Teoria de corpos de classe e aplicações

Luan Alberto Ferreira

Teoria de corpos de classe e aplicações*

Luan Alberto Ferreira

Orientador: **Prof. Dr. Oziride Manzoli Neto**

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências - Matemática . *VERSÃO REVISADA*

USP – São Carlos
Setembro de 2012

*O autor teve suporte financeiro da FAPESP.

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados fornecidos pelo(a) autor(a)

F383t

Ferreira, Luan Alberto
Teoria de corpos de classe e aplicações / Luan Alberto Ferreira; orientador Oziride Manzoli Neto. -- São Carlos, 2012.
96 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2012.

1. Corpos ciclotômicos. 2. Teoria algébrica dos números. 3. Teoria de corpos de classe. 4. Problema inverso de Galois. 5. Extensões abelianas. I. Manzoli Neto, Oziride, orient. II. Título.

A todos que acreditaram em mim,
quando eu mesmo não acreditei em mim.

Agradecimentos

É sempre difícil escrever uma seção de agradecimentos. Peço desculpas aqueles que julguei mal, seja por excesso, seja por falta - não quero cometer injustiças.

Agradeço inicialmente à FAPESP pelo apoio financeiro e ao professor Eduardo Tengan, que foi quem propôs este belo tema de estudo.

Agradeço aos meus amigos e colegas do ICMC, em especial à Camila Mariana Ruiz, Danilo Franchini de Souza, Felipe Alves da Louza, Fernando de Mello Trevisani, Henrique Barbosa da Costa, João Paulo Poli, José Augusto Fioruci, Júlia Silva Silveira Borges, Juliana Rodrigues Dionísio Pereira, Leandro Mattiolli, Lucas Esperancini Moreira e Moreira, Marcelo Silveira Querino, Markus Diego Sampaio da Silva Dias, Matheus Dorival Leonardo Bombonato Menes, Raquel Filippi de Souza e Rodolfo Collegari. Obrigado pelas horas de estudo em grupo, pelas risadas, pelas conversas, pelos conselhos e por sempre acreditarem em mim.

Agradeço a todos os professores que, de uma forma ou de outra, contribuíram em minha formação, seja profissional ou pessoal. Cabe aqui um agradecimento ao Instituto Embraer de Educação e Pesquisa, a sua iniciativa social e ao seu excelente corpo docente. Devo muito de minha formação a eles. Quanto aos professores do ICMC, gostaria de agradecer em especial a Carlos Biasi, Eduardo Alex Hernández Morales, Janete Crema, Sérgio Henrique Monari Soares, Valdir Antonio Menegatto e Wagner Vieira Leite Nunes por todos terem contribuído de forma significativa na minha formação.

Agradeço aos funcionários do ICMC, que sempre me trataram com muita cordialidade e respeito.

Agradeço à minha família que me apoiou. Em especial, agradeço muitíssimo às quatro mulheres que, sem as quais, eu não seria nada do que sou hoje: às minhas mamães Maria Isabel Ferreira Claudio e Valda Maria Ferreira e às minhas irmãs Bianca Ferreira de Jesus e Thaís Fernanda Ferreira Claudio. Muito obrigado por vocês sempre acreditarem em mim, no meu potecial e no meu futuro!

Agradeço especialmente a três professores do ICMC: ao professor Luiz Augusto da Costa Ladeira, não sei como posso expressar o reconhecimento e o respeito que tenho pelo senhor, professor, por todos os conselhos que me deu e por sempre acreditar no meu potencial! Ao meu orientador e professor Oziride Manzoli Neto, sou eternamente grato pelo voto de confiança que recebi e por ter me acolhido de braços abertos! Agradeço pelas conversas que tivemos, pelos momentos de descontração e trabalho árduo juntos, por compartilhar comigo seus problemas com o

grupo $P72$ e por me ouvir falando sobre o que os números primos têm a ver com os espaços métricos! Sou muito grato e fico muito feliz de ter conhecido e poder ter trabalhado com o senhor, professor! Quanto à professora Ires Dias, bem, não tenho palavras para descrever tudo o que ela fez por mim durante meus anos em São Carlos. Possivelmente tudo seria diferente se eu não a tivesse conhecido, professora. Só saiba que a senhora foi como uma mãe para mim aqui em São Carlos.

Agradeço especialmente também aos meus amigos do Vale do Paraíba: Braulio Augusto Freire, Denise Clarice Caputo de Souza, Fanny Sene Fidelis de Oliveira, Fernando Luiz Bustamante Bueno Oliveira, Gabriel *O.* Godoy, Luana Menezes Nunes, Lucas Renan Coelho Teixeira, Luis Fernando da Costa Oliveira, Luiz Rafael dos Santos Leite, Miriam Silva Freitas Dias, Nilson Henrique Chagas Oliveira, Orlando Pasqual Filho (sim, Landinho, você é do Vale também!), Paula Salles Gória, Priscila Aparecida Gonçalves e Thiago Augusto dos Santos Silva. Não sei o que seria de mim sem vocês, pessoal. Se fosse listar tudo o que vocês já fizeram por mim gastaria mais tempo nisso do que escrevendo esta dissertação! Vocês são como irmãos e irmãs para mim. Muito obrigado por tudo!

Finalmente, agradeço de todo o coração à Diana Renata Gonçalves Gama, por todo o apoio, carinho, compreensão, amor, cuidado e atenção que recebi e recebo! Nao sei onde estaria agora se não fosse por você! Muito obrigado por compartilhar sua vida comigo, pelo apoio incondicional e por todos os momentos que vivemos juntos!

Resumo

Neste projeto, propomos estudar a chamada "Teoria de Corpos de Classe," que oferece uma descrição simples das extensões abelianas de corpos locais e globais, bem como algumas de suas aplicações, como os teoremas de Kronecker-Weber e Scholz-Reichardt.

Abstract

In this work, we study the so called "Class Field Theory", which give us a simple description of the abelian extension of local and global fields. We also study some applications, like the Kronecker-Weber and Scholz-Reichardt theorems.

Sumário

1 Corpos de números **15**

1.1 Anéis noetherianos 15

1.2 Elementos integrais 17

1.3 Domínios integralmente fechados 20

1.4 Domínios de Dedekind 22

1.5 O anel de números de um corpo de números 27

1.6 Norma, traço e discriminante 30

1.7 Bases integrais 36

1.8 O anel de números de $\mathbb{Q}(\zeta_m)$ 39

1.9 Apêndice 42

2 O teorema de Scholz-Reichardt **45**

2.1 O problema inverso de Galois 45

2.2 O problema inverso de Galois para grupos abelianos 45

2.3 Ramificação 47

2.4 Homologia e cohomologia de grupos 50

2.5 O problema de extensão de grupos 55

2.6 O teorema de Scholz-Reichardt 56

2.6.1 O caso $\widetilde{G} \simeq G \times \dfrac{\mathbb{Z}}{l\mathbb{Z}}$ 57

2.6.2 O caso $\widetilde{G} \not\simeq G \times \dfrac{\mathbb{Z}}{l\mathbb{Z}}$ 58

3 Lei de reciprocidade local de Artin **61**

3.1 Algumas propriedades do anel $A[[X]]$ 61

3.2 Leis de grupo formais 63

3.3 Leis de grupo de Lubin-Tate 66

3.4 A lei de reciprocidade local 70

3.5 Os teoremas de Kronecker-Weber 74

4 Lei de reciprocidade global de Artin **77**

4.1 Cohomologia de grupos cíclicos 77

4.2 O quociente de Herbrand de um módulo de permutação 80

4.3 Módulus e grupo ideal de um corpo de números 81

4.4 S-unidades 83

4.5 O quociente de Herbrand $q(\mathbf{U}_L)$ 85

4.6 A norma de um módulus 87

4.7 A lei de reciprocidade global 88

Introdução

O objetivo desta dissertação é estudar os fundamentos da teoria algébrica dos números. Como parte deste estudo, objetivamos enunciar e demonstrar os teoremas de Kronecker-Weber, Scholz-Reichardt e a lei de reciprocidade de Artin. Assumimos ainda que o leitor possui um conhecimento em álgebra a nível de graduação, o que inclui um pouco de álgebra linear, teoria de grupos, anéis e corpos, e teoria básica de Galois.

O capítulo 1 apresenta os pré-requisitos básicos da teoria algébrica dos números, como alguns de seus teoremas e exemplos sobre os corpos quadráticos e ciclotômicos.

O capítulo 2 apresenta, além de mais alguns tópicos acerca dos corpos de números, um esboço da demonstração do teorema de Scholz-Reichardt.

O capítulo 3 contém o enunciado e a demonstração da lei de reciprocidade local de Artin, bem como o enunciado e a demonstração do teorema de Kronecker-Weber.

O capítulo 4, último desta dissertação, versa sobre alguns pré-requisitos necessários para provar a lei de reciprocidade global de Artin, bem como seu enunciado e demonstração.

Capítulo 1

Corpos de números

Neste capítulo veremos alguns conceitos básicos da teoria algébrica dos números, alguns dos quais serão utilizados por toda esta dissertação. A última seção deste capítulo (o apêndice) contém alguns pequenos resultados usados neste capítulo inicial. Nesta dissertação, a menos de menção contrária, o termo anel será usado para designar anel comutativo com unidade. Se A for um anel, denotaremos por $A^\times$ o conjunto dos elementos inversíveis de A.

1.1 Anéis noetherianos

Proposição 1.1.1. *Seja A um anel. As seguintes condições são equivalentes:*

1. *Todo ideal de A é finitamente gerado.*
2. *Toda cadeia ascendente de ideais de A estabiliza, i.e., se $\mathfrak{i}_0 \subseteq \mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \cdots$ é uma cadeia ascendente de ideais de A, então existe $n_0 \in \mathbb{N}$ tal que se $n \geq n_0$, então $\mathfrak{i}_n = \mathfrak{i}_{n_0}$.*
3. *Se $S \neq \emptyset$ é um conjunto de ideais de A, então S possui um elemento maximal $\mathfrak{i}_{max}$, isto é, se $\mathfrak{i} \in S$ e $\mathfrak{i}_{max} \subseteq \mathfrak{i}$, então $\mathfrak{i} = \mathfrak{i}_{max}$.*

Demonstração: 1) $\Rightarrow$ 2) Seja $\mathfrak{i}_0 \subseteq \mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \ldots$ uma cadeia ascendente de ideais de A. Então $\mathfrak{i} = \bigcup_{i=0}^{\infty} \mathfrak{i}_i$ é um ideal que, por hipótese, é finitamente gerado. Escreva $\mathfrak{i} = (a_1, \ldots, a_r)$. Então $\exists\, n_0 \in \mathbb{N}$ tal que $\{a_1, \ldots, a_r\} \subseteq \mathfrak{i}_{n_0} \Rightarrow \mathfrak{i} = \mathfrak{i}_{n_0} \Rightarrow \mathfrak{i} = \mathfrak{i}_n,\ \forall\, n \geq n_0$.

2) $\Rightarrow$ 3) Pela contra-recíproca. Seja $S \neq \emptyset$ um conjunto de ideais de A que não possui elemento maximal. Como $S \neq \emptyset$, então existe $\mathfrak{i}_0 \in S$. Como S não possui elemento maximal, existe $\mathfrak{i}_1 \in S$ tal que $\mathfrak{i}_0 \subsetneq \mathfrak{i}_1$. Repetindo este processo indefinidamente, encontramos uma cadeia ascendente de ideais $\mathfrak{i}_0 \subsetneq \mathfrak{i}_1 \subsetneq \mathfrak{i}_2 \subsetneq \ldots$ de A que não estabiliza.

3) $\Rightarrow$ 1) Seja $\mathfrak{i}$ um ideal de A e seja S o conjunto de todos os ideais de A finitamente gerados contidos em $\mathfrak{i}$. Então $S \neq \emptyset$, pois $(0) \in S$. Por hipótese, S possui um elemento maximal $\mathfrak{i}_{max}$. Então $\mathfrak{i}_{max} \in S \Rightarrow \mathfrak{i}_{max} \subseteq \mathfrak{i}$ e $\mathfrak{i}_{max}$ é finitamente gerado, digamos $\mathfrak{i}_{max} = (a_1, \ldots, a_r)$. Se $\mathfrak{i} \neq \mathfrak{i}_{max}$, então existe $a \in \mathfrak{i} - \mathfrak{i}_{max}$. Assim $(a_1, \ldots, a_r, a) \in S$ e $(a_1, \ldots, a_r, a) \supsetneq \mathfrak{i}_{max}$, contradizendo a maximalidade de $\mathfrak{i}_{max}$. Logo $\mathfrak{i} = \mathfrak{i}_{max} = (a_1, \ldots, a_r)$. □

Definição 1.1.2. *Um anel A que cumpre uma e, portanto, todas as condições equivalentes acima é chamado anel noetheriano.*

Exemplo 1.1.3. *Todo domínio de ideais principais (DIP) é noetheriano, enquanto que $\mathbb{Z}[x_1, x_2, \ldots]$ não o é, pois a cadeia ascendente de ideais $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \ldots$ não estabiliza.*

Uma propriedade muito conhecida dos anéis noetherianos é dada pelo

Teorema 1.1.4 (Teorema da base de Hilbert)**.** *Se A é um anel noetheriano, assim o é $A[x]$.*

Demonstração: Vamos mostrar que todo ideal $\mathfrak{i}$ de $A[x]$ é finitamente gerado. Para isto, seja $\mathfrak{i}$ ideal de $A[x]$. Seja $\mathfrak{j}$ o conjunto de todos os coeficientes líderes dos elementos de $\mathfrak{i}$. Então $\mathfrak{j}$ é um ideal A. Como A é noetheriano, $\mathfrak{j}$ é finitamente gerado, isto é, $\mathfrak{j} = (a_1, \ldots a_n)$. Para cada $i \in \{1, \ldots, n\}$, seja $f_i \in \mathfrak{i}$ um polinômio com coeficiente líder a_i. Sejam $d_i = \partial(f_i)$ e $D = \max\limits_{i \in \{1,\ldots,n\}} \{d_i\}$.

Agora, para cada $k \in \{0, \ldots, D-1\}$, seja $\mathfrak{j}_k$ o conjunto de todos os coeficientes líderes dos elementos de $\mathfrak{i}$ com grau no máximo k. De novo, $\mathfrak{j}_k$ é um ideal de A e portanto é finitamente gerado, isto é, $\mathfrak{j}_k = (a_1^k, \ldots, a_{m_k}^k)$. Como antes, seja $f_j^k \in \mathfrak{i}$ tendo coeficiente líder a_j^k, $j \in \{1, \ldots m_k\}$. Seja $\mathfrak{h}$ o ideal gerado pelos f_i, $i \in \{1, \ldots, n\}$ e pelos f_j^k, $k \in \{0, \ldots, D-1\}$, $j \in \{1, \ldots, m_k\}$.

