = y^{-1}yy^t = y^t$ pertencem a K_1, logo $K_0' \leq K_1$. Por outro lado, temos que cada conjugado $y^{t^i s^j} = (y^{t^i})^{s^j} = ([y,s]^{t^{i-1}})^{s^j} = [y^{t^{i-1}s^j}, s^{t^{i-1}s^j}] \in K_0'$, logo $K_1 \leq K_0'$. Portanto, $K_0' = K_1$.

■

Queremos mostrar que K_0' é abeliano, deste modo, como K/K_0' é abeliano, segue portanto que K_0 é metabeliano.

Afirmação 2: Os conjugados y^{t^i}, $i \in \mathbb{Z}$ comutam.

Demonstração: Temos que $[y, y^t] = 1$, daí $\langle y, y^t \rangle$ é abeliano. Suponha que $\langle y, y^t, \ldots, y^{t^n} \rangle$ seja abeliano para algum $n \in \mathbb{N}$, deste modo, $\langle y^t, y^{t^2}, \ldots, y^{t^{n+1}} \rangle$ é abeliano, pois para cada $i = 1, \ldots, n+1$, temos que $y^{t^i} y^{t^{n+1}} = t^{-i}yt^i t^{-(n+1)}yt^{n+1} = t^{-i}y(t^{-(n+1-i)}yt^{n+1-i})t^i = t^{-i}yy^{t^{n+1-i}}t^i = t^{-i}y^{t^{n+1-i}}yt^i = (t^{-(n+1)}yt^{n+1})(t^{-i}yt^i) = y^{t^{n+1}}y^{t^i}$. Agora, mostremos que y comuta com $y^{t^{n+1}}$, e daí $\langle y, y^t, y^{t^2}, \ldots, y^{t^{n+1}} \rangle$ é abeliano, e pelo princípio de indução, segue que $\langle y, y^t, y^{t^2}, \ldots, y^{t^{n+1}} \rangle$ é abeliano $\forall n \in \mathbb{N}$. Com efeito,

$1 = [y, y^{t^n}] = [y, y^{t^n}]^s = [y^s, (y^{t^n})^s] = [y^s, y^{t^n s}] = [y^s, y^{st^n}] = [y^s, (y^s)^{t^n}] = [yy^t, (yy^t)^{t^n}] =$
$[yy^t, y^{t^n} y^{t^{n+1}}] = (y^t)^{-1} y^{-1} (y^{t^{n+1}})^{-1} (y^{t^n})^{-1} yy^t y^{t^n} y^{t^{n+1}} =$
$(y^t)^{-1} y^{-1} (y^{t^{n+1}})^{-1} yy^t ((y^{t^n})^{-1} y^{t^n}) y^{t^{n+1}} = (y^t)^{-1} y^{-1} (y^{t^{n+1}})^{-1} yy^t y^{t^{n+1}} =$
$y^{-1} (y^{t^{n+1}})^{-1} ((y^t)^{-1} y^t) yy^{t^{n+1}} = y^{-1} (y^{t^{n+1}})^{-1} yy^{t^{n+1}} = [y, y^{t^{n+1}}]$. Como queríamos.

Note que usamos que $\langle y^t, y^{t^2}, \ldots, y^{t^{n+1}} \rangle$ e $\langle y, y^t, \ldots, y^{t^n} \rangle$ são abelianos.

■

Afirmação 3: Se $j \geq 0$, então y^{s^j} é um produto dos elementos $y, y^t, \ldots, y^{t^j}$.
Demonstração: Basta usar as relações $y^s = yy^t$ e $ts = st$ e inserir termos da forma ss^{-1} afim de obter conjugados. Por exemplo, $y^{s^2} = s^{-2} y s^2 = s^{-1} y^s s = s^{-1} yy^t s = s^{-1} y (ss^{-1}) y^t s = y^s (y^t)^s = y^s (y^s)^t = yy^t (yy^t)^t = yy^t y^t y^{t^2} = y (y^t)^2 y^{t^2}$

■

Lema 3.3.2. $[y, y^{t^i s^j}] = 1, \forall i, j \in \mathbb{Z}$

Demonstração: Deste modo, usando as Afirmações 2 e 3, segue que $[y, y^{t^i s^j}] = [y^{t^{-1}}, y^{s^j}]^{t^i} = 1^{t^i} = 1, \forall i \in \mathbb{N}, \forall j \geq 0$. E para $j < 0$, temos que $1 = [y^{s^{-j}}, y^{t^i}] = [y^{s^{-j}}, y^{t^i}]^{s^j} = [y, y^{t^i s^j}]$. Portanto, $[y, y^{t^i s^j}] = 1, \forall i, j \in \mathbb{Z}$.

■

Lema 3.3.3. *O grupo derivado de*

$$K_0 = \langle t, s, y \mid [t, s] = 1, y^s = yy^t, [y, y^t] = 1 \rangle$$

é abeliano.