É claro que $\mathfrak{h} \subseteq \mathfrak{i}$. Já se $\mathfrak{h} \subsetneq \mathfrak{i}$, então existe $f \in \mathfrak{i} - \mathfrak{h}$, de grau mínimo d e coeficiente líder a. Como $f \in \mathfrak{i}$, então $a \in \mathfrak{j} \Rightarrow a = r_1 a_1 + \ldots + r_n a_n$, $r_i \in A$, $i \in \{1, .., n\}$. Agora, suponha $d \geq D$. Se $g = r_1 x^{d-d_1} f_1 + .. + r_n x^{d-d_n} f_n$, então $\partial(g) = d$ e o coeficiente líder de g é $r_1 a_1 + \ldots + r_n a_n = a$, pois cada parcela $x^{d-d_i} f_i$ tem grau d. Como $g \in \mathfrak{h}$, então $f - g \notin \mathfrak{h}$. Mas $\partial(f - g) < d$, pois $\partial(f) = \partial(g) = d$, contradizendo a minimalidade do grau de f. Já se $d < D$, então $a \in \mathfrak{j}_d$ e uma construção análoga nos levará à mesma contradição. Logo $\mathfrak{h} = \mathfrak{i}$ e, portanto, $\mathfrak{i}$ é finitamente gerado. □

Corolário 1.1.5. *Se A é um anel noetheriano, assim o é $A[x_1, \ldots, x_n]$.*

Uma outra propriedade satisfeita pelos anéis noetherianos é dada pela proposição abaixo:

Proposição 1.1.6. *Seja A um anel noetheriano. Então todo ideal próprio de A contém um produto de ideais primos. Se A for um domínio de integridade, então todo ideal próprio não nulo de A contém um produto de ideais primos não nulos.*

Demonstração: Vamos provar a primeira afirmação; a demonstração da segunda é análoga. Suponha por absurdo que o resultado seja falso. Então existe $\mathfrak{i}$ um ideal próprio de A tal que $\mathfrak{i}$ não contém um produto de primos. Se S é o conjunto de todos os ideais próprios de A que não contêm um produto de primos, então $S \neq \emptyset$, pois $\mathfrak{i} \in S$. Como A é noetheriano, então S possui um elemento maximal $\mathfrak{i}_{max}$. Como $\mathfrak{i}_{max} \in S$, então, $\mathfrak{i}_{max}$ não é um ideal primo. Como $\mathfrak{i}_{max} \neq A$ (pois $\mathfrak{i}_{max} \subsetneq A$), então existem $a, b \in A$ tais que $ab \in \mathfrak{i}_{max}$ e $a, b \notin \mathfrak{i}_{max}$.

Assim $\mathfrak{i}_{max} \subsetneq \mathfrak{i}_{max} + (a)$ e $\mathfrak{i}_{max} \subsetneq \mathfrak{i}_{max} + (b)$. Pela maximalidade de $\mathfrak{i}_{max}$, então $\mathfrak{i}_{max} + (a)$ e $\mathfrak{i}_{max} + (b)$ contêm um produto de ideais primos, digamos $P_1 \cdot \ldots \cdot P_n \subseteq \mathfrak{i}_{max} + (a)$ e $Q_1 \cdot \ldots \cdot Q_m \subseteq \mathfrak{i}_{max} + (b)$. Dessa forma,

$$P_1 \cdot \ldots \cdot P_n \cdot Q_1 \cdot \ldots \cdot Q_m \subseteq (\mathfrak{i}_{max} + (a)) \cdot (\mathfrak{i}_{max} + (b)) \subseteq \mathfrak{i}_{max}.$$

Logo $\mathfrak{i}_{max}$ contém um produto de ideais primos, absurdo. □

1.2 Elementos integrais

Definição 1.2.1. *Seja B/A uma extensão de anéis. Dizemos que $b \in B$ é integral sobre A se existe $f(x) \in A[x]$ mônico tal que $f(b) = 0$.*

Exemplo 1.2.2. *Seja m um inteiro livre de quadrados e considere $\mathbb{Z} \subseteq \mathbb{Q}(\sqrt{m})$. Então $\sqrt{m}$ é integral sobre $\mathbb{Z}$: basta tomar $f(x) = x^2 - m$.*

Exemplo 1.2.3. *Sejam $m \in \mathbb{N}^*$, $\zeta_m = e^{2\pi i/m}$ e considere $\mathbb{Z} \subseteq \mathbb{Q}(\zeta_m)$. Então ζ_m é integral sobre $\mathbb{Z}$: basta tomar $f(x) = x^m - 1$.*

Definição 1.2.4. *Seja B/A uma extensão de anéis. Definimos o fecho integral de A em B por $\mathcal{O}_{B/A} = \{b \in B : b \text{ é integral sobre } A\}$.*

É claro que se $C/B/A$ são extensões de anéis, então $\mathcal{O}_{C/A} \cap B = \mathcal{O}_{B/A}$. Para demonstrar que $\mathcal{O}_{B/A}$ é um anel, precisamos antes do seguinte lema técnico:

Lema 1.2.5. *Sejam A um anel, $M \in \mathcal{M}_n(A)$ e $x = (x_1, \ldots, x_n)$ um vetor em A^n. Se $M \cdot x^t = (0)$, então $det(M) \cdot x_i = 0$, $\forall\ i \in \{1, \ldots, n\}$.*

Demonstração: Se M^* é a matriz adjunta de M, então $M^*M = \det(M)I_n$, onde I_n é a matriz identidade de ordem n sobre A. Assim, se $M \cdot x^t = 0$, multiplicamos à esquerda por M^* e obtemos $M^*M \cdot x^t = (0) \Rightarrow \det(M)I_n \cdot x^t = (0) \Rightarrow det(M) \cdot x_i = 0$, $\forall\ i \in \{1, \ldots, n\}$. □

Proposição 1.2.6. *Sejam B/A uma extensão de anéis e $b_1, \ldots, b_n \in B$. São equivalentes:*

1. *$b_1, \ldots, b_n$ são integrais sobre A;*
2. *O anel $A[b_1, \ldots, b_n]$ é um A-módulo finitamente gerado.*

Demonstração: (1) $\Rightarrow$ (2) : Por indução sobre n. Suponha então $n = 1$. Como b_1 é integral sobre A, então existe um polinômio mônico $f_1(x) \in A[x]$ de grau $d \geq 1$ tal que $f_1(b_1) = 0$. Então $A[b_1]$ é gerado por $1, b_1, \ldots, {b_1}^{d-1}$.

Suponha então que $b_1, \ldots, b_n, b_{n+1}$ são integrais sobre A e que $A[b_1, \ldots, b_n]$ é um A-módulo fiintamente gerado. Como b_{n+1} é integral sobre A, então b_{n+1} é integral sobre $A[b_1, \ldots, b_n]$. Logo $A[b_1, \ldots, b_n, b_{n+1}]$ é um $A[b_1, \ldots, b_n]$-módulo finitamente gerado. Como, por hipótese de indução, $A[b_1, \ldots, b_n]$ é um A-módulo finitamente gerado, então $A[b_1, \ldots, b_n, b_{n+1}]$ é um A-módulo finitamente gerado.

(2) $\Rightarrow$ (1) : Suponha que $A[b_1, \ldots, b_n]$ seja um A-módulo finitamente gerado por, digamos, $\omega_1, \ldots, \omega_m \in A[b_1, \ldots, b_n]$. Seja $b \in A[b_1, \ldots, b_n]$. Expressando cada $b \cdot \omega_i$ como uma combinação A-linear, existe uma matriz quadrada $M \in \mathcal{M}_m(A)$ tal que $\begin{pmatrix} b \cdot \omega_1 \\ \cdots \\ b \cdot \omega_m \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \cdots \\ \omega_m \end{pmatrix}$. Se I_m é a matriz identidade de ordem m em $\mathcal{M}_m(A)$ e $\omega = (\omega_1, \ldots, \omega_m)$, então $(M - b \cdot I_m) \cdot \omega^t = (0)$.

Pelo lema 1.2.5, $\det(M - b \cdot I_m) \cdot \omega_i = 0, \ \forall \ i \in \{1, \ldots, m\}$. Como $1 \in A[b_1, \ldots, b_n]$, então existem $c_1, \ldots, c_m \in A$ tais que $1 = c_1\omega_1 + \cdots + c_m\omega_m$. Multiplicando cada equação $\det(M - b \cdot I_m) \cdot \omega_i = 0$ por c_i e somando-as, obtemos $\det(M - b \cdot I_m) = 0$, ou seja, obtemos um polinômio mônico com coeficientes em A tendo b como raiz. Logo b é integral sobre A. □

Note que a demonstração acima mostra que *qualquer* elemento $b \in A[b_1, \ldots, b_n]$ é integral sobre A. Em particular, dados $b_1, \ b_2 \in B$ integrais sobre A, então $b_1 - b_2$ e b_1b_2 também são integrais sobre A. Assim, provamos o seguinte

Corolário 1.2.7. *Seja B/A uma extensão de anéis. Então $\mathcal{O}_{B/A}$ é um anel que satisfaz $A \subseteq \mathcal{O}_{B/A} \subseteq B$. Em particular, se A é um domínio de integridade e L é um corpo contendo $Frac(A)$, então $\mathcal{O}_{L/A}$ é um domínio de integridade que satisfaz $A \subseteq \mathcal{O}_{L/A} \subseteq L$.*

A propriedade a seguir, conhecida como *truque do determinante*, será usada mais à frente.

Lema 1.2.8. *Sejam A um domínio noetheriano e $\gamma \in K = Frac(A)$. Se existe um ideal $\mathfrak{i} \neq (0)$ em A tal que $\gamma\mathfrak{i} \subseteq \mathfrak{i}$, então, $\gamma \in \mathcal{O}_{K/A}$.*

Demonstração: Como A é noetheriano, então $\mathfrak{i} = (a_1, \ldots, a_n) \neq (0)$. Da relação $\gamma\mathfrak{i} \subseteq \mathfrak{i}$, segue que existe uma matriz $M \in \mathcal{M}_n(A)$ tal que

$$\gamma \begin{pmatrix} a_1 \\ \ldots \\ a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \ldots \\ a_n \end{pmatrix} \Rightarrow (\gamma I_n - M) \begin{pmatrix} a_1 \\ \ldots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \ldots \\ 0 \end{pmatrix}.$$

Pelo lema 1.2.5, $\det(\gamma I_n - M) \cdot a_i = 0, \ \forall \ i \in \{1, \ldots, n\}$. Como A é um domínio de integridade e $\mathfrak{i} \neq (0)$, então $\det(\gamma I_n - M) = 0 \Rightarrow \gamma$ é raiz do polinômio característico de M, o qual é um polinômio mônico sobre A. □

Definição 1.2.9. *Seja B/A uma extensão de anéis. Dizemos que B é integral sobre A (ou que B/A é uma extensão integral de anéis) se $\mathcal{O}_{B/A} = B$.*

Exemplo 1.2.10. *Se m é um inteiro positivo livre de quadrados, então $\mathbb{Z}[\sqrt{m}]$ é integral sobre $\mathbb{Z}$. De fato, se $a+b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, então $a+b\sqrt{m}$ é raiz do polinômio mônico $p(x) = x^2 - 2ax + a^2 - mb^2 \in \mathbb{Z}[x]$.*

Exemplo 1.2.11. *Se m é um inteiro positivo livre de quadrados, então $\mathbb{Z}[i\sqrt{m}]$ é integral sobre $\mathbb{Z}$. De fato, se $a+ib\sqrt{m} \in \mathbb{Z}[i\sqrt{m}]$, então $a+ib\sqrt{m}$ é raiz do polinômio mônico $p(x) = x^2 - 2ax + a^2 + mb^2 \in \mathbb{Z}[x]$.*

Vale ressaltar que ser integral é uma propriedade transitiva:

Proposição 1.2.12. *Sejam $C/B/A$ extensões de anéis. Se C é integral sobre B e B é integral sobre A, então C é integral sobre A.*

Demonstração: Seja $c \in C$. Como C é integral sobre B, então $\exists\ b_1, \ldots, b_n \in B$ tais que $c^n + b_1c^{n-1} + \cdots + b_n = 0$. Segue que $A[b_1, \ldots, b_n, c]$ é um $A[b_1, \ldots, b_n]$-módulo finitamente gerado. Agora, como B e integral sobre A, então $A[b_1, \ldots, b_n]$ é um A-módulo finitamente gerado $\Rightarrow A[b_1, \ldots, b_n, c]$ é um A-módulo finitamente gerado. Pela proposição 1.2.6, c é integral sobre A. □

Proposição 1.2.13. *Seja A um subanel de um domínio de integridade B e suponha que B é integral sobre A. Dessa forma, A é um corpo se, e somente se, B o é.*

Demonstração: ($\Rightarrow$) Suponha que A é um corpo e seja $b \in B - \{0\}$. Como A é um corpo, a proposição 1.2.6 nos dá que $A[b]$ é um A-espaço vetorial de dimensão finita.

Seja $f:\ A[b] \to A[b]$ dada por $f(z) = bz$. Note que f é uma transformação A-linear que é injetora, pois B é um domínio de integridade. Pelo Teorema do Núcleo e da Imagem, f é sobrejetora $\Rightarrow\ \exists\ z_0 \in A[b] \subseteq B$ tal que $f(z_0) = bz_0 = 1$. Logo $z_0 = b^{-1} \in B \Rightarrow B$ é um corpo.

($\Leftarrow$) Suponha agora que B seja um corpo e seja $a \in A - \{0\}$. Como $A \subseteq B$, $\exists\ a^{-1} \in B$. Agora, B é integral sobre A, logo existem $c_1, \ldots, c_n \in A$ tais que $(a^{-1})^n + c_1(a^{-1})^{n-1} + \cdots + c_n = 0$. Multiplicando esta equação por a^n, obtemos $1 + c_1a + \cdots + c_na^n = 0 \Rightarrow 1 = a\underbrace{(-c_1 - \cdots - c_na^{n-1})}_{=a^{-1}\in A} \Rightarrow A$ é um corpo. □

Corolário 1.2.14. *Seja B/A uma extensão integral de anéis. Seja $\mathfrak{q}$ um ideal primo de B e seja $\mathfrak{p} = \mathfrak{q} \cap A$. Então:*

1. *$\mathfrak{p}$ é um ideal primo de A e $\dfrac{A}{\mathfrak{p}}$ é isomorfo a um subanel de $\dfrac{B}{\mathfrak{q}}$.*
2. *$\dfrac{B}{\mathfrak{q}}$ é integral sobre $\dfrac{A}{\mathfrak{p}}$.*
3. *$\mathfrak{p}$ é um ideal maximal de A se, e somente se, $\mathfrak{q}$ é um ideal maximal de B.*

Demonstração: 1. Se $\mathfrak{p} = A$, então $\mathfrak{q} \cap A = A \Rightarrow A \subseteq \mathfrak{q}$. Como $1 \in A$, então $1 \in \mathfrak{q} \Rightarrow \mathfrak{q} = B$, absurdo, pois $\mathfrak{q}$ é um ideal primo de B.

Agora, sejam $x,\ y \in A$ tais que $xy \in \mathfrak{p}$. Então $xy \in \mathfrak{q}$. Como $\mathfrak{q}$ é um ideal primo de B, podemos supor sem perda de generalidade que $x \in \mathfrak{q}$. Logo $x \in \mathfrak{p} \Rightarrow \mathfrak{p}$ é um ideal primo de A.

Por fim, seja $f : \dfrac{A}{\mathfrak{p}} \to \dfrac{B}{\mathfrak{q}}$ dada por $f(\overline{x}) = \overline{\overline{x}}$, onde a barra denota a classe de equivalência de x em A módulo $\mathfrak{p}$ e as duas barras denotam a classe de equivalência de x em B módulo $\mathfrak{q}$. Então f está bem definida: de fato, se $\overline{x} = \overline{y}$, então $x - y \in \mathfrak{p} \Rightarrow x - y \in \mathfrak{q} \Rightarrow \overline{\overline{x}} = \overline{\overline{y}} \Rightarrow f(\overline{x}) = f(\overline{y})$. f é um homomorfismo injetor. É claro que f é um homomorfismo. Para ver sua injetividade, se $f(\overline{x}) = \overline{\overline{0}}$, então $\overline{\overline{x}} = \overline{\overline{0}} \Rightarrow x \in \mathfrak{q} \Rightarrow x \in \mathfrak{p} \Rightarrow \overline{x} = \overline{0}$.

2. Seja $\overline{\overline{x}} \in \dfrac{B}{\mathfrak{q}}$. Como B é integral sobre A, então existem $a_1, \ldots, a_n \in A$ tais que $x^n + a_1 x^{n-1} + \cdots + a_n = 0 \Rightarrow \overline{\overline{x}}^n + \overline{a_1}\ \overline{\overline{x}}^{n-1} + \cdots + \overline{a_n} = \overline{\overline{0}} \Rightarrow \overline{\overline{x}}$ é integral sobre $\dfrac{A}{\mathfrak{p}}$.

3. É consequência direta da proposição 1.2.13 e do item anterior. □

1.3 Domínios integralmente fechados

Definição 1.3.1. *Seja A um domínio de integridade e $K = Frac(A)$. Dizemos que A é um domínio integralmente fechado (DIF) se $\mathcal{O}_{K/A} \subseteq A$.*

Proposição 1.3.2. *Todo domínio domínio de fatoração única (DFU) é um DIF.*

Demonstração: Sejam A um DFU e $\dfrac{a}{b} \in \mathcal{O}_{K/A}$. Como A é um DFU, podemos supor que a e b não têm fatores em comum. Como $\dfrac{a}{b} \in \mathcal{O}_{K/A}$, então existem a_1, ..., $a_n \in A$ tais que $\left(\dfrac{a}{b}\right)^n + a_1 \left(\dfrac{a}{b}\right)^{n-1} + \ldots + a_n = 0$. Multiplicando tal equação por b^n, obtemos

$$a^n + a_1 b a^{n-1} + \ldots + b^n a_n = 0 \Rightarrow a^n = -b(a_1 a^{n-1} + \ldots + b^{n-1} a_n) \Rightarrow b \mid a^n.$$

Como a e b não têm fatores em comum, então $b \in A^\times \Rightarrow \dfrac{a}{b} \in A \Rightarrow A$ é integralmete fechado. □

Note então que todo corpo é um domínio euclidiano (DE), todo DE é um DIP, todo DIP é um DFU e todo DFU é um DIF.

Exemplo 1.3.3. *$\mathbb{Z}$ é um DIF.*

Exemplo 1.3.4. *Seja K um corpo e considere o subanel $A = K[x^2, x^3] \subseteq K[x]$. Então A é um domínio de integridade que não é integralmente fechado. De fato, seja $L = Frac(A) = K(x)$. Então $x = \dfrac{x^3}{x^2} \in \mathcal{O}_{L/A} - A$. De fato, x é raiz do polinômio mônico $T^2 - x^2 \in L[T]$.*

É interessante notar que vale o análogo do teorema da base de Hilbert para domínios integralmente fechados. Para demonstrarmos esse resultado, precisamos antes do seguinte

Lema 1.3.5. *Sejam A um DIF, $K = Frac(A)$, $b \in K$ e $g(x) \in A[x]$. Seja $f(x) = bx^m + g(x)$, onde $m \in \mathbb{N}$. Se existem polinômios $p_1(x), \ldots, p_r(x) \in A[x]$ tais que*

$$f(x)^r + p_1(x)f(x)^{r-1} + \cdots + p_r(x) = 0,$$

então $b \in A$. Em particular, $f(x) \in A[x]$.

Demonstração: Da equação

$$f(x)^r + p_1(x)f(x)^{r-1} + \cdots + p_r(x) = 0$$

obtemos

$$[bx^m + g(x)]^r + p_1(x)[bx^m + g(x)]^{r-1} + \cdots + p_r(x) = 0$$

donde

$$b^r x^{mr} + \sum_{i=1}^{r} \left(\begin{array}{c} r \\ i \end{array} \right) b^{r-i} x^{m(r-i)} g(x)^i + p_1(x)[bx^m + g(x)]^{r-1} + \cdots + p_r(x) = 0.$$

Note que qualquer parcela da soma acima diferente de $b^r x^{mr}$ tem como coeficiente do monômio de grau mr potências de b com expoentes estritamente menores que r. Como $g(x),\ p_1(x), \ldots, p_r(x) \in A[x]$ e a igualdade acima ocorre em $K[x]$ (que é um domínio de integridade), segue que b satisfaz um polinômio mônico com coeficientes em A. Assim, b é integral sobre A. Como A é um DIF, $b \in A$. □

Proposição 1.3.6. *Se A é um DIF, assim o é $A[x]$.*

Demonstração: Seja $K = \text{Frac}(A)$ e seja $f(x) \in \text{Frac}(A[x]) = A(x)$ um elemento integral sobre $A[x]$. Como $A[x] \subseteq K[x] \subseteq A(x)$, então $f(x)$ é integral sobre $K[x]$. Como $K[x]$ é um DIF (pois é um DIP), então $f(x) \in K[x]$. Escreva

$$f(x) = a_n x^n + \cdots + a_0, \qquad \text{onde } a_0, \ldots, a_n \in K.$$

Como $f(x)$ é integral sobre $A[x]$, existem polinômios $p_1(x), \ldots, p_r(x) \in A[x]$ tais que

$$f(x)^r + p_1(x)f(x)^{r-1} + \cdots + p_r(x) = 0.$$

Vamos mostrar por indução em $n = \partial(f)$ que $f(x) \in A[x]$. Se $n = 0$, então o resultado segue do lema anterior aplicado a $b = a_0,\ m = 0$ e $g(x) = 0$. Suponha então o resultado válido para todo polinômio de grau no máximo $n - 1$. Assim, se $\partial(f) = n$, seja $g(x) = f(x) - a_n x^n \in A[x]$, por hipótese de indução. De novo, o resultado segue do lema anterior, agora tomando $b = a_n$ e $m = n$. □

Corolário 1.3.7. *Se A é um domínio integralmente fechado, assim o é $A[x_1, \ldots, x_n]$.*

Antes de finalizarmos essa seção, vejamos uma propriedade satisfeita pelos DIFs. Para isso, precisamos antes da seguinte:

Proposição 1.3.8. *Seja A um domínio de integridade, $K = Frac(A)$ e L/K uma extensão de corpos. Se $\alpha \in L$ é algébrico sobre K, então existe $d \in A - \{0\}$ tal que $d\alpha$ é integral sobre A.*

Demonstração: Por hipótese, α satisfaz uma equação

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0, \qquad a_i \in K, \quad i \in \{1, \ldots, m\}.$$

Se $d \in A$ é um denominador comum dos a_i, então $d \neq 0$ e $d \cdot a_i \in A$, $\forall\ i \in \{1, \ldots, m\}$. Multiplicando a igualdade acima por d^m, obtemos

$$d^m\alpha^m + a_1 d^m\alpha^{m-1} + \ldots + d^m a_m = 0,$$

ou seja,

$$(d\alpha)^m + a_1 d(d\alpha)^{m-1} + .. + a_m d^m = 0.$$

Como $a_1 d$, $\ldots$, $a_m d^m \in A$, então $d\alpha$ é integral sobre A. □

Corolário 1.3.9. *Seja A um domínio de integridade, $K = Frac(A)$ e L/K uma extensão de corpos. Se L é algébrico sobre K, então $Frac(\mathcal{O}_{L/A}) = L$.*

Demonstração: Seja $\alpha \in L$. Como L/K é uma extensão algébrica, então α é algébrico sobre K. Pela proposição anterior, existe $d \in A - \{0\}$ tal que $d\alpha \in \mathcal{O}_{L/A}$. Assim $\alpha = \dfrac{d\alpha}{d}$, onde $d\alpha \in \mathcal{O}_{L/A}$ e $d \in A - \{0\} \subseteq \mathcal{O}_{L/A} \Rightarrow L \subseteq \text{Frac}(\mathcal{O}_{L/A})$. Como a outra inclusão é trivial, o corolário está demonstrado. □

1.4 Domínios de Dedekind

Definição 1.4.1. *Seja A um domínio de integridade. Dizemos que A é um domínio de Dedekind se:*

1. *A é noetheriano;*
2. *A é integralmente fechado;*
3. *Todo ideal primo não nulo de A é maximal.*

Exemplo 1.4.2. *Todo DIP é um domínio de Dedekind. Em particular, $\mathbb{Z}$ é um domínio de Dedekind e se K é um corpo, então tanto K quanto $K[x]$ são domínios de Dedekind.*

Exemplo 1.4.3. *Se A é um domínio de Dedekind, então não necessariamente $A[x]$ o é. De fato, $\mathbb{Z}$ é um domínio de Dedekind, enquanto que $\mathbb{Z}[x]$ não o é, pois o ideal $\mathfrak{i} = (x)$ é primo mas não é maximal, dado que $\dfrac{\mathbb{Z}[x]}{(x)} \approx \mathbb{Z}$.*

Proposição 1.4.4. *Seja K um corpo tal que $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$. Então $\mathcal{O}_{K/\mathbb{Z}}$ é um DIF e todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_{K/\mathbb{Z}}$ é maximal.*

Demonstração: Primeiramente, devemos mostrar que $\mathcal{O}_{\mathrm{Frac}(\mathcal{O}_{K/\mathbb{Z}})/\mathcal{O}_{K/\mathbb{Z}}} \subseteq \mathcal{O}_{K/\mathbb{Z}}$. Para isto, seja $x \in \mathcal{O}_{\mathrm{Frac}(\mathcal{O}_{K/\mathbb{Z}})/\mathcal{O}_{K/\mathbb{Z}}} = \{x \in \mathrm{Frac}(\mathcal{O}_{K/\mathbb{Z}}) : x \text{ é integral sobre } \mathcal{O}_{K/\mathbb{Z}}\}$. Como $x \in \mathrm{Frac}(\mathcal{O}_{K/\mathbb{Z}}) \subseteq K$, então $x \in K$. Agora, como x é integral sobre $\mathcal{O}_{K/\mathbb{Z}}$ e $\mathcal{O}_{K/\mathbb{Z}}$ é integral sobre $\mathbb{Z}$, segue da proposição 1.2.12 que x é integral sobre $\mathbb{Z} \Rightarrow x \in \mathcal{O}_{K/\mathbb{Z}}$.

Agora, mostremos que todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_{K/\mathbb{Z}}$ é maximal. Ora, como $\mathfrak{p}$ é não nulo, existe $y \in \mathfrak{p} - \{0\}$. Como $y \in \mathcal{O}_{K/\mathbb{Z}}$, então existem $a_1, \ldots, a_n \in \mathbb{Z}$ tais que

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0.$$

Como podemos tomar n o menor possível, então $a_n \neq 0$. Pelo corolário 1.2.14, $\mathfrak{p} \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$ que é não nulo, pois, $a_n \in \mathfrak{p} \cap \mathbb{Z}$. Como $\mathbb{Z}$ é um domínio de Dedekind, então $\mathfrak{p} \cap \mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$. De novo pelo corolário 1.2.14, $\mathfrak{p}$ é um ideal maximal de $\mathcal{O}_{K/\mathbb{Z}}$, e a proposição está demonstrada. □

É interessante notar que para cada uma das três condições que definem um domínio de Dedekind, existe um domínio A não satisfazendo tal condição e satisfazendo as outras duas. Veja:

- $\mathbb{Z}[x]$ satisfaz *1* e *2*, mas não *3*. Mais geralmente, se A é um domínio noetheriano integralmente fechado, então $A[x, y]$ satisfaz *1* e *2*, mas não *3*. De fato, (y) é um ideal primo não-nulo de $A[x, y]$ que não é maximal, pois, $\dfrac{A[x, y]}{(y)} \approx A[x]$.
- Se K é um corpo, o domínio $A = K[x^2, x^3] \subseteq K[x]$ do exemplo 1.3.4 satisfaz *1* e *3* (pois é um DIP - veja lema 1.9.1), mas não *2*.
- Mais à frente daremos um exemplo clássico de um domínio que satisfaz *2*, *3*, mas não *1*.

Dois serão os principais resultados acerca dos domínios de Dedekind que demonstraremos nesta seção. Para isso, precisamos antes de alguns lemas.

Lema 1.4.5. *Seja $\mathfrak{i}$ um ideal próprio não nulo de um domínio de Dedekind A com corpo de frações K. Então existe $\gamma \in K - A$ tal que $\gamma\mathfrak{i} \subseteq A$.*

Demonstração: Como $\mathfrak{i} \neq (0)$, seja $a \in \mathfrak{i} - \{0\}$. Note que $a \notin A^\times$, pois $\mathfrak{i} \neq A$. Pela proposição 1.1.6, o ideal (a) contém um produto de ideais primos não nulos $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, onde r é mínimo.

Como $\mathfrak{i}$ é um ideal próprio de A, o lema 1.9.2 implica a existência de um ideal maximal (o qual é necessariamente primo) $\mathfrak{p}$ tal que $\mathfrak{i} \subseteq \mathfrak{p}$. Então $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{i} \subseteq \mathfrak{p}$. Como $\mathfrak{p}$ é ideal primo, então existe $i \in \{1, \ldots r\}$ tal que $\mathfrak{p}_i \subseteq \mathfrak{p}$. Suponha sem perda de generalidade que $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Como A é um domínio de Dedekind, $\mathfrak{p} = \mathfrak{p}_1$.

Se $r = 1$, então $(a) = \mathfrak{i} = \mathfrak{p}$. Como $\mathfrak{p}$ é um ideal primo, existe $b \in A - (a)$. Assim, $\gamma = \dfrac{b}{a} \in K - A$. Com efeito, se $\dfrac{b}{a} \in A$, então $\exists\ c \in A$ tal que $\dfrac{b}{a} = c \Rightarrow b = ac \in (a)$, absurdo. Dessa forma, $\gamma\mathfrak{i} = \gamma(a) = (b) \subseteq A$.

Suponha então $r \geq 2$. Como r é mínimo, (a) não pode conter um produto de ideais primos que tem menos do que r fatores. Logo existe $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r - (a)$. Procedendo como antes, $\gamma = \dfrac{b}{a} \in K - A$. Ademais, $\gamma\mathfrak{i} \subseteq A$. De fato, $b\mathfrak{p}_1 \subseteq \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq (a) \Rightarrow b\mathfrak{p}_1 \subseteq (a) \Rightarrow \left(\dfrac{b}{a}\right)\mathfrak{p}_1 \subseteq A \Rightarrow \gamma\mathfrak{i} \subseteq \gamma\mathfrak{p} = \gamma\mathfrak{p}_1 \subseteq A$. □

Lema 1.4.6. *Seja* $\mathfrak{i}$ *um ideal não nulo de um domínio de Dedekind* A*. Então existe um ideal não nulo* $\mathfrak{j}$ *de* A *tal que* $\mathfrak{ij}$ *é principal e não nulo.*

Demonstração: Como $\mathfrak{i} \neq (0)$, sejam $\alpha \in \mathfrak{i} - \{0\}$ e $\mathfrak{j} = \{\beta \in A : \beta\mathfrak{i} \subseteq (\alpha)\}$. Então $\mathfrak{j}$ é um ideal não nulo de A (pois $\alpha \in \mathfrak{j}$) tal que $\mathfrak{ij} \subseteq (\alpha)$. Vamos mostrar que $(\alpha) \subseteq \mathfrak{ij}$.