Demonstração: Basta mostrarmos que os comutadores entre geradores são triviais, de fato $[y^{t^k s^l}, y^{t^i s^j}] = [y, y^{t^{i-k} s^{j-l}}]^{t^k s^l} = 1$, uma vez que pelo Lema 3.3.2 $[y, y^{t^{i-k} s^{j-l}}] = 1$, e $[s, t] = 1$. Portanto, K_0' é abeliano.

■

Teorema 3.3.4. *O grupo*

$$K_0 = \langle t, s, y \mid [t, s] = 1, y^s = yy^t, [y, y^t] = 1 \rangle$$

é metabeliano.

Demonstração: K_0' e K_0/K_0' são abelianos, logo K_0 é metabeliano.

■

Corolário 3.3.5. *O grupo*

$$K_0 = \langle t, s, y \mid [t, s] = 1, y^s = yy^t, [y, y^t] = 1 \rangle$$

tem max−n.

Demonstração: K_0 é um grupo abeliano finitamente gerado, logo pelo Corolário 3.2.12, K_0 tem a propriedade maximal sobre subgrupos normais.

■

Para o caso com mais de 3 geradores, usando o mesmo procedimento, obtemos que o grupo derivado é abeliano, deste modo temos o

Teorema 3.3.6. *O grupo com apresentação dada por*

$$K = \langle t, s, y_1, \ldots, y_m \mid [t, s] = 1, y_i^s = y_i y_i^t, [y_i, y_j] = [y_i, y_j^t] = 1, 1 \leq i, j \leq m \rangle.$$

é metabeliano.

■

3.4 Grupos metabelianos com os mesmos quocientes finitos

Nesta seção, construíremos com base no artigo [1], uma quantidade infinita de grupos metabelianos finitamente apresentados não-isomorfos, mas com os mesmos quocientes finitos. Para tal escolheremos um anel R convenientemente, para este teremos que o grupo de Picard é infinito, de modo que podemos obter uma quantidade infinita de módulos projetivos M de posto 1 sobre R. Daremos uma condição necessária e suficiente para que dois módulos finitamente gerados M e N tenham quocientes finitos isomorfos como R-módulos, $\mathrm{QFI_R}$. Em particular, quando M e N são projetivos de posto 1, veremos que M e N têm os mesmos quocientes finitos. A partir desses construíremos uma quantidade infinita de grupos $G_M = M \rtimes A$, que são não-isomorfos, mas têm os mesmos quocientes finitos.

Lema 3.4.1. *Se R é um anel noetheriano comutativo com 1, e M é um R-módulo finito, então existem inteiros positivos k_i e ideais maximais $\mathfrak{p}_i$ de índice finito em R, tal que o anulador de M, $Ann(M)$, contém o produto de ideais $\prod_{i=1}^{n} \mathfrak{p}_i{}^{k_i}$.*

Demonstração: Pela definição de módulos, segue que existe um homomorfismo de anéis

$$\varphi : R \longrightarrow End(M),$$

note que $Ker\varphi = \{r \in R \ ; \ \varphi(r) = 0_{End(M)}\}$= $\{ r \in R \ ; \ \varphi(r)(m) = 0, \ \forall m \in M\} = \{ r \in R \ ; \ r.m = 0, \ \forall m \in M\}$=$Ann(M)$. Pelo 1º Teorema de homomorfismos, temos que $R/Ann(M) \cong Im\varphi \leq End(M)$, mas como M é finito, segue que o anel $End(M)$ é finito, daí $Ann(M)$ é um ideal de índice finito em R. Agora, como R é noetheriano, cada ideal de R possui uma decomposição primária, a qual podemos supor minimal, deste modo, podemos decompor $Ann(M) = \bigcap_{i=1}^{n} \mathfrak{a}_i$, em que cada $\mathfrak{a}_i$ é um ideal primário pertencente a um único ideal primo $\mathfrak{p}_i$, i.e. $r(\mathfrak{a}_i) = \mathfrak{p}_i$. Como $\mathfrak{p}_i$ é um ideal primo, temos que $R/\mathfrak{p}_i$ é um domínio de integridade, além disso, de $\mathfrak{p}_i$= $r(\mathfrak{a}_i) \supseteq \mathfrak{a}_i \supseteq Ann(M)$, segue que $[R : \mathfrak{p}_i] \leq [R : Ann(M)] < \infty$, portanto $R/\mathfrak{p}_i$ é um domínio de integridade finito, daí $R/\mathfrak{p}_i$ é um corpo (finito), consequentemente $\mathfrak{p}_i$ é um ideal maximal de índice finito em R. Por outro lado, como R é um anel noetheriano, segue que cada ideal contém uma potência de seu radical, logo para cada $\mathfrak{a}_i$ existe $k_i \in \mathbb{N}$ tal que $\mathfrak{a}_i \supseteq r(\mathfrak{a}_i)^{k_i} = \mathfrak{p}_i{}^{k_i}$, de modo que $Ann(M) = \bigcap_{i=1}^{n} \mathfrak{a}_i \supseteq \bigcap_{i=1}^{n} \mathfrak{p}_i{}^{k_i} \supseteq \prod_{i=1}^{n} \mathfrak{p}_i{}^{k_i}$.