Considere o conjunto $\mathfrak{h} = \dfrac{1}{\alpha}\mathfrak{ij} \subseteq A$, que é também um ideal não nulo de A. Se $\mathfrak{h} = A$, então $\mathfrak{ij} = (\alpha)$. De fato, se $x \in (\alpha)$, então $\exists\ y \in A$ tal que $x = \alpha y$. Como $y \in A = \dfrac{1}{\alpha}\mathfrak{ij}$, então $\exists\ z \in \mathfrak{ij}$ tal que $y = \dfrac{1}{\alpha}z$. Logo $x = \alpha y = \alpha \cdot \dfrac{1}{\alpha}z = z \in \mathfrak{ij} \Rightarrow (\alpha) \subseteq \mathfrak{ij}$.

Caso contrário, $\mathfrak{h}$ é um ideal próprio, no qual nós podemos aplicar o lema 1.4.5. Então $\gamma\mathfrak{h} \subseteq A$, para algum $\gamma \in K - A$, com $K = \mathrm{Frac}(A)$. Vamos mostrar que $\gamma \in \mathcal{O}_{K/A}$. Como A é Dedekind, A é integralmente fechado $\Rightarrow \mathcal{O}_{K/A} \subseteq A \Rightarrow \gamma \in A$, absurdo.

Como $\mathfrak{j} \subseteq \mathfrak{h}$ (pois $\alpha \in \mathfrak{i}$), então $\gamma\mathfrak{j} \subseteq \gamma\mathfrak{h} \subseteq A$. Afirmo que $\gamma\mathfrak{j} \subseteq \mathfrak{j}$. De fato, seja $j \in \mathfrak{j}$. Precisamos mostrar que $\gamma j\mathfrak{i} \subseteq (\alpha)$. Para isso, seja $i \in \mathfrak{i}$. Então $\gamma\dfrac{1}{\alpha}ij \in \gamma\mathfrak{h} \subseteq A \Rightarrow \gamma\dfrac{1}{\alpha}ij \in A \Rightarrow\ \exists\ a \in A$ tal que $\gamma\dfrac{1}{\alpha}ij = a \Rightarrow \gamma ij = \alpha a \in (\alpha) \Rightarrow \gamma ji \in (\alpha) \Rightarrow \gamma j\mathfrak{i} \subseteq (\alpha)$. Logo, $\gamma\mathfrak{j} \subseteq \mathfrak{j}$. Pelo lema 1.2.8, $\gamma \in \mathcal{O}_{K/A}$. □

O lema anterior mostra a existência de um *ideal principalizador* para um ideal não nulo de um domínio de Dedekind. Em particular, ele implica a *lei do cancelamento de ideais não nulos em um domínio de Dedekind*:

Corolário 1.4.7. *Se* $\mathfrak{i}_1$*,* $\mathfrak{i}_2$ *e* $\mathfrak{i}_3$ *são ideais não nulos em um domínio de Dedekind tais que* $\mathfrak{i}_1\mathfrak{i}_2 = \mathfrak{i}_1\mathfrak{i}_3$*, então* $\mathfrak{i}_2 = \mathfrak{i}_3$*.*

Demonstração: Sabemos que existe $\mathfrak{j} \neq (0)$ um ideal tal que $\mathfrak{i}_1\mathfrak{j}$ é principal e não nulo. Seja $\mathfrak{i}_1\mathfrak{j} = (\alpha) \neq (0)$. Então $(\alpha)\mathfrak{i}_2 = \mathfrak{i}_1\mathfrak{j}\mathfrak{i}_2 = \mathfrak{j}\mathfrak{i}_1\mathfrak{i}_2 = \mathfrak{j}\mathfrak{i}_1\mathfrak{i}_3 = \mathfrak{i}_1\mathfrak{j}\mathfrak{i}_3 = (\alpha)\mathfrak{i}_3 \Rightarrow \mathfrak{i}_2 = \mathfrak{i}_3$. □

Corolário 1.4.8. *Seja* A *um domínio de Dedekind. Se* $\mathfrak{i}_1$ *e* $\mathfrak{i}_2$ *são dois ideais não nulos de* A *tais que* $\mathfrak{i}_1 \subseteq \mathfrak{i}_2$*, então existe um ideal não nulo* $\mathfrak{j}$ *de* A *tal que* $\mathfrak{i}_1 = \mathfrak{i}_2\mathfrak{j}$*.*

Demonstração: Pelo lema 1.4.6, existe um ideal não nulo $\mathfrak{h}$ de A tal que $\mathfrak{i}_2\mathfrak{h}$ é principal e não nulo; digamos $\mathfrak{i}_2\mathfrak{h} = (\alpha),\ \alpha \in A - \{0\}$. Seja $\mathfrak{j} = \frac{1}{\alpha}\mathfrak{i}_1\mathfrak{h}$.

Afirmo que $\mathfrak{j}$ é um ideal não nulo de A. De fato, para ver que $\mathfrak{j} \subseteq A$, note que $\mathfrak{i}_1 \subseteq \mathfrak{i}_2 \Rightarrow \mathfrak{i}_1\mathfrak{h} \subseteq \mathfrak{i}_2\mathfrak{h} = (\alpha) \Rightarrow \mathfrak{i}_1\mathfrak{h} \subseteq (\alpha) \Rightarrow \mathfrak{j} = \frac{1}{\alpha}\mathfrak{i}_1\mathfrak{h} \subseteq A$. Ademais, $\mathfrak{j} \neq (0)$, pois $\mathfrak{i}_1,\ \mathfrak{h} \neq (0)$. Por fim, $\mathfrak{i}_2\mathfrak{j} = \mathfrak{i}_2\frac{1}{\alpha}\mathfrak{i}_1\mathfrak{h} = \mathfrak{i}_1\frac{1}{\alpha}\mathfrak{i}_2\mathfrak{h} = \mathfrak{i}_1\frac{1}{\alpha}(\alpha) = \mathfrak{i}_1$. □

O cororálario 1.4.7 funciona como uma *lei do cancelamento* para ideais não nulos de um domínio de Dedekind. Com ele, obtemos o *teorema da fatoração única de ideais em domínios de Dedekind*. Mais precisamente,

Teorema 1.4.9. *Todo ideal próprio não nulo* $\mathfrak{i}$ *de um domínio de Dedekind* A *é unicamente representável como um produto de ideais primos.*

Demonstração: Existência: Seja S o conjunto de todos os ideais próprios não nulos $\mathfrak{i}$ de A tais que $\mathfrak{i}$ não é representável como um produto de ideais primos. Se $S \neq \emptyset$, então S admite um elemento maximal $\mathfrak{i}_{max}$, pois A é noetheriano. Pelo lema 1.9.2, $\mathfrak{i}_{max} \subseteq \mathfrak{p}$, para algum ideal primo $\mathfrak{p}$ de A (pois todo ideal maximal é primo). Pelo corolário 1.4.8, $\mathfrak{i}_{max} = \mathfrak{p}\mathfrak{j}$, para algum ideal não nulo $\mathfrak{j}$ de A. Logo $\mathfrak{i}_{max} \subseteq \mathfrak{j}$, e a inclusão é estrita. De fato, se $\mathfrak{i}_{max} = \mathfrak{j}$, então $A\mathfrak{i}_{max} = A\mathfrak{p}\mathfrak{j} = \mathfrak{p}\mathfrak{j} = \mathfrak{p}\mathfrak{i}_{max} \Rightarrow A = \mathfrak{p}$, absurdo. Assim $\mathfrak{i}_{max} \subsetneq \mathfrak{j}$. Pela maximalidade de $\mathfrak{i}_{max}$, $\mathfrak{j}$ é um produto de ideais primos $\Rightarrow \mathfrak{i}_{max} = \mathfrak{p}\mathfrak{j}$ é um produto de ideais primos, contradição.

Unicidade: Suponha que $\mathfrak{i} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$ são duas representações de $\mathfrak{i}$ como um produto de ideais primos. Então $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \subseteq \mathfrak{p}_1$. Assim existe $i \in \{1, \ldots, s\}$ tal que $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. Suponha sem perda de generalidade que $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Como A é Dedekind, $\mathfrak{q}_1$ é um ideal maximal de A. Então $\mathfrak{p}_1 = \mathfrak{q}_1$, e, pelo corolário 1.4.7, $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s$. Continando assim, iremos obter $r = s$ e $\mathfrak{q}_i = \mathfrak{p}_i$, para todo $i \in \{1, \ldots, r = s\}$. □

Corolário 1.4.10. *Seja* A *um domínio de Dedekind. Então* A *é um DIP se, e somente se, é um DFU.*

Demonstração: Precisamos apenas provar a recíproca. Mostrarems inicialmente que todo ideal primo não nulo de A é principal. Assim, seja $\mathfrak{p} \neq (0)$ um ideal primo de A e seja $a \in \mathfrak{p} - \{0\}$. Como A é um DFU, então a se fatora como um produto de elementos irredutíveis de A, i.e., $a = p_1 \cdot \ldots \cdot p_n$. Como $\mathfrak{p}$ é um ideal primo de A, então $\mathfrak{p}$ contém um desses elementos irredutíveis p_i. Então $(p_i) \subseteq \mathfrak{p}$. Agora, como p_i é um elemento irredutível de A, que é um DFU, então (p_i) é um ideal primo de A. Como A é Dedekind, então (p_i) é um ideal maximal. Como $(p_i) \subseteq \mathfrak{p} \subsetneq A$, então $(p_i) = \mathfrak{p}$.

Finalizando, como todo ideal próprio de um domínio de Dedekind pode ser escrito como um produto de ideais primos, então todo ideal próprio de um domínio de Dedekind pode ser escrito como um produto de ideais principais. Agora, como o produto de ideais principais é principal, o corolário está demonstrado. □

O teorema 1.4.9 implica também o seguinte refinamento do lema 1.4.6:

Proposição 1.4.11. *Seja* $\mathfrak{i}$ *um ideal não nulo de um domínio de Dedekind* A*. Então existe um ideal não nulo* $\mathfrak{j}$ *de* A *tal que* $\mathfrak{ij}$ *é principal e não nulo. Se* $\mathfrak{h}$ *é qualquer ideal não nulo de* A*, então* $\mathfrak{j}$ *pode ser escolhido coprimo com* $\mathfrak{h}$*.*

Demonstração: Como todo ideal é coprimo com o anel todo, o lema 1.4.6 é o caso particular $\mathfrak{h} = A$. Portanto podemos supor $\mathfrak{h}$ um ideal não nulo e próprio de A. Pelo teorema 1.4.9, $\mathfrak{h} = \mathfrak{p}_1^{\alpha_1} \cdot \ldots \cdot \mathfrak{p}_n^{\alpha_n}$, onde $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ são ideais primos não nulos de A e $\mathfrak{p}_i \neq \mathfrak{p}_j$ se $i \neq j$.

1º caso: $n = 1$.

Então $\mathfrak{h} = \mathfrak{p}_1^{\alpha_1}$, onde $\alpha_1 \in \mathbb{N}^*$. Afirmo que $\mathfrak{ip}_1 \subsetneq \mathfrak{i}$. De fato, se $\mathfrak{ip}_1 = \mathfrak{i} = \mathfrak{i}A$, então pela lei do cancelamento $\mathfrak{p}_1 = A$, absurdo. Logo $\exists\ a \in \mathfrak{i} - \mathfrak{ip}_1$. Em particular, $a \neq 0$. Como $(a) \subseteq \mathfrak{i}$, pelo corolário 1.4.8 existe um ideal não nulo $\mathfrak{j}$ de A tal que $(a) = \mathfrak{ij}$. Afirmo que $\mathfrak{j}$ é coprimo com $\mathfrak{p}_1$. De fato, suponha por absurdo que $\mathfrak{j} \subseteq \mathfrak{p}_1$. Então $(a) = \mathfrak{ij} \subseteq \mathfrak{ip}_1 \Rightarrow a \in \mathfrak{ip}_1$, absurdo. Logo $\mathfrak{j} \nsubseteq \mathfrak{p}_1$. Como A é um domínio de Dedekind, $\mathfrak{p}_1$ é maximal, e logo $\mathfrak{j}$ é coprimo com $\mathfrak{p}_1$, em virtude do lema 1.9.5. Pelo lema 1.9.4, $\mathfrak{j} + \mathfrak{p}_1^{\alpha_1} = \mathfrak{j} + \mathfrak{h} = A$.

2º caso: $n \geq 2$.

Sejam $\mathfrak{h}_0 = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$ e $\mathfrak{q}_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} \mathfrak{p}_j,\ \forall\ i \in \{1, \ldots, n\}$. Note que $\mathfrak{h}_0 = \mathfrak{q}_i\mathfrak{p}_i \subseteq \mathfrak{q}_i \Rightarrow \mathfrak{ih}_0 \subseteq \mathfrak{iq}_i,\ \forall\ i \in \{1, \ldots, n\}$. Afirmo que $\mathfrak{ih}_0 \subsetneq \mathfrak{iq}_i,\ \forall\ i \in \{1, \ldots, n\}$. Com efeito, se $\mathfrak{ih}_0 = \mathfrak{iq}_i$, para algum $i \in \{1, \ldots, n\}$, então, pela lei do cancelamento, $\mathfrak{h}_0 = \mathfrak{q}_i$, absurdo pelo teorema da fatoração única. Assim, $\mathfrak{ih}_0 \subsetneq \mathfrak{iq}_i,\ \forall\ i \in \{1, \ldots, n\}$. Para cada $i \in \{1, \ldots, n\}$, seja $a_i \in \mathfrak{iq}_i - \mathfrak{ih}_0$ e seja $a = \sum_{i=1}^{n} a_i$. Como $a_i \in \mathfrak{iq}_i \subseteq \mathfrak{i}$, então $a_i \in \mathfrak{i},\ \forall\ i \in \{1, \ldots, n\} \Rightarrow a \in \mathfrak{i}$.

Afirmo que $a \notin \mathfrak{ip}_i,\ \forall\ i \in \{1, \ldots, n\}$. De fato, suponha que $a \in \mathfrak{ip}_{i_0}$, para algum $i_0 \in \{1, \ldots, n\}$. Escreva $a = a_{i_0} + \sum_{\substack{i=1 \\ i \neq i_0}}^{n} a_i$. Se $i \neq i_0$, então $\mathfrak{q}_i \subseteq \mathfrak{p}_{i_0} \Rightarrow \mathfrak{iq}_i \subseteq \mathfrak{ip}_{i_0}$. Como $a_i \in \mathfrak{iq}_i$, então $a_i \in \mathfrak{ip}_{i_0}$. Logo $\sum_{\substack{i=1 \\ i \neq i_0}}^{n} a_i \in \mathfrak{ip}_{i_0}$. Como estamos supondo que $a \in \mathfrak{ip}_{i_0}$, então $a_{i_0} \in \mathfrak{ip}_{i_0}$. Mas a_{i_0} também pertence a $\mathfrak{iq}_{i_0}$. Logo $a_{i_0} \in \mathfrak{ip}_{i_0} \cap \mathfrak{iq}_{i_0} \subseteq \mathfrak{i} \cap \mathfrak{p}_{i_0} \cap \mathfrak{i} \cap \mathfrak{q}_{i_0} = \mathfrak{i} \cap \underbrace{\mathfrak{p}_{i_0} \cap \mathfrak{q}_{i_0}}_{=\mathfrak{h}_0} = \mathfrak{ih}_0$, absurdo. Logo $a \notin \mathfrak{ip}_i,\ \forall\ i \in \{1, \ldots, n\}$. Em particular, $a \neq 0$.