■

Denotaremos por $\mathrm{F_R(M)}$, o conjunto das classes de R-isomorfismos dos módulos quocientes finitos de M. Diremos que dois R-módulos M e N têm quocientes finitos isomorfos como R-módulos ($\mathrm{QFI_R}$) quando $\mathrm{F_R(M)} = \mathrm{F_R(N)}$.

Teorema 3.4.2. *Sejam R um anel noetheriano comutativo com 1, M e N, R-módulos finitamente gerados . Então M e N têm QFI_R se, e somente se, $M/\mathfrak{p}^k M$ é isomorfo a $N/\mathfrak{p}^k N$ para todo $k \in \mathbb{N}$ e para todos ideais maximais $\mathfrak{p}$ de índice finito em R.*

Demonstração:
($\Leftarrow$) Seja M um R-módulo finitamente gerado, considere que M/M' seja um quociente finito de M, daí pelo Lema 3.4.1, temos que existem inteiros positivos k_i e ideais maximais $\mathfrak{p}_i$ de índice finito em R, tais que $Ann(M/M') \supseteq \prod_{i=1}^{n} \mathfrak{p}_i{}^{k_i}$. Por hipótese, $M/\mathfrak{p}^k M \cong N/\mathfrak{p}^k N$

para todo $k \in \mathbb{N}$ e para todos ideais maximais $\mathfrak{p}$ de índice finito em R, logo $M/{\mathfrak{p}_i}^{k_i}M \cong N/{\mathfrak{p}_i}^{k_i}N, \forall i$, daí $\bigoplus_{i=1}^{n} M/{\mathfrak{p}_i}^{k_i}M \cong \bigoplus_{i=1}^{n} N/{\mathfrak{p}_i}^{k_i}N$, mas como os ideais $\mathfrak{p}_i$'s são maximais, segue que para $i \neq j$, $\mathfrak{p}_i + \mathfrak{p}_j$ contém o ideal maximal $\mathfrak{p}_i$ propriamente, logo $\mathfrak{p}_i + \mathfrak{p}_j = R$, i.e, $\mathfrak{p}_i$ e $\mathfrak{p}_j$ são comaximais se $i \neq j$, daí também são os ideais ${\mathfrak{p}_i}^{k_i}$'s, logo pelo Teorema Chinês dos Restos para Módulos 2.0.43, temos que

$$M/(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})M \cong N/(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})N.$$

Agora note que $(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})M \subseteq M'$, com efeito, se $x \in (\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})M$, então podemos escrever x como $\sum_{i=1}^{t} r_i m_i$ para algum natural t, com $r_i \in \prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i}$ e $m_i \in M$, no entanto, temos que $\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i} \subseteq Ann(M/M')$, deste modo, $r_i \in Ann(M/M')$, logo $r_i(M/M') = 0$, ou seja, $r_i m \in M', \forall m \in M$, portanto $r_i m_i \in M', \forall i$, consequentemente $\sum_{i=1}^{t} r_i m_i \in M'$. Em suma, temos que $(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})M \subseteq M' \subseteq M$, logo pelo 3º Teorema de homomorfismos, segue que

$$M/M' \cong \frac{\left(\dfrac{M}{(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})M}\right)}{\left(\dfrac{M'}{(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})M}\right)},$$

isto é, M/M' é um quociente de $M/(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})M$, mas como $M/(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})M \cong N/(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})N$, segue que M/M' é isomorfo a um quociente de $N/(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})N$, digamos

$$M/M' \cong \frac{\left(\dfrac{N}{(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})N}\right)}{\left(\dfrac{N'}{(\prod_{i=1}^{n} {\mathfrak{p}_i}^{k_i})N}\right)} \cong N/N',$$

logo $M/M' \cong N/N'$, portanto M e N têm QFI_R.
($\Rightarrow$) Sejam $k \in \mathbb{N}$ e $\mathfrak{p}$ um ideal maximal de índice finito em R, mostremos que $M/\mathfrak{p}^k M$ é o maior quociente finito de M anulado por $\mathfrak{p}^k$. De fato,

$$Ann(M/\mathfrak{p}^k M) = \{r \in R \ ; \ r(m + \mathfrak{p}^k M) = 0, \forall m \in M\} = \{r \in R \ ; \ rm \in \mathfrak{p}^k M, \forall m \in M\},$$

daí $\mathfrak{p}^k \subseteq Ann(M/\mathfrak{p}^k M)$. Agora, suponha que M/M' seja um quociente finito de M anulado por $\mathfrak{p}^k$, daí $\mathfrak{p}^k(m + M') = 0, \forall m \in M$, logo $\mathfrak{p}^k m \subseteq M', \forall m \in M$, portanto $\mathfrak{p}^k M \subseteq M'$, deste modo, $[M : \mathfrak{p}^k M] \geq [M : M']$, logo $M/\mathfrak{p}^k M$ é um quociente de M maior que M/M'. Analogamente, temos que $N/\mathfrak{p}^k N$ é o maior quociente finito de N anulado por $\mathfrak{p}^k$, mas como, por hipótese, M e N têm QFI_R, segue que $M/\mathfrak{p}^k M$ e $N/\mathfrak{p}^k N$ são isomorfos.

■

Indicaremos por $F(G)$, a classe de isomorfismos de quocientes finitos do grupo G, e diremos que dois grupos G e H têm os mesmos quocientes finitos quando $F(G) = F(H)$. Vamos construir grupos não-isomorfos que têm quocientes finitos isomorfos. Posteriormente, mostraremos que existe uma quantidade infinita desses grupos, os quais determinam uma quantidade infinita de classes de isomorfismos distintas.

Agora, considere que A seja um subgrupo das unidades $\mathcal{U}(R)$ de R que gera R como um anel, assim se M é um R-módulo finitamente gerado, podemos formar o produto semidireto de M por A, $G_M = M \rtimes A$ com ação de A em M induzida pela ação de módulo de R sobre M, isto é, temos um homomorfismo:

$$\begin{array}{rccl} \theta & : & A & \longrightarrow & \mathrm{Aut(M)} \\ & & a & \longmapsto & \theta(a) : m \mapsto m^{a^{-1}} \end{array}$$

Note que $\theta(a)$ é de fato um automorfismo de M, uma vez que os elementos de A são unidades em R. Observe também que a ação m^a de módulo de a sobre m coincide com a conjugação usual. Por fim, veja que G_M é metabeliano, pois M e $A \cong G/M$ são abelianos.

Lema 3.4.3. *Sejam A um subgrupo do grupo das unidades $\mathcal{U}(R)$ de R que gera R como um anel, considere que M e N sejam R-módulos finitamente gerados com QFI_R. Então, os grupos $G_M = M \rtimes A$ e $G_N = N \rtimes A$ têm os mesmos quocientes finitos.*

Demonstração: Suponha que M' seja um subgrupo normal de $G_M = M \rtimes A$ de índice finito, daí $(M \rtimes A)/M'$ é um quociente finito de $M \rtimes A$. Defina $M'' := M \cap M'$, mostremos que M'' é um R-submódulo de M de índice finito. Com efeito, se $x, y \in M''$, então $x, y \in M$ e $x, y \in M'$, como M e M' são grupos (abelianos), segue que $x - y \in M$ e $x - y \in M'$, logo $x - y \in M''$, portanto M'' é um subgrupo de M. Agora, verifiquemos que M'' é fechado sob multiplicação por elementos de R, de fato, se $r \in R$ e $m \in M''$, então como $M'' \subseteq M$, e M é um R-módulo, temos que $rm \in M$, por outro lado, como A gera R como anel, segue que cada elemento de R pode ser escrito como uma soma finita de produtos com elementos de A, no entanto, A age em M pela ação do módulo, que coincide com a ação por conjugação, em particular, quando age em $M' \cap M$, segue que o resultado da ação permanece em M', por exemplo, se $a_1 a_2 \dots a_k$ é uma das parcelas que compõe r, então quando esta age em $m \in M''$, segue que $(a_1 a_2 \dots a_k)m = a_1 a_2 \dots m'_k$, em que $a_k m = m'_k \in M'$, pois a_k age em $m \in M'$ por conjugação, uma vez que $M' \trianglelefteq G_M$, agora recursivamente, temos que a_{k-1}

age em m'_k, resultando novamente num elemento m'_{k-1} de M', deste modo, ao fim deste processo, obtemos um elemento de M', aplicando o mesmo procedimento a todas parcelas que compõem r, segue que $rm \in M'$, logo $rm \in M''$. Falta mostrarmos que M/M'' é um quociente finito de M, de fato,

$$[G_M : M'] = [G_M : M + M'][M + M' : M'],$$

(note que $M' + M \leq G_M$, pois $M' \trianglelefteq G_M$), mas como $[G_M : M'] < \infty$, segue que $[M + M' : M'] < \infty$, no entanto, $M/M'' \cong (M + M')/M'$, portanto $[M/M''] < \infty$. Já que M e N têm QFI_R, existe um R-submódulo N'' de N tal que $M/M'' \cong N/N''$ como R-módulos, daí $(M/M'') \rtimes A \cong (N/N'') \rtimes A$ como grupos. Agora, note que $(M/M'') \rtimes A \cong (M \rtimes A)/M''$, uma vez que as ações de A em M/M'' e de A em M (módulo M'') se relacionam por: $r(m+M'') = rm+M''$. Agora, mostremos que $(M \rtimes A)/M'$ é um quociente de $(M/M'') \rtimes A$, de fato, como $M'' \subseteq M' \subseteq M \rtimes A$, segue pelo 3º Teorema de homomorfismos que

$$\frac{M \rtimes A}{M'} \cong \frac{\left(\dfrac{M \rtimes A}{M''}\right)}{\left(\dfrac{M'}{M''}\right)} \cong \frac{\left(\dfrac{M}{M''} \rtimes A\right)}{\left(\dfrac{M'}{M''}\right)}.$$