Como $a \in \mathfrak{i}$, então $(a) \subseteq \mathfrak{i}$. Pelo corolário 1.4.8, existe um ideal não nulo $\mathfrak{j}$ de A tal que $(a) = \mathfrak{ij}$. Se $\mathfrak{j} \subseteq \mathfrak{p}_i$, para algum $i \in \{1, \ldots, n\}$, então de novo pelo corolário 1.4.8 existe um ideal não nulo $\mathfrak{j}_0$ de A tal que $\mathfrak{j} = \mathfrak{p}_i\mathfrak{j}_0 \Rightarrow (a) = \mathfrak{ij} = \mathfrak{ip}_i\mathfrak{j}_0 \subseteq \mathfrak{ip}_i \Rightarrow a \in \mathfrak{ip}_i$, absurdo. Então $\mathfrak{j} \nsubseteq \mathfrak{p}_i,\ \forall\ i \in \{1, \ldots, n\}$. Pelo lema 1.9.5, $\mathfrak{j} + \mathfrak{p}_i = A,\ \forall\ i \in \{1, \ldots, n\}$. Pelo lema 1.9.3, $\mathfrak{j} + \mathfrak{p}_i^{\alpha_i} = A,\ \forall\ i \in \{1, \ldots, n\}$. Pelo lema 1.9.4, $\mathfrak{j} + \mathfrak{p}_1^{\alpha_1} \cdot \ldots \cdot \mathfrak{p}_n^{\alpha_n} = \mathfrak{j} + \mathfrak{h} = A$. □

Corolário 1.4.12. *Seja* $\mathfrak{i}$ *um ideal não nulo de um dominio de Dedekind* A*, e seja* $\alpha \in \mathfrak{i} - \{0\}$*. Então* $\exists\ \beta \in \mathfrak{i}$ *tal que* $\mathfrak{i} = (\alpha, \beta)$*.*

Demonstração: Como $\alpha \in \mathfrak{i}$, então $(\alpha) \subseteq \mathfrak{i}$. Como $\alpha \neq 0$, pelo corolário 1.4.8 existe um ideal $\mathfrak{h}$ não nulo de A tal que $(\alpha) = \mathfrak{i}\mathfrak{h}$. Como $\mathfrak{i} \neq (0)$, a proposição 1.4.11 garante a existência de um ideal $\mathfrak{j}$ não nulo de A tal que $\mathfrak{j}$ é coprimo com $\mathfrak{h}$ e $\mathfrak{i}\mathfrak{j}$ é principal e não nulo. Escreva $\mathfrak{i}\mathfrak{j} = (\beta),\ \beta \in A - \{0\}$.

Então $(\alpha, \beta) = (\alpha) + (\beta) = \mathfrak{i}\mathfrak{h} + \mathfrak{i}\mathfrak{j} = \mathfrak{i}(\mathfrak{h} + \mathfrak{j}) = \mathfrak{i}A = \mathfrak{i}$. □

Corolário 1.4.13. *Um domínio de Dedekind* A *com um número finito de ideais primos é um DIP.*

Demonstração: Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ todos os ideais primos não nulos de A e seja $\mathfrak{h} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$. Seja $\mathfrak{i}$ um ideal próprio não nulo de A. Pela proposição 1.4.11, existe um ideal $\mathfrak{j}$ não nulo de A tal que $\mathfrak{j}$ é coprimo com $\mathfrak{h}$ e $\mathfrak{i}\mathfrak{j}$ é principal e não nulo. Escreva $\mathfrak{i}\mathfrak{j} = (a),\ a \in A - \{0\}$.

Como $\mathfrak{j}$ é coprimo com $\mathfrak{h}$, então $\mathfrak{j} = A$. De fato, se $\mathfrak{j} \subsetneq A$, então pelo teorema 1.4.9, $\mathfrak{j}$ é um produto de ideais primos não nulos de A. Logo $\mathfrak{h} \subseteq \mathfrak{j} \Rightarrow \mathfrak{h} + \mathfrak{j} = \mathfrak{j}$. Mas como $\mathfrak{h}$ é coprimo com $\mathfrak{j}$, então $\mathfrak{h} + \mathfrak{j} = A \Rightarrow \mathfrak{j} = A$, absurdo. Então $\mathfrak{i} = \mathfrak{i}A = \mathfrak{i}\mathfrak{j} = (a)$. □

É interessante notar que o teorema 1.4.9 é, na verdade, uma caracterização dos domínios de Dedekind:

Proposição 1.4.14. *Seja* A *um domínio de integridade tal que todo ideal próprio não nulo admite uma fatoração única em ideais primos. Então* A *é um domínio de Dedekind.*

A demonstração desta proposição foge um pouco do escopo desta dissertação e por isso será omitida. Entretanto, uma prova dela pode ser encontrada em [2], p. 494 - 495.

1.5 O anel de números de um corpo de números

Definição 1.5.1. *Um corpo de números é um corpo* $K \subseteq \mathbb{C}$ *tal que* $[K : \mathbb{Q}] < \infty$*.*

Claramente, os corpos da forma $\mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$, m livre de quadrados, são corpos de números, denominados *corpos quadráticos*. Se $m > 0$, então $\mathbb{Q}(\sqrt{m})$ é chamado de *corpo quadrático real*. Caso $m < 0$, então $\mathbb{Q}(\sqrt{m})$ é chamado de *corpo quadrático imaginário*.

Outro exemplo de corpo de números é $\mathbb{Q}(\zeta_m)$, onde $\zeta_m = e^{2\pi i/m}$, $m \in \mathbb{N}^*$, chamado de *m-ésimo corpo ciclotômico*. Registramos no teorema abaixo as propriedades básicas do corpo $\mathbb{Q}(\zeta_m)$. Para uma demonstração, veja [16], p. 63 - 94.

Teorema 1.5.2. *Seja φ a função de Euler. Se $m \in \mathbb{N}^*$, então a extensão $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ é galoisiana, $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ e $\mathrm{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \cong \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$, onde o isomorfismo pode ser dado por:*

$$\sigma : \begin{array}{ccc} \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* & \to & \mathrm{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \\ \overline{k} & \mapsto & \sigma_k \end{array}, \text{ onde } \sigma_k : \begin{array}{ccc} \mathbb{Q}(\zeta_m) & \to & \mathbb{Q}(\zeta_m) \\ \zeta_m & \mapsto & \zeta_m{}^k \end{array}.$$

Se $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ é a fatoração de m em fatores primos, então $\bigcap_{i=1}^{n} \mathbb{Q}(\zeta_{p_i^{\alpha_i}}) = \mathbb{Q}$ (se $n \geq 2$) e $\mathbb{Q}(\zeta_{p_1^{\alpha_1}}, \ldots, \zeta_{p_n^{\alpha_n}}) = \mathbb{Q}(\zeta_m)$. Além disso,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{\alpha_1}})/\mathbb{Q}) \times \cdots \mathrm{Gal}(\mathbb{Q}(\zeta_{p_n^{\alpha_n}})/\mathbb{Q}).$$

Em particular, $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^\times \simeq \left(\frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}}\right)^\times \times \cdots \times \left(\frac{\mathbb{Z}}{p_n^{\alpha_n}\mathbb{Z}}\right)^\times$.

Tanto os corpos quadráticos quanto os corpos ciclotômicos receberão atenção especial até o final deste capítulo.

Definição 1.5.3. *Seja K um corpo de números. Definimos o anel de números $\mathcal{O}_K$ de K como sendo o fecho integral de $\mathbb{Z}$ em K, ou seja, $\mathcal{O}_K = \mathcal{O}_{K/\mathbb{Z}}$.*

Também podemos chamar $\mathcal{O}_K$ de *anel de inteiros* de K. Toda a teoria desenvolvida até agora sobre domínios de Dedekind será agora utilizada para obtermos importantes resultados acerca da estrutura aritmética dos corpos de números. Vamos calcular o anel de números de alguns corpos de números de modo concreto.

Proposição 1.5.4. *Seja m um inteiro livre de quadrados.*

1. *Se $m \equiv 2$ ou $3 \pmod 4$, então $\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\sqrt{m}]$.*
2. *Se $m \equiv 1 \pmod 4$, então $\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \left\{ \frac{a + b\sqrt{m}}{2} : a,\ b \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}$.*

Demonstração: 1. A inclusão $\mathbb{Z}[\sqrt{m}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ segue diretamente do exemplo 1.2.10. Já se $a + b\sqrt{m} \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, com $b \neq 0$, então o polinômio minimal de $a + b\sqrt{m}$ sobre $\mathbb{Q}$ é o polinômio $p(x) = x^2 - 2ax + a^2 - mb^2$ descrito acima. Pelo teorema 1.9.7, $2a \in \mathbb{Z}$ e $a^2 - mb^2 \in \mathbb{Z}$. Logo $4a^2 \in \mathbb{Z}$ e $4a^2 - 4mb^2 \in \mathbb{Z} \Rightarrow 4mb^2 = m(2b)^2 \in \mathbb{Z}$. Como m é livre de quadrados, então $2b \in \mathbb{Z}$. Dessa forma existem $u,\ v \in \mathbb{Z}$ tais que $2a = u$ e $2b = v$. Como $a^2 - mb^2 \in \mathbb{Z}$, então $4a^2 - 4mb^2 \equiv 0 \pmod 4 \Rightarrow u^2 - mv^2 \equiv 0 \pmod 4 \Rightarrow u^2 \equiv mv^2 \pmod 4$.

Se u é ímpar, então $u^2 \equiv 1 \pmod 4 \Rightarrow mv^2 \equiv 1 \pmod 4$. Por hipótese, $m \equiv 3 \pmod 4 \Rightarrow 3v^2 \equiv 1 \pmod 4 \Rightarrow v^2 \equiv 3 \pmod 4$, absurdo. Logo u é par. Isto implica que $a \in \mathbb{Z}$ e que $u^2 \equiv 0 \pmod 4 \Rightarrow mv^2 \equiv 0 \pmod 4$. Se v é ímpar, então $v^2 \equiv 1 \pmod 4 \Rightarrow m \equiv 0 \pmod 4$, absurdo. Logo v é par e $b \in \mathbb{Z}$.

2. Seja $\frac{a+b\sqrt{m}}{2} \in \left\{\frac{a+b\sqrt{m}}{2} : a,\ b \in \mathbb{Z},\ a \equiv b \pmod 2\right\}$. Como $m \equiv 1 (\text{mod } 4)$, então $m = 4n+1$, para algum $n \in \mathbb{Z}$. Como $a \equiv b \pmod 2$, então $a-b = 2k$, para algum $k \in \mathbb{Z}$. Assim $\frac{a+b\sqrt{m}}{2}$ anula $p(x) = x^2 - ax + k^2 + kb - nb^2$, que é um polinômio mônico em $\mathbb{Z}[x]$. Logo $\frac{a+b\sqrt{m}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.

Para a outra inclusão, seja $a+b\sqrt{m} \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, com $b \neq 0$. Procedendo como antes, existem $u,\ v \in \mathbb{Z}$ tais que $2a = u,\ 2b = v$ e $u^2 \equiv mv^2 \pmod 4$. Assim $a+b\sqrt{m} = \frac{u+v\sqrt{m}}{2}$. É necessário então mostrar apenas que $u \equiv v \pmod 2$. Mas como $m \equiv 1 \pmod 4$, então $u^2 \equiv v^2 \pmod 4 \Rightarrow u \equiv v \pmod 2$. □

O objetivo agora é provar que o anel de números de um corpo de números K é um domínio de Dedekind. Para isso precisamos dos seguintes resultados:

Lema 1.5.5. *Seja $\mathfrak{m}$ um ideal não nulo de $\mathcal{O}_K$. Então $\mathfrak{m} \cap \mathbb{Z} \neq \{0\}$.*

Demonstração: Como $\mathfrak{m} \neq \{0\}$, seja $\alpha \in \mathfrak{m} - \{0\}$ satisfazendo seu polinômio minimal $x^r + a_{r-1}x^{r-1} + \cdots + a_0 = 0$, onde $a_0, \ldots, a_{r-1} \in \mathbb{Z}$ e $a_0 \neq 0$. Então $a_0 = -(\alpha^r + \cdots + a_1\alpha)$. O lado esquerdo desta equação está em $\mathbb{Z}$, enquanto que o lado direito desta equação está em $\mathfrak{m}$. Logo $0 \neq a_0 \in \mathfrak{m} \cap \mathbb{Z}$. □

Corolário 1.5.6. *Seja $\mathfrak{m}$ um ideal não nulo de $\mathcal{O}_K$. Então $\#\left(\frac{\mathcal{O}_K}{\mathfrak{m}}\right) < \infty$.*

Demonstração: Pelo lema anterior, existe $m \in \mathfrak{m} \cap \mathbb{Z} - \{0\}$. Então $m\mathcal{O}_K \subseteq \mathfrak{m}$. Como $\#\left(\frac{\mathcal{O}_K}{m\mathcal{O}_K}\right) = m^{[K:\mathbb{Q}]}$, segue que $\#\left(\frac{\mathcal{O}_K}{\mathfrak{m}}\right) \leq m^{[K:\mathbb{Q}]} < \infty$. □

Definição 1.5.7. *Sejam K um corpo de números e $\mathfrak{m}$ um ideal não nulo em $\mathcal{O}_K$. Definimos a norma do ideal $\mathfrak{m}$ como sendo $N(\mathfrak{m}) = \#\left(\frac{\mathcal{O}_K}{\mathfrak{m}}\right)$.*

Lema 1.5.8. *Se $(0) \subsetneq \mathfrak{i} \subsetneq \mathfrak{j}$ são ideais de $\mathcal{O}_K$, então $N(\mathfrak{i}) > N(\mathfrak{j})$.*

Demonstração: Seja $f : \frac{\mathcal{O}_K}{\mathfrak{i}} \to \frac{\mathcal{O}_K}{\mathfrak{j}}$ dada por $f(x+\mathfrak{i}) = x+\mathfrak{j}$. Como $\mathfrak{i} \subsetneq \mathfrak{j}$, então f está bem definida e é sobrejetora.