Em suma,

$$\frac{M \rtimes A}{M'} \cong \frac{\left(\dfrac{M}{M''} \rtimes A\right)}{\left(\dfrac{M'}{M''}\right)},$$

mas como $(M/M'') \rtimes A \cong (N/N'') \rtimes A$, segue que $(M \rtimes A)/M'$ é isomorfo a um quociente de $(N/N'') \rtimes A \cong (N \rtimes A)/N''$, logo existe $X/N'' \trianglelefteq (N \rtimes A)/N''$ tal que

$$\frac{M \rtimes A}{M'} \cong \frac{\left(\dfrac{N \rtimes A}{N''}\right)}{\left(\dfrac{X}{N''}\right)} \cong \frac{N \rtimes A}{X},$$

portanto $(M \rtimes A)/M'$ é isomorfo a um quociente finito de $N \rtimes A$, analogamente, podemos tomar um quociente finito de $N \rtimes A$ e mostrarmos que este é isomorfo a um quociente finito de $M \rtimes A$. Portanto, $M \rtimes A$ e $N \rtimes A$ têm os mesmos quocientes finitos.

■

Proposição 3.4.4. *Todos R-módulos projetivos de posto 1 têm QFI_R. Além disso, tais R-módulos são fiéis.*

Demonstração: Sejam M e N módulos projetivos de posto 1 sobre R, logo $M_{\mathfrak{m}} \cong R_{\mathfrak{m}} \cong N_{\mathfrak{m}}$ para cada ideal maximal $\mathfrak{m}$ de R. Agora, pela Proposição 2.5.14, temos que

$$\frac{M}{\mathfrak{m}^k M} \cong \frac{M_{\mathfrak{m}}}{\mathfrak{m}^k M_{\mathfrak{m}}},$$

para cada $k \in \mathbb{N}$. Logo,

$$\frac{M}{\mathfrak{m}^k M} \cong \frac{M_{\mathfrak{m}}}{\mathfrak{m}^k M_{\mathfrak{m}}} \cong \frac{R_{\mathfrak{m}}}{\mathfrak{m}^k R_{\mathfrak{m}}} \cong \frac{R}{\mathfrak{m}^k R}.$$

Analogamente,

$$\frac{N}{\mathfrak{m}^k N} \cong \frac{R}{\mathfrak{m}^k R}.$$

Portanto, $M/\mathfrak{m}^k M \cong N/\mathfrak{m}^k N$ para todo ideal maximal $\mathfrak{m}$ de R (em particular, para os ideais maximais $\mathfrak{m}$ de índice finito em R), e para todo $k \in \mathbb{N}$, logo pelo Teorema 3.4.2, segue que M e N têm QFI_R. Mostremos agora que M é fiel, isto é, $Ann(M) = 0$. Com efeito, seja $r \in R$ tal que $rM = 0$, daí para todo $s \in R - \mathfrak{m} = S$, e para todo $m \in M$, temos que $rm/s = 0/s$, logo $(r/1)M_{\mathfrak{m}} = 0/s$ para todo $s \in S$, mas como $M_{\mathfrak{m}} \cong R_{\mathfrak{m}}$, segue que $(r/1)R_{\mathfrak{m}}$ é nulo em $R_{\mathfrak{m}}$, em particular, $(r/1).(1/1) = 0/1$, equivalentemente, $r/1 = 0/1$, mas como 0 é uma propriedade local(vide Afirmação), segue que $r = 0$, portanto $Ann(M) = 0$.

Afirmação Considere que R seja um anel comutativo com 1. Então, x é nulo em R se, e somente se, $x/1$ é nulo em $R_{\mathfrak{m}}$, para cada ideal maximal $\mathfrak{m}$ de R.

Demonstração: Se $x = 0$ em R, então $x/1 = 0/1$, que é nulo em $R_{\mathfrak{m}}$. Reciprocamente, considere que $x/1$ seja nulo em $R_{\mathfrak{m}}$, para cada ideal maximal $\mathfrak{m}$ de R. Suponha, por absurdo, que $x \neq 0$ em R. Defina I como sendo o ideal anulador de x, ou seja, $I = (0 : x) = \{r \in R \mid rx = 0\}$, como $1.x = x \neq 0$, segue que $1 \notin I$, logo I é um ideal próprio de R, portanto existe um ideal maximal $\mathfrak{m}$ que contém I. Mas pela hipótese, temos que $x/1$ é nulo em $R_{\mathfrak{m}}$, logo existe $u \in R - \mathfrak{m}$, tal que $ux = 0$, mas então $u \in I$, o que implica que $u \in \mathfrak{m}$, que é uma contradição. Portanto, $x = 0$ em R.

■

Doravante, consideremos que R seja o anel $\mathbb{Z}G[x, x^{-1}, (x+1)^{-1}]$, em que G é um grupo abeliano finito, cuja ordem não é livre de quadrados; A o subgrupo das unidades de R gerado por G, x e $x+1$. Temos que, se M é um R-módulo projetivo, então o grupo $G_M = M \rtimes A$ pode ser formado, em que a ação de A em M é induzida pela ação de módulo de R sobre M como descrita anteriormente.

Teorema 3.4.5. *Se M e N são R-módulos projetivos de posto 1, então os grupos $G_M = M \rtimes A$ e $G_N = N \rtimes A$ têm os mesmos quocientes finitos, i.e, $F(G_M) = F(G_N)$.*

Demonstração: Como A é um subgrupo das unidades de R que o gera como anel; e M e N são R-módulos projetivos e finitamente gerados (haja vista que M e N têm posto 1), e pela Proposição 3.4.4, M e N têm QFI_R. Pelo Lema 3.4.3, segue que $G_M = M \rtimes A$ e $G_N = N \rtimes A$ têm os mesmos quocientes finitos.

■

Proposição 3.4.6. *Considerando A e G_M como descritos acima. O grupo derivado ${G_M}'$ de $G_M = M \rtimes_\theta A$, coincide com M.*

Demonstração: Por conveniência, adotaremos notação multiplicativa para o R-módulo M. Temos que $G_M/M \cong A$ é abeliano, logo ${G_M}' \subseteq M$, por outro lado, como $M = M^x$, pois $\theta(x^{-1})$ é automorfismo de M, segue que cada elemento de M pode ser escrito por $m^x = m^{-1+(x+1)} = m^{-1}m^{x+1} = [m, x+1]$, daí $M \subseteq {G_M}'$. Portanto, ${G_M}' = M$. Note que a ação de $x+1$ em m, induzida pela ação de módulo, coincide com a conjugação usual, de modo que -1 age invertendo m em G_M, além disso observe que $m^{x+1} = m.m^x$, pois estamos usando notação multiplicativa para o módulo M.

■

Proposição 3.4.7. *O grupo $Pic(\mathbb{Z}G[x, x^{-1}, (x+1)^{-1}])$ é infinito.*

Demonstração: Bass e Murthy, em [6], mostram que quando o grupo abeliano G é finito de ordem não livre de quadrados, então o grupo $Pic(\mathbb{Z}G[x])$ é infinito, no entanto, Murthy e Pedrini, em [10], mostram que existe uma aplicação injetiva de $Pic(\mathbb{Z}G[x])$ em $Pic(\mathbb{Z}G[x, x^{-1}, (x+1)^{-1}])$, daí como o primeiro grupo é infinito, segue que o segundo também o é.

■

Mostremos que os grupos metabelianos $G_M = M \rtimes A$ determinam uma quantidade infinita de classes de isomorfismos distintas. Novamente usaremos notação multiplicativa para os módulos.

Proposição 3.4.8. *Os grupos G_M determinam uma quantidade infinita de classes de isomorfismos distintas.*

Demonstração: Seja ψ um automorfismo de R, e N um R-módulo, deste modo podemos formar o módulo torcido ψ_N, ou seja, a multiplicação escalar em ψ_N é dada por $r \star n = \psi(r)n$ para cada $r \in R$ e para cada $n \in N$. Note que dois R-módulos M e N são isomorfos se, e somente se, os módulos torcidos ψ_M e ψ_N são isomorfos. Seja $\varphi : G_M \longrightarrow G_N$ um isomorfismo, temos pela Proposição 3.4.6, que ${G_M}' = M$, e ${G_N}' = N$, daí $\varphi(M) = N$, agora já que $G_M/M \cong A \cong G_N/N$, segue que existe um automorfismo $\overline{\varphi}$ em A (subgrupo das unidades de R que o gera como anel) induzido pelas abelianizações de G_M e G_N. Agora, note que para cada $n = \varphi(m) \in \varphi(M) = N$, temos que

$$\varphi(m)^{\varphi(x+1)} = \varphi(x+1)^{-1}\varphi(m)\varphi(x+1) = \varphi(m^{x+1}) = \varphi(m^x m) = \varphi(m)^{\varphi(x)}\varphi(m) = \varphi(m)^{\varphi(x)+1}$$