Agora, como $\mathfrak{i} \subsetneq \mathfrak{j}$, existe $y \in \mathfrak{j} - \mathfrak{i}$. Então $y+\mathfrak{i} \neq 0$ mas $f(y+\mathfrak{i}) = 0 \Rightarrow f$ não é injetora. Como tanto o domínio quanto o contra-domínio de f são finitos, temos o desejado. □

Teorema 1.5.9. *Se K é um corpo de números, então $\mathcal{O}_K$ é um domínio de Dedekind.*

Demonstração: Basta provarmos que $\mathcal{O}_K$ é noetheriano, pois o restante segue da proposição 1.4.4. Para isto, suponha por absurdo que exista uma sequência ascendente de ideais de $\mathcal{O}_K$

$$\mathfrak{i}_1 \subsetneq \mathfrak{i}_2 \subsetneq \mathfrak{i}_3 \subsetneq \cdots$$

que nunca estabiliza. Pelo lema anterior, $N(\mathfrak{i}_1) > N(\mathfrak{i}_2) > N(\mathfrak{i}_3) > \cdots$. Mas $N(\mathfrak{i}_1)$ sendo finito, isto é impossível. Logo $\mathcal{O}_K$ é noetheriano. □

Definição 1.5.10. *Dizemos que $\alpha \in \mathbb{C}$ é um inteiro algébrico se $\alpha \in \mathcal{O}_{\mathbb{C}}$.*

O domínio $\mathcal{O}_{\mathbb{C}/\mathbb{Z}}$ é o contra-exemplo que faltava na seção anterior:

Proposição 1.5.11. *O domínio $\mathcal{O}_{\mathbb{C}/\mathbb{Z}}$ não é noetheriano, mas é integralmente fechado e todo ideal primo não nulo seu é maximal.*

Demonstração: Para ver que $\mathcal{O}_{\mathbb{C}/\mathbb{Z}}$ não é noetheriano, basta considerar a seguinte cadeia ascendente de ideais que nunca estabiliza: $(\sqrt{2}) \subsetneq (\sqrt[4]{2}) \subsetneq (\sqrt[8]{2}) \subsetneq \cdots$. De fato, se existe $n \in \mathbb{N}^*$ tal que $(\sqrt[2^n]{2}) = (\sqrt[2^{n+1}]{2})$, então $\sqrt[2^{n+1}]{2} \in (\sqrt[2^n]{2}) \Rightarrow \exists\, a \in \mathcal{O}_{\mathbb{C}/\mathbb{Z}}$ tal que $\sqrt[2^{n+1}]{2} = \sqrt[2^n]{2}a$. Elevando tal equação a 2^{n+1}, obtemos $2 = 4a^{2^{n+1}} \Rightarrow a^{2^{n+1}} = \dfrac{1}{2}$. Mas como $a \in \mathcal{O}_{\mathbb{C}/\mathbb{Z}}$, então $a^{2^{n+1}} \in \mathcal{O}_{\mathbb{C}/\mathbb{Z}} \Rightarrow \dfrac{1}{2} \in \mathcal{O}_{\mathbb{C}/\mathbb{Z}}$, absurdo. O restante do resultado segue da proposição 1.4.4. □

O restante deste capítulo será dedicado a estudar algumas ferramentas básicas para a demonstrarmos que $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.

1.6 Norma, traço e discriminante

Definição 1.6.1. *Seja L/K uma extensão de corpos de números de grau n. Sejam $\sigma_1, \ldots, \sigma_n$ os n mergulhos de L em $\mathbb{C}$ que fixam K ponto a ponto. Se $\alpha \in L$, definimos o traço e a norma de α por*

$$T_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \qquad\qquad N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

respectivamente.

O traço e a norma têm as seguintes propriedades:

Proposição 1.6.2. *Se L/K uma extensão de corpos de números de grau n, então*

1. $T_{L/K}(\alpha + \beta) = T_{L/K}(\alpha) + T_{L/K}(\beta),\ \forall\ \alpha,\ \beta \in L$;
2. $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta),\ \forall\ \alpha,\ \beta \in L$;
3. $T_{L/K}(\delta) = n\delta,\ \forall\ \delta \in K$;
4. $N_{L/K}(\delta) = \delta^n,\ \forall\ \delta \in K$;
5. $T_{L/K}(\delta\alpha) = \delta T_{L/K}(\alpha),\ \forall\ \delta \in K,\ \forall\ \alpha \in L$; *e,*
6. $N_{L/K}(\delta\alpha) = \delta^n T_{L/K}(\alpha),\ \forall\ \delta \in K,\ \forall\ \alpha \in L$.

Tais propriedades decorrem diretamente da definição e são de fácil verificação. Entretanto, há ainda uma outra fórmula que também permite o cálculo do traço e da norma de um elemento $\alpha \in L$ que será útil mais tarde. Para isto, precisamos da seguinte definição:

Definição 1.6.3. *Sejam α um inteiro algébrico e K um corpo de números. Definimos os conjugados de α sobre K como sendo as raízes do polinômio minimal de α sobre K. Definimos também o grau de α sobre K como sendo o grau de seu polinômio minimal sobre K.*

Teorema 1.6.4. *Seja L/K uma extensão do corpos de números de grau n e suponha que $\alpha \in L$ tenha grau d sobre K. Denote por $\mathrm{t}(\alpha)$ e $\mathrm{n}(\alpha)$ a soma e o produto, respectivamente, dos d conjugados de α sobre K. Então*

$$T_{L/K}(\alpha) = \frac{n}{d}\,\mathrm{t}(\alpha) \qquad e \qquad N_{L/K}(\alpha) = \mathrm{n}(\alpha)^{n/d}.$$

Demonstração: Note inicialmente que $\dfrac{n}{d} \in \mathbb{Z}$, pois $\dfrac{n}{d} = [L : K(\alpha)]$. Além disso, $\mathrm{t}(\alpha) = T_{K(\alpha)/K}(\alpha)$ e $\mathrm{n}(\alpha) = N_{K(\alpha)/K}(\alpha)$. Agora, como cada mergulho de $K(\alpha)$ em $\mathbb{C}$ se extende de $\dfrac{n}{d} = [L : K(\alpha)]$ maneiras a um mergulho de L em $\mathbb{C}$, segue que $T_{L/K}(\alpha) = \dfrac{n}{d}\,\mathrm{t}(\alpha)$ e $N_{L/K}(\alpha) = \mathrm{n}(\alpha)^{n/d}$. □

Corolário 1.6.5. *Com as notações do teorema anterior, $T_{L/K}(\alpha),\ N_{L/K}(\alpha) \in K$. Se $\alpha \in \mathcal{O}_L$, então $T_{L/K}(\alpha),\ N_{L/K}(\alpha) \in \mathcal{O}_K$.*

Demonstração: Para a primieira afirmação, é suficiente mostrar que $\mathrm{t}(\alpha),\ \mathrm{n}(\alpha) \in K$. Para isto, seja $p_{\alpha|K}(x) = x^d + a_1x^{d-1} + \cdots + a_d \in K[x]$ o polinômio minimal de α sobre K. Como $\mathrm{t}(\alpha) = -a_1$ e $\pm\,\mathrm{n}(\alpha) = a_d$, temos provado a primeira afirmação.

Já a segunda afirmação é simples: como $\alpha \in \mathcal{O}_L$, então todos os seus d conjugados também pertencem a $\mathcal{O}_L$. Isto implica $\mathrm{t}(\alpha),\ \mathrm{n}(\alpha) \in \mathcal{O}_L \cap K = \mathcal{O}_K$. Como $\dfrac{n}{d} \in \mathbb{Z}$, segue que $T_{L/K}(\alpha),\ N_{L/K}(\alpha) \in \mathcal{O}_K$. □

Se temos uma torre de corpos de números $M/L/K$ o traço e a norma relacionam-se da seguinte forma:

Teorema 1.6.6. *Se $M/L/K$ é uma torre de corpos de números, então*

1. $T_{L/K}(T_{M/L}(\alpha)) = T_{M/K}(\alpha),\ \forall\ \alpha \in M$;
2. $N_{L/K}(N_{M/L}(\alpha)) = N_{M/K}(\alpha),\ \forall\ \alpha \in M$.

Demonstração: Sejam inicialmente $\sigma_1, \ldots, \sigma_n$ os $n = [L : K]$ mergulhos de L em $\mathbb{C}$ que fixam K ponto a ponto e sejam $\tau_1, \ldots, \tau_m$ os $m = [M : L]$ mergulhos de M em $\mathbb{C}$ que fixam L ponto a ponto. O que faremos será compor os σ_i com os τ_j, mas nós não podemos fazer isto de início, pois precisamos primeiro estender cada um destes mergulhos a automorfismos de algum corpo. Para isto, seja $N \subseteq \mathbb{C}$ uma extensão finita e normal de $\mathbb{Q}$ que contém M. Então todos os σ_i e todos os τ_j podem

agora ser estendidos a automorfismos de N. Fixe uma extensão para cada um destes mergulhos e denote-as também por σ_i e τ_j (não há risco de confusão). Agora, como podemos compor tais automorfismos, obtemos

$$T_{L/K}\left(T_{M/L}(\alpha)\right) = \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \tau_j(\alpha) \right) = \sum_{\substack{1\le i\le n \\ 1\le j\le m}} \sigma_i(\tau_j(\alpha))$$

$$N_{L/K}\left(N_{M/L}(\alpha)\right) = \prod_{i=1}^{n} \sigma_i \left(\prod_{j=1}^{m} \tau_j(\alpha) \right) = \prod_{\substack{1\le i\le n \\ 1\le j\le m}} \sigma_i(\tau_j(\alpha)).$$

Assim, precisamos mostrar que os mn mergulhos $\sigma_i \circ \tau_j$, quando restritos a M, nos dão todos os $mn = [M : L] \cdot [L : K] = [M : K]$ mergulhos de M em $\mathbb{C}$ que fixam K ponto a ponto. Como todos os mergulhos $\sigma_i \circ \tau_j$ claramente fixam K ponto a ponto, é suficiente mostrar que eles são dois a dois distintos quando restritos a M.

Com efeito, suponha que $(\sigma_i \circ \tau_j)|_M = (\sigma_{i'} \circ \tau_{j'})|_M$. Então

$$\begin{aligned}
(\sigma_i \circ \tau_j)|_L &= (\sigma_{i'} \circ \tau_{j'})|_L \\
\Rightarrow \sigma_i \circ (\tau_j|_L) &= \sigma_{i'} \circ (\tau_{j'}|_L) \\
\Rightarrow \sigma_i \circ (\mathrm{id}\,|_L) &= \sigma_{i'} \circ (\mathrm{id}\,|_L) \\
\Rightarrow (\sigma_i \circ \mathrm{id}\,|_N)|_L &= (\sigma_{i'} \circ \mathrm{id}\,|_N)|_L \\
\Rightarrow \sigma_i|_L &= \sigma_{i'}|_L \\
\Rightarrow \sigma_i &= \sigma_{i'} \\
\Rightarrow (\sigma_i \circ \tau_j)|_M &= (\sigma_i \circ \tau_{j'})|_M \\
\Rightarrow \sigma_i \circ (\tau_j|_M) &= \sigma_i \circ (\tau_{j'}|_M) \\
\Rightarrow \tau_j|_M &= \tau_{j'}|_M \\
\Rightarrow \tau_j &= \tau_{j'} \\
\Rightarrow \sigma_i \circ \tau_j &= \sigma_{i'} \circ \tau_{j'},
\end{aligned}$$

como desejávamos. □

Definição 1.6.7. *Seja L/K uma extensão de corpos de números de grau n sejam $\sigma_1, \ldots, \sigma_n$ os n mergulhos de L em $\mathbb{C}$ que fixam K ponto a ponto. Se $\alpha_1, \ldots, \alpha_n \in L$, definimos o discriminante da n-upla $(\alpha_1, \ldots, \alpha_n) \in L^n$ por*

$$\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) = |\sigma_i(\alpha_j)|^2.$$

Denotamos aqui por $[a_{ij}]$ a matriz tendo o elemento a_{ij} na i-ésima linha e na j-ésima coluna, e por $|a_{ij}|$ o seu determinante. Note que o quadrado na definição do discriminante faz com que o mesmo independa da ordem dos σ_i e dos α_j.

O seguinte teorema é uma fórmula muito útil para o discriminante de uma n-upla:

Teorema 1.6.8. *Seja L/K uma extensão de corpos de números. Se $(\alpha_1, \ldots, \alpha_n) \in L^n$, então* $\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) = |T_{L/K}(\alpha_i\alpha_j)|$.

Demonstração: Como $\det(A) = \det(A^T)$, então $|\sigma_i(\alpha_j)| = |\sigma_j(\alpha_i)|$. Assim,

$$\begin{aligned} |T_{L/K}(\alpha_i\alpha_j)| &= |\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)| = |\sigma_j(\alpha_i)||\sigma_i(\alpha_j)| = \\ &= |\sigma_i(\alpha_j)| \cdot |\sigma_i(\alpha_j)| = |\sigma_i(\alpha_j)|^2 = \mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

□

Segue diretamente do corolário 1.6.5 que se L/K é uma extensão de corpos de números e $(\alpha_1, \ldots, \alpha_n) \in L^n$, então $\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) \in K$. Além disso, se os α_i são todos inteiros algébricos, então $\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) \in \mathcal{O}_K$.

O discriminante de uma n-upla de um corpo de números ainda satisfaz a seguinte propriedade:

Teorema 1.6.9. *Seja L/K uma extensão de corpos de números. Se $(\alpha_1, \ldots, \alpha_n) \in L^n$, então $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0 \Leftrightarrow \alpha_1, \ldots, \alpha_n$ são linearmente dependentes sobre K.*

Demonstração: ($\Leftarrow$) Suponha que $\alpha_1, \ldots, \alpha_n$ são linearmente dependentes sobre K. Então existem $a_1, \ldots, a_n \in K$ não todos nulos tais que $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$. Logo as colunas da matriz

$$[\sigma_i(\alpha_j)] = \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \cdots & \cdots & \cdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}$$

são linearmente dependentes. Assim, seu determinante é zero.

Portanto $\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) = |\sigma_i(\alpha_j)|^2 = 0$.