Mas como N é um R-módulo fiel, e $\varphi(x+1)$ e $\varphi(x)+1$ agem sobre N da mesma forma, segue que $\varphi(x+1) = \varphi(x) + 1$, daí $\overline{\varphi}(x+1) = \overline{\varphi}(x) + 1$. No entanto, temos que o gerador x de $A = \langle x, x+1, G\rangle$ é levado em x ou x^{-1} por $\overline{\varphi}$, note que x não pode ser levado em $x+1$, pois já que $\overline{\varphi}(x+1) = \overline{\varphi}(x)+1$, teríamos $\overline{\varphi}(x+1) = x+2.1$, que não é uma unidade. Agora note que os elementos de ordem finita de A, que são os elementos do grupo finito G, são invariantes em G, assim existe uma quantidade finita de automorfismos $\overline{\varphi}$. Mas como $\overline{\varphi}(x+1) = \overline{\varphi}(x) + 1$ e A gera R como anel, podemos estender $\overline{\varphi}$ a um automorfismo de R. Restringindo φ a M, temos um isomorfismo de grupos entre M e N, obtendo-se um R-isomorfismo entre M e um módulo torcido $\overline{\varphi}_N$ de N. Em suma, sempre que $G_M \cong G_N$, temos que M é isomorfo a algum módulo torcido $\overline{\varphi}_N$ de N, em que $\overline{\varphi} \in \mathrm{Aut(R)}$ é algum dos finitos automorfismos induzidos. Agora mostremos que existem infinitas classes de isomorfismos determinadas pelos grupos G_M. Fixe um módulo projetivo de posto 1, M_1. Como pela Proposição 3.4.7, o grupo de Picard de $R = \mathbb{Z}G[x, x^{-1}, (x+1)^{-1}]$ é infinito, podemos escolher um módulo projetivo M_2 de posto 1 que não seja isomorfo a nenhum dos módulos torcidos de M_1. Daí G_{M_2} e G_{M_1} não são isomorfos. Usando este mesmo procedimento, podemos escolher um módulo projetivo M_3 de posto 1 que não seja isomorfo a nenhum dos módulos torcidos de M_1 e de M_2, Logo G_{M_3} não é isomorfo nem a G_{M_1} nem a G_{M_2}, obtendo-se outra classe de isomorfismo não-isomorfa às anteriores. Procedendo deste modo, concluímos que existe uma quantidade infinita de classes de isomorfismos distintas nas quais jazem os grupos G_M.

■

Lema 3.4.9 (Bass). *Seja $S = \mathbb{Z}[x, x^{-1}, (x+1)^{-1}]$, que é um subanel de $R = \mathbb{Z}G[x, x^{-1}, (x+1)^{-1}]$. Então todos S-módulos projetivos são livres.*

Demonstração: [5], p.210.

■

Proposição 3.4.10. *Se M é um módulo projetivo de posto 1 sobre $R = \mathbb{Z}G[x, x^{-1}, (x+1)^{-1}]$, então M é isomorfo a R, como módulo sobre $S = \mathbb{Z}[x, x^{-1}, (x+1)^{-1}]$.*

Demonstração: Como G é finito, podemos supor que $G = \{x_1, \ldots, x_n\}$. Seja M um R-módulo projetivo, assim M é um somando direto de um R-módulo livre, mas R é livre com base G quando considerado como um $S-$módulo, daí $R \cong S^n \Rightarrow R_{\mathfrak{p}} \cong S^n_{\mathfrak{p}}$, logo M considerado como um S-módulo é um somando direto de um S-módulo livre, portanto M é um S-módulo projetivo, mas pelo Lema 3.4.9, todos S-módulos projetivos são livres, logo $M \cong S^{k(M)} \Rightarrow M_{\mathfrak{p}} \cong S^{k(M)}_{\mathfrak{p}}$, no entanto como M é um $R-$módulo projetivo de posto 1, segue que $M_{\mathfrak{p}} \cong R_{\mathfrak{p}}$, logo $S^{k(M)}_{\mathfrak{p}} \cong S^n_{\mathfrak{p}}$, daí $k(M) = n$, portanto $R \cong S^n \cong S^{k(M)} \cong M$, segue que o R-módulo M é isomorfo a R como S-módulo.

■

Observação 3.4.11. *Considere que C seja o subgrupo das unidades de S gerado por x e $x+1$, podemos assim formar o grupo $H_M = M \rtimes C$. Pela Proposição anterior, temos que M é isomorfo a R como S-módulo, daí H_M é isomorfo a $B := R \rtimes C$. Deste modo, para cada módulo M, temos que $G_M = M \rtimes A = H_M \rtimes G \cong B \rtimes G$, em que há uma ação de G sobre B escolhida convenientemente via o isomorfismo entre B e H_M.*

Proposição 3.4.12. *Existe uma quantidade infinita de extensões de decomposição metabelianas não-isomorfas do grupo metabeliano $B = R \rtimes C$ pelo grupo abeliano finito G com os mesmos quocientes finitos.*

Demonstração: Pela Observação 3.4.11, temos que $G_M \cong B \rtimes G$, daí G_M é uma extensão do grupo(metabeliano) B pelo grupo G, mas pela Proposição 3.4.8, mostramos que existe uma quantidade infinita de grupos (metabelianos) G_M não-isomorfos com os mesmos quocientes finitos, daí segue o resultado.

■

Proposição 3.4.13. *Os grupos G_M são finitamente apresentados.*

Demonstração: Temos que G é finito, suponha que seus elementos sejam $x_1, \ldots, x_n$, deste modo, já que $R = \mathbb{Z}G[x, x^{-1}, (x+1)^{-1}]$ e $S = \mathbb{Z}[x, x^{-1}, (x+1)^{-1}]$, segue que $x_1, \ldots, x_n$ é uma base de R sobre S. Defina o grupo K pela apresentação

$$\langle t, s, y_1, \ldots, y_n : \ [t,s] = 1, y_i^s = y_i y_i^t, [y_i, y_j] = [y_i, y_j^t] = 1, 1 \leq i, j \leq n \rangle,$$

K é deste modo finitamente apresentado, além disso, K é metabeliano, pelo Teorema 3.3.6. Consideremos a aplicação $t \mapsto x, s \mapsto (x+1), y_i \mapsto x_i$, a qual pelo Teorema de von Dyck 1.2.13, induz um epimorfismo de K sobre $B = R \rtimes C$, no entanto, como K é metabeliano, e grupos metabelianos satisfazem a condição maximal sobre subgrupos normais, temos pelo Corolário 3.2.13 que B deve ser finitamente apresentado, mas como cada G_M é uma extensão finita de B, segue que cada grupo G_M é finitamente apresentado.

■

Podemos agora demonstrar o resultado principal:

Teorema 3.4.14. *Existe uma quantidade infinita de grupos metabelianos finitamente apresentados não-isomorfos com os mesmos quocientes finitos.*

Demonstração: Pela Proposição 3.4.8, temos que existe uma quantidade infinita de grupos metabelianos não-isomorfos G_M, os quais pela Proposição 3.4.13 são finitamente apresentados, e por fim pelo Teorema 3.4.5 têm os mesmos quocientes finitos.

■

REFERÊNCIAS BIBLIOGRÁFICAS

[1] PICKEL, Paul F. *Metabelian groups with the same finite quotients*, Bull. Austral. Math. Soc., **11**, 1974, 115-120.

[2] BAUMSLAG, Gilbert *A finitely presented metabelian group with a free abelian derived group of infinite rank*, Proc. Amer. Math. Soc. **35**, 1972, 61-62.

[3] HALL, P. *Finiteness conditions for soluble groups*, Proc. London Math. Soc. (3) **4**, 1954, 419-436.

[4] ATIYAH, M. F.; MACDONALD, I. G. *Introduction to Commutative Algebra*, Addison-Wesley, London,1969.

[5] BASS, Hyman. *Algebraic K-theory*, Benjamin, New York, Amsterdam, 1968.

[6] BASS, Hyman; MURTHY, M. Pavaman. , *Grothendieck groups and Picard groups of abelian group rings*, Ann. of Math.(2) **86**, 1967, 16-73.

[7] BOURBAKI, N. *Elements of Mathematics, Commutative Algebra*, Addison-Wesley, 1972.

[8] BRIGHMAM, Robert C. *On the isomorphism problem for just-infinite groups*, Comm. Pure Appl. Math. **24**(1971),789-796;

[9] DYER, Joan Landman. *On the isomorphism problem for polycyclic groups*, Math. Z. **112** (1969), 145-153;

[10] MURTHY, M. Pavaman; PEDRINI, Claudio. K_0 *e* K_1 *of polynomial rings*, Algebraic K-theory II, 109-121.

[11] PICKEL, Paul F. *On the isomorphism problem for finitely generated torsion free nilpotent groups*, (PhD thesis, Rice University, Houston, Texas, 1970);

[12] REMESLENNIKOV, V.N. *Groups that are residually finite with respect to conjugacy*, Siberian Math. J. **12** (1971), 783-792.

[13] ROBINSON, Derek J. S. *A course in the theory of groups*, 2nd ed., Springer-Verlag, New York Inc, 1996.

[14] ROTMAN, J. J. *An introduction to homological algebra*, 1979;

[15] ROTMAN, J.J. *An introduction to the theory of groups*, 4th ed., Springer-Verlag, New York Inc., 1995.

[16] WEIBEL, Charles. *The K-book: An introduction to algebraic K-theory* , disponível na página pessoal do autor: http://www.math.rutgers.edu/ weibel/Kbook.html

[17] ZARISKI, Oscar; SAMUEL, Pierre. *Commutative algebra, Volume I*, Van Nostrand, Princeton, New jersey; Toronto; New York; London; 1958.