($\Rightarrow$) Suponha agora que $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$. Então as colunas $R_1, \ldots, R_n$ da matriz

$$[T_{L/K}(\alpha_i\alpha_j)] = \begin{bmatrix} T_{L/K}(\alpha_1\alpha_1) & \cdots & T_{L/K}(\alpha_1\alpha_n) \\ \cdots & \cdots & \cdots \\ T_{L/K}(\alpha_n\alpha_1) & \cdots & T_{L/K}(\alpha_n\alpha_n) \end{bmatrix}$$

são linearmente dependentes sobre K. Logo existem $a_1, \ldots, a_n \in K$ não todos nulos tais que $a_1R_1 + \cdots + a_nR_n = \overrightarrow{0}$, ou seja,

$$\begin{bmatrix} 0 \\ \cdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_1T_{L/K}(\alpha_1\alpha_1) + \cdots + a_nT_{L/K}(\alpha_1\alpha_n) \\ \cdots \\ a_1T_{L/K}(\alpha_n\alpha_1) + \cdots + a_nT_{L/K}(\alpha_n\alpha_n) \end{bmatrix}.$$

Seja $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$. Se supormos por absurdo que $\alpha_1, \ldots, \alpha_n$ são linearmente independentes sobre K, então $\alpha \neq 0$. Além disso, se $j \in \{1, \ldots, n\}$, então

$$T_{L/K}(\alpha\alpha_j) = T_{L/K}(a_1\alpha_1\alpha_j + \cdots + a_n\alpha_n\alpha_j) = a_1T_{L/K}(\alpha_1\alpha_j) + \cdots + a_nT_{L/K}(\alpha_n\alpha_j) = 0.$$

Como estamos supondo que $\alpha_1, \ldots, \alpha_n$ são linearmente independentes sobre K, então eles formam uma base de L sobre K. Como $\alpha \neq 0$, então $\{\alpha\alpha_1, \ldots, \alpha\alpha_n\}$

também é base de L sobre K. Mas isto implica que $T_{L/K}(\beta) = 0,\ \forall\ \beta \in L$, já que β será uma combinação linear dos $\alpha\alpha_j$. Em particular, $T_{L/K}(1) = 0$, absurdo. □

Assim, o teorema 1.6.9 nos diz que o discriminante de uma base de uma extensão de corpos de números L/K é não nulo. Vamos registrar abaixo o caso no qual a base consiste de potências de um único elemento. Para isto, precisamos antes de um pequeno lema:

Lema 1.6.10. *Seja $f(x)$ um polinômio mônico e irredutível sobre um corpo de números K e seja $\alpha \in \mathbb{C}$ uma de suas raízes. Então $f'(\alpha) = \prod_{\beta\neq\alpha}(\alpha - \beta)$, onde o produto é calculado sobre todas as raízes $\beta \neq \alpha$ de $f(x)$.*

Demonstração: Como $f(x)$ é irredutível, então $f(x)$ não tem raízes repetidas. Pelo Teorema Fundamental da Álgebra, $f(x) = (x - \alpha)\prod_{\beta\neq\alpha}(x - \beta)$, onde o produto é calculado sobre todas as raízes $\beta \neq \alpha$ de $f(x)$. Se $g(x) = \prod_{\beta\neq\alpha}(x - \beta)$, então $f(x) = (x - \alpha)g(x)$. Diferenciando, obtemos $f'(x) = g(x) + (x - \alpha)g'(x)$. Assim, $f'(\alpha) = g(\alpha) = \prod_{\beta\neq\alpha}(\alpha - \beta)$. □

Teorema 1.6.11. *Sejam K um corpo de números e α um inteiro algébrico de grau n sobre $L = K[\alpha]$. Se $\alpha_1, \ldots, \alpha_n$ denotam os n conjugados de α sobre K, então*

$$\mathrm{disc}_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1\leq r<s\leq n}(\alpha_r - \alpha_s)^2 = \pm N_{L/K}(f'(\alpha)),$$

onde $f(x)$ é o polinômio minimal de α sobre K. O sinal de $+$ vale se, e somente se, $n \equiv 0$ ou 1 (mod 4).

Demonstração: Sejam $\sigma_1, \ldots, \sigma_n$ os n mergulhos de L em $\mathbb{C}$ que fixam K ponto a ponto e suponha sem perda de generalidade que $\sigma_i(\alpha) = \alpha_i,\ \forall\ i \in \{1, \ldots, n\}$.

É conhecido o fato de que se M é uma matriz de Vandermonde sobre um anel comutativo A (isto é, $[a_{i,j}] = [a_i^{j-1}]$), então seu determinante é dado por

$$|a_{i,j}| = \prod_{1\leq r<s\leq n}(a_s - a_r).$$

Assim,

$$\begin{aligned}\mathrm{disc}_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) &= |\sigma_i(\alpha^{j-1})|^2 = |\sigma_i(\alpha)^{j-1}|^2 = |\alpha_i^{j-1}|^2 = \\ &= \left(\prod_{1\leq r<s\leq n}(\alpha_s - \alpha_r)\right)^2 = \prod_{1\leq r<s\leq n}(\alpha_r - \alpha_s)^2.\end{aligned}$$

Vamos agora mostrar a segunda igualdade. Sabemos que

$$\prod_{1\leq r<s\leq n}(\alpha_r - \alpha_s)^2 = \pm\prod_{r\neq s}(\alpha_r - \alpha_s),$$

onde o segundo produto é calculado sobre todos os $n(n-1)$ pares ordenados de índices distintos. Como temos $\frac{n(n-1)}{2}$ trocas de sinal, o sinal de $+$ vale se, e somente se, $\frac{n(n-1)}{2}$ é par. Mas isto acontece se, e somente se, $n \equiv 0$ ou $1 \pmod 4$. Dessa forma, precisamos apenas mostrar que $\prod_{r \neq s}(\alpha_r - \alpha_s) = N_{L/K}(f'(\alpha))$.

Como $f(x) \in K[x]$, então

$$N_{L/K}(f'(\alpha)) = \prod_{r=1}^{n} \sigma_r(f'(\alpha)) = \prod_{r=1}^{n} f'(\sigma_r(\alpha)) = \prod_{r=1}^{n} f'(\alpha_r).$$

Pelo lema anterior, $f'(\alpha_r) = \prod_{s \neq r}(\alpha_r - \alpha_s) \Rightarrow N_{L/K}(f'(\alpha)) = \prod_{r=1}^{n} f'(\alpha) = \prod_{r=1}^{n}\prod_{s \neq r}(\alpha_r - \alpha_s) = \prod_{r \neq s}(\alpha_r - \alpha_s)$. □

Corolário 1.6.12. *Se p é um número primo ímpar, então* $\mathrm{disc}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = \pm p^{p-2}$.

Demonstração: Seja $L = \mathbb{Q}(\zeta_p)$. Pelo teorema anterior, precisamos apenas mostrar que $N_{L/K}(f'(\zeta_p)) = p^{p-2}$, onde $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ é o polinômio minimal de ζ_p sobre $\mathbb{Q}$.

Escrevendo $x^p - 1 = (x-1)f(x)$ e diferenciando, obtemos

$$px^{p-1} = f(x) + (x-1)f'(x).$$

Calculando em $x = \zeta_p$, obtemos $p\zeta_p^{p-1} = f(\zeta_p) + (\zeta_p - 1)f'(\zeta_p)$. Como $f(\zeta_p) = 0$ e $\zeta_p^{p-1} = \frac{1}{\zeta_p}$, então $f'(\zeta_p) = \frac{p}{\zeta_p(\zeta_p - 1)}$. Tomando a norma,

$$N_{L/\mathbb{Q}}(f'(\zeta_p)) = \frac{N_{L/\mathbb{Q}}(p)}{N_{L/\mathbb{Q}}(\zeta_p)N_{L/\mathbb{Q}}(\zeta_p - 1)}.$$

Como $N_{L/\mathbb{Q}}(p) = p^{p-1}$ e $N_{L/\mathbb{Q}}(\zeta_p) = \prod_{i=1}^{p-1} \zeta_p^i = \zeta_p^{\frac{p(p-1)}{2}} = (\zeta_p^p)^{\frac{p-1}{2}} = 1$, precisamos apenas mostrar que $N_{L/\mathbb{Q}}(\zeta_p - 1) = p$. Com efeito, $N_{L/\mathbb{Q}}(\zeta_p - 1) = N_{L/\mathbb{Q}}(-1)N_{L/\mathbb{Q}}(1 - \zeta_p) = (-1)^{p-1}N_{L/\mathbb{Q}}(1 - \zeta_p) = N_{L/\mathbb{Q}}(1 - \zeta_p) = \prod_{i=1}^{p-1}(1 - \zeta_p^i) = f(1) = p$. □

A partir de agora, se α é um inteiro algébrico de grau n sobre $\mathbb{Q}$, escreveremos $\mathrm{disc}(\alpha) = \mathrm{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1})$. Lembre que, neste caso, $\mathrm{disc}(\alpha) \in \mathbb{Z}$. Além disso, o teorema 1.6.11 implica o seguinte

Corolário 1.6.13. *Seja $\alpha \in \mathbb{C}$ um inteiro algébrico. Se β é um de seus conjugados, então* $\mathrm{disc}(\alpha) = \mathrm{disc}(\beta)$.

Demonstração: Como β é um dos conjugados de α, então tanto α quanto β têm os mesmo conjugados $\alpha_1, \ldots, \alpha_n$. Assim, pelo teorema 1.6.11,

$$\mathrm{disc}(\alpha) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = \mathrm{disc}(\beta).$$

□

Para finalizar esta seção, demonstraremos a seguinte proposição, que será útil mais à frente:

Proposição 1.6.14. *Se $m \in \mathbb{N} - \{0\}$, então* $\mathrm{disc}(\zeta_m)$ *divide* $m^{\varphi(m)}$.

Demonstração: Seja $L = \mathbb{Q}(\zeta_m)$ e seja $f(x)$ o polinômio minimal de ζ_m sobre $\mathbb{Q}$. Então existe $g(x) \in \mathbb{Z}[x]$ tal que $x^m - 1 = f(x)g(x)$. Diferenciando e calculando em ζ_m, obtemos $m\zeta_m^{m-1} = f'(\zeta_m)g(\zeta_m) \Rightarrow m = \zeta_m f'(\zeta_m)g(\zeta_m)$. Tomando normas, pelo teorema 1.6.11 obtemos

$$\begin{aligned} N_{L/\mathbb{Q}}(m) &= N_{L/\mathbb{Q}}(f'(\zeta_m))N_{L/\mathbb{Q}}(\zeta_m g(\zeta_m)) \\ &= \pm \mathrm{disc}_{L/\mathbb{Q}}(1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1})N_{L/\mathbb{Q}}(\zeta_m g(\zeta_m)) \\ &= \pm \mathrm{disc}(\zeta_m)N_{L/\mathbb{Q}}(\zeta_m g(\zeta_m)). \end{aligned}$$

Como $N_{L/\mathbb{Q}}(m) = m^{\varphi(m)}$, temos a equação $m^{\varphi(m)} = \pm \mathrm{disc}(\zeta_m)N_{L/\mathbb{Q}}(\zeta_m g(\zeta_m))$. Como $\mathrm{disc}(\zeta_m) \in \mathbb{Z}$, então $N_{L/\mathbb{Q}}(\zeta_m g(\zeta_m)) \in \mathbb{Q}$. Mas como $\zeta_m g(\zeta_m) \in \mathcal{O}_L$, então $N_{L/\mathbb{Q}}(\zeta_m g(\zeta_m)) \in \mathcal{O}_L \cap \mathbb{Q} = \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Logo temos o desejado. □

1.7 Bases integrais

Definição 1.7.1. *Dizemos que um grupo G é abeliano livre de posto n se existe $n \in \mathbb{N}^*$ tal que $G \simeq \mathbb{Z}^n$.*

Claramente, se H é um subgrupo de um grupo abeliano livre de posto n, então H também é um grupo abeliano livre com posto no máximo n. Note também que o posto de um grupo abeliano livre está bem definido, pois os grupos $\mathbb{Z}^n$ são dois a dois não isomorfos.

Nesta seção, usaremos o discriminante para mostrar que se K é um corpo de números sobre $\mathbb{Q}$, então seu anel de inteiros $\mathcal{O}_K$ é um grupo abeliano livre de posto $[K : \mathbb{Q}]$. Começamos com um simples lema:

Lema 1.7.2. *Existe uma base de K sobre $\mathbb{Q}$ consistindo apenas de inteiros algébricos.*

Demonstração: Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de K sobre $\mathbb{Q}$. Pela proposição 1.3.8, para cada α_i existe $m_i \in \mathbb{Z} - \{0\}$ tal que $m_i\alpha_i$ é um inteiro algébrico. Se $m = \prod_{i=1}^{n} m_i \neq 0$, então $\{m\alpha_1, \ldots, m\alpha_n\}$ é uma base de K sobre $\mathbb{Q}$ consistindo apenas de inteiros algébricos. □

Definição 1.7.3. *Fixada uma base de $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}_K$ de K sobre $\mathbb{Q}$, definimos o grupo abeliano livre de posto n gerado por $\{\alpha_1, \ldots, \alpha_n\}$ por*

$$A = \{m_1\alpha_1, \ldots, m_n\alpha_n\} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Note que $A \subseteq \mathcal{O}_K$.

Teorema 1.7.4. *Seja $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}_K$ uma base do corpo de números K sobre $\mathbb{Q}$ e seja $d = \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$. Se $\alpha \in \mathcal{O}_K$, então existem $m_1, \ldots, m_n \in \mathbb{Z}$ tais que $\alpha = \dfrac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$ e $d | m_i^2,\ \forall\ i \in \{1, \ldots, n\}$.*

Demonstração: Note inicialmente que $d \neq 0$ pois $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de K sobre $\mathbb{Q}$, e que $d \in \mathbb{Z}$ já que $\alpha_1, \ldots, \alpha_n$ são inteiros algébricos.

Escreva $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$, onde $x_1, \ldots, x_n \in \mathbb{Q}$. Se $\sigma_1, \ldots, \sigma_n$ são os n mergulhos de K em $\mathbb{C}$ que fixam $\mathbb{Q}$ ponto a ponto, obtemos

$$\begin{cases} \sigma_1(\alpha) &= x_1\sigma_1(\alpha_1) + \cdots + x_n\sigma_1(\alpha_n) \\ & \cdots \\ \sigma_n(\alpha) &= x_1\sigma_n(\alpha_1) + \cdots + x_n\sigma_n(\alpha_n). \end{cases}$$

Resolvendo o sistema linear anterior via regra de Cramer, obtemos $x_j = \dfrac{y_j}{\delta}$, onde $\delta = |\sigma_i(\alpha_j)|$ e y_j é obtido de δ trocando a j-ésima coluna por $\sigma_i(\alpha)$. Como cada $\sigma_i(\alpha_j)$ é um inteiro algébrico, assim como cada $\sigma_i(\alpha)$, então tanto δ quanto os y_j são também inteiros algébricos e $\delta^2 = d$. Segue que $dx_j = \dfrac{dy_j}{\delta} = \delta y_j \Rightarrow dx_j$ é um inteiro algébrico. Como $dx_j \in \mathbb{Q}$, então $dx_j \in \mathbb{Z}$. Seja $m_j = dx_j,\ \forall\ j \in \{1, \ldots, n\}$.

Resta então mostrar que $\dfrac{m_j^2}{d} \in \mathbb{Z}$. Claramente $\dfrac{m_j^2}{d} \in \mathbb{Q}$. Agora, como $\dfrac{m_j^2}{d} = \dfrac{d^2x_j^2}{d} = dx_j^2 = \delta^2x_j^2 = (\delta x_j)^2 = y_j^2$ é também um inteiro algébrico, temos o desejado. □

Assim, $\mathcal{O}_K \subseteq \mathbb{Z}\dfrac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\dfrac{\alpha_n}{d}$. Logo $\mathcal{O}_K$ contém e está contido em grupos abelianos livres de posto n. Isto claramente implica o

Teorema 1.7.5. *Se K é um corpo de números, então $\mathcal{O}_K$ é um grupo abeliano livre de posto $[K : \mathbb{Q}]$.*

Equivalentemente, $\mathcal{O}_K$ tem uma base sobre $\mathbb{Z}$: existem $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$ tais que cada $\alpha \in \mathcal{O}_K$ é representado unicamente como $m_1\beta_1 + \cdots + m_n\beta_n$, onde $m_i \in \mathbb{Z}$.

Definição 1.7.6. *Seja K um corpo de números de grau n sobre $\mathbb{Q}$. Dizemos que $\{\beta_1, \ldots, \beta_n\} \subseteq \mathcal{O}_K$ é uma base integral de $\mathcal{O}_K$ sobre $\mathbb{Z}$ se cada $\alpha \in \mathcal{O}_K$ é representado unicamente como $m_1\beta_1 + \cdots + m_n\beta_n$, onde $m_i \in \mathbb{Z}$.*

Assim, o teorema 1.7.5 afirma que todo anel de números de um corpo de números tem uma base integral sobre $\mathbb{Z}$. Note que se K é um corpo de números tal que $[K : \mathbb{Q}] = n$, então toda base integral $\{\beta_1, \ldots, \beta_n\}$ de $\mathcal{O}_K$ sobre $\mathbb{Z}$ é uma base de K sobre $\mathbb{Q}$. Com efeito, o conjunto $\{\beta_1, \ldots, \beta_n\} \subseteq \mathcal{O}_K \subseteq K$ é linearmente independente sobre $\mathbb{Q}$ (pela unicidade de representação do 0) e possui $[K : \mathbb{Q}] = n$ elementos. Vejamos um exemplo, que segue diretamente da proposição 1.5.4:

Exemplo 1.7.7. *Seja m um inteiro livre de quadrados.*

- *Se $m \equiv 2$ ou 3 $(mod\ 4)$, então uma base para $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é $\{1, \sqrt{m}\}$.*
- *Se $m \equiv 1$ $(mod\ 4)$, então uma base para $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é $\left\{1, \dfrac{1+\sqrt{m}}{2}\right\}$.*

Proposição 1.7.8. *Sejam K um corpo de números e $\{\beta_1, \ldots, \beta_n\}$, $\{\gamma_1, \ldots, \gamma_n\}$ duas bases integrais para $\mathcal{O}_K$. Então $\operatorname{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \operatorname{disc}_{K/\mathbb{Q}}(\gamma_1, \ldots, \gamma_n)$.*

Demonstração: Escrevendo os β_i em termos dos γ_i, obtemos $\begin{pmatrix} \beta_1 \\ \cdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \gamma_1 \\ \cdots \\ \gamma_n \end{pmatrix}$, para alguma matriz $M \in \mathcal{M}_{n\times n}(\mathbb{Z})$.

Se $\sigma_1, \ldots, \sigma_n$ denotam os n merguhos de K em $\mathbb{C}$, aplicando cada σ_j a cada uma das linhas da equação matricial acima, obtemos $[\sigma_j(\beta_i)] = M[\sigma_j(\gamma_i)]$. Tomando os determinantes e elevando ao quadrado, obtemos

$$\operatorname{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = |M|^2 \operatorname{disc}_{K/\mathbb{Q}}(\gamma_1, \ldots, \gamma_n).$$

Como $|M| \in \mathbb{Z}$, então $\operatorname{disc}_{K/\mathbb{Q}}(\gamma_1, \ldots, \gamma_n) | \operatorname{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$. Além disso eles têm o mesmo sinal. Como podemos usar o mesmo argumento escrevendo os γ_i em termos dos β_i, os discriminantes são iguais. □

Definição 1.7.9. *Seja K um corpo de números. Definimos o discriminante de K, denotado por $\operatorname{disc}(K)$, como sendo o discriminante (sobre $\mathbb{Q}$) de qualquer base integral de seu anel de inteiros $\mathcal{O}_K$.*

Vale lembrar que o discriminante de qualquer corpo de números é sempre um número inteiro. Para finalizar esta seção, apresentamos o exemplo abaixo, que é simples e pode ser verificado por qualquer um dos métodos apresentados até agora:

Exemplo 1.7.10. *Seja m um inteiro livre de quadrados.*

- *Se $m \equiv 2$ ou 3 $(mod\ 4)$, então $\operatorname{disc}(\mathbb{Q}(\sqrt{m})) = 4m$.*
- *Se $m \equiv 1$ $(mod\ 4)$, então $\operatorname{disc}(\mathbb{Q}(\sqrt{m})) = m$.*

1.8 O anel de números de $\mathbb{Q}(\zeta_m)$

No ponto em que estamos já conseguimos mostrar que $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$, para $m = p^r$ potência de um primo. Precisamos de mais três resultados, apenas:

Lema 1.8.1. *Seja $m = p^r$ uma potência de um número primo. Então*

$$\prod_{\substack{k=1 \\ \text{mdc}(p,k)=1}}^{m} (1 - \zeta_m^k) = p.$$

Demonstração: Seja $f(x) = \dfrac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}$.

Assim, se $1 \leq k \leq m$ e $\text{mdc}(p, k) = 1$ então ζ_m^k é raiz de f (pois é raiz do polinômio $x^{p^r} - 1$) mas não é raiz de $g(x) = x^{p^{r-1}} - 1$. Portanto

$$f(x) = \prod_{\substack{k=1 \\ \text{mdc}(p,k)=1}}^{m} (x - \zeta_m^k)$$

pois existem exatamente $\varphi(p^r) = (p-1)p^{r-1}$ valores para k. Tomando $x = 1$ obtemos o resultado. □

Lema 1.8.2. *Sejam L/K uma extensão de corpos de números, $\alpha \in \mathcal{O}_L$ e $m \in K$. Sejam $\alpha_1, \ldots, \alpha_n$ os n conjugados de α sobre K. Então $\alpha + m$ também tem n conjugados sobre $\mathbb{Q}$, sendo eles $\alpha_1 + m, \ldots, \alpha_n + m$. Analogamente, $-\alpha$ também tem n conjugados sobre $\mathbb{Q}$, sendo eles $-\alpha_1, \ldots, -\alpha_n$.*

Demonstração: Seja $p(x) \in K[x]$ o polinômio minimal de α sobre K. Então $p(\alpha) = 0$ e $\partial(p) = n$. Afirmo que $q(x) = p(x - m) \in K[x]$ é o polinômio minimal de $\alpha + m$ sobre K. Claramente $q(x)$ é mônico e irredutível. Além disso, $q(\alpha + m) = p(\alpha) = 0$. Logo $q(x)$ é o polinômio minimal de $\alpha + m$ sobre K.

Dessa forma, $\alpha + m$ também tem $\partial(q) = \partial(p) = n$ conjugados sobre K. Se β é um destes conjugados, então $q(\beta) = 0 \Rightarrow p(\beta - m) = 0 \Rightarrow \beta - m$ é um conjugado de α. Logo existe $i \in \{1, \ldots, n\}$ tal que $\beta - m = \alpha_i \Rightarrow \beta = \alpha_i + m$. Como $q(x)$ é irredutível, $q(x)$ não tem raízes repetidas. Logo os n conjugados de $\alpha + m$ sobre K são dois a dois distintos. Isto implica a tese.

Para o caso do $-\alpha$ basta repetir esta prova, tomando $q(x) = p(-x)$. □

Corolário 1.8.3. *Seja $m \in \mathbb{N},\ m \geq 3$. Então* $\text{disc}(1 - \zeta_m) = \text{disc}(\zeta_m)$.

Demonstração: Se $\alpha_1, \ldots, \alpha_n$ são os n conjugados de ζ_m sobre $\mathbb{Q}$, segue do lema anterior que $-\alpha_1, \ldots, -\alpha_n$ são os n conjugados de $-\zeta_m$ sobre $\mathbb{Q}$ e que, portanto, $1-\alpha_1, \ldots, 1-\alpha_n$ são os n conjugados de $1-\zeta_m$ sobre $\mathbb{Q}$. Assim, pelo teorema 1.6.11, $\text{disc}(\zeta_m) = \displaystyle\prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = \prod_{1 \leq r < s \leq n} ((1 - \alpha_r) - (1 - \alpha_s))^2 = \text{disc}(1 - \zeta_m)$. □

Teorema 1.8.4. *Se $m = p^r$ é uma potência de um número primo, então $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.*

Demonstração: Como $\mathbb{Z}[1-\zeta_m] = \mathbb{Z}[\zeta_m]$, mostraremos que $\mathbb{Z}[1-\zeta_m] = \mathcal{O}_{\mathbb{Q}(\zeta_m)}$. Como $1,\ \zeta_m \in \mathcal{O}_{\mathbb{Q}(\zeta_m)}$, então $1-\zeta_m \in \mathcal{O}_{\mathbb{Q}(\zeta_m)} \Rightarrow \mathbb{Z}[1-\zeta_m] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_m)}$. Suponha por absurdo, que $\mathbb{Z}[1-\zeta_m] \subsetneq \mathcal{O}_{\mathbb{Q}(\zeta_m)}$. Então existe $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_m)} - \mathbb{Z}[1-\zeta_m]$.

Como $\{1, \zeta_m, \ldots, \zeta_m^{n-1}\}$ é base de $\mathbb{Q}(\zeta_m)$ sobre $\mathbb{Q}$, onde $n = \varphi(m) = p^r - p^{r-1}$, então $\{1, 1-\zeta_m, \ldots, (1-\zeta_m)^{n-1}\}$ também é base de $\mathbb{Q}(\zeta_m)$ sobre $\mathbb{Q}$. Pelo teorema 1.7.4, existem $m_1, \ldots, m_n \in \mathbb{Z}$ tais que

$$\alpha = \frac{m_1 + m_2(1-\zeta_m) + \cdots + m_n(1-\zeta_m)^{n-1}}{d},$$

onde $d = \mathrm{disc}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(1, 1-\zeta_m, \ldots, (1-\zeta_m)^{n-1}) = \mathrm{disc}(1-\zeta_m) = \mathrm{disc}(\zeta_m)$. Como d divide $m^{\varphi(m)}$ (proposição 1.6.14), então d é uma potência de p.

Como $\alpha \notin \mathbb{Z}[1-\zeta_m]$, então existe $\widetilde{i} \in \{1, \ldots, n\}$ tal que d não divide $m_{\widetilde{i}}$. Seja i o menor índice tal que d não divide m_i e considere

$$\beta = \frac{m_i(1-\zeta_m)^{i-1} + m_{i+1}(1-\zeta_m)^i + \cdots + m_n(1-\zeta_m)^{n-1}}{p^s},$$

onde $d = p^s$ e $p^s \nmid m_i$. Se escrevermos cada $m_j,\ j \in \{i, \ldots, n\}$ da forma $p^{s_j}t_j$, onde $\mathrm{mdc}(p, t_j) = 1$, teremos $s_i < s$ e

$$\beta = \frac{p^{s_i}t_i(1-\zeta_m)^{i-1} + p^{s_{i+1}}t_{i+1}(1-\zeta_m)^i + \cdots + p^{s_n}t_n(1-\zeta_m)^{n-1}}{p^s}.$$

Se $x = \min\{s_i, \ldots, s_n\}$, então

$$\beta p^{s-x-1} = p^{s_i-x-1}t_i(1-\zeta_m)^{i-1} + p^{s_{i+1}-x-1}t_{i+1}(1-\zeta_m)^i + \cdots + p^{s_n-x-1}t_n(1-\zeta_m)^{n-1}.$$

Note que se $j \in \{i, \ldots, n\}$, então $s_j - x - 1 \geq -1$. Logo $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$ contém um elemento da forma

$$\gamma = \frac{t_i(1-\zeta_m)^{i-1} + t_{i+1}(1-\zeta_m)^i + \cdots + t_n(1-\zeta_m)^{n-1}}{p}$$

para algum $i \leq n,\ t_i, t_{i+1}, \ldots, t_n \in \mathbb{Z}$ e $p \nmid t_i$.

Como $\dfrac{1-\zeta_m^k}{1-\zeta_m} \in \mathbb{Z}[\zeta_m],\ \forall\ k \in \mathbb{N}$, o lema 1.8.1 nos fala que

$$\prod_{\substack{k=1 \\ \mathrm{mdc}(p,k)=1}}^{m} \frac{1-\zeta_m^k}{1-\zeta_m} = \frac{\displaystyle\prod_{\substack{k=1 \\ \mathrm{mdc}(p,k)=1}}^{m} (1-\zeta_m^k)}{\displaystyle\prod_{\substack{k=1 \\ \mathrm{mdc}(p,k)=1}}^{m} (1-\zeta_m)} = \frac{p}{(1-\zeta_m)^n} \in \mathbb{Z}[\zeta_m].$$

Como $i \leq n$, então $\frac{p}{(1-\zeta_m)^i} \in \mathbb{Z}[\zeta_m] \Rightarrow \frac{\gamma p}{(1-\zeta_m)^i} \in \mathcal{O}_{\mathbb{Q}(\zeta_m)} \Rightarrow \frac{t_i}{1-\zeta_m} \in \mathcal{O}_{\mathbb{Q}(\zeta_m)}$. Logo existe $y \in \mathcal{O}_{\mathbb{Q}(\zeta_m)}$ tal que $t_i = (1-\zeta_m)y$. Tomando $N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}$ em cada lado desta equação e lembrando que $N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(y) \in \mathbb{Z}$ uma vez que $y \in \mathcal{O}_{\mathbb{Q}(\zeta_m)}$, obtemos $t_i^n = pN_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(y) \Rightarrow p|t_i^n \Rightarrow p|t_i$, absurdo. □

Definição 1.8.5. *Sejam L e M duas extensões de um corpo K. Definimos o compósito de L e M sobre K, denotado por LM, como sendo a menor extensão de K contendo $L \cup M$.*

Para terminar a demonstração de que $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$ para qualquer natural m, precisamos do seguinte lema:

Lema 1.8.6. *Sejam K e L dois corpos de números de graus m e n sobre $\mathbb{Q}$, respectivamente. Se $d = \text{mdc}(\text{disc}(K), \text{disc}(L))$ e $[KL : \mathbb{Q}] = mn$, então $d\mathcal{O}_{KL} \subseteq \mathcal{O}_K\mathcal{O}_L$.*

Demonstração: Sejam $\{\alpha_1, \ldots, \alpha_m\}$ e $\{\beta_1, \ldots, \beta_n\}$ bases integrais de $\mathcal{O}_K$ e $\mathcal{O}_L$ sobre $\mathbb{Z}$, respectivamente. Então $\{\alpha_1, \ldots, \alpha_m\}$ e $\{\beta_1, \ldots, \beta_n\}$ são bases de K e L sobre $\mathbb{Q}$, respectivamente. Como $[KL : \mathbb{Q}] = mn$, $\{\alpha_i\beta_j\}_{1\leq i\leq m, 1\leq j\leq n}$ é uma base de KL sobre $\mathbb{Q}$, assim como é também uma base de $\mathcal{O}_K\mathcal{O}_L$ sobre $\mathbb{Z}$.

Dessa forma, cada $\gamma \in \mathcal{O}_{KL}$ pode ser escrito da forma $\gamma = \sum_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \frac{m_{ij}}{r}\alpha_i\beta_j$, onde r e todos os m_{ij} são inteiros primos entre si. Portanto, $d\gamma = \sum_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \frac{dm_{ij}}{r}\alpha_i\beta_j$, de onde tiramos que é suficiente mostrar que $r|d$.

Iremos primeiro mostrar que $r|\,\text{disc}(K)$. Como $[K : \mathbb{Q}] = m$, sejam $\sigma_1, \ldots, \sigma_m$ os m mergulhos de K em $\mathbb{C}$. Sabemos da teoria básica de Galois que cada mergulho σ_s, $s \in \{1, \ldots, m\}$, se estende a um mergulho (ainda denotado por σ_s, sem risco de confusão) de KL em $\mathbb{C}$ que fixa L ponto a ponto.

Se $x_i = \sum_{j=1}^{n} \frac{m_{ij}}{r}\beta_j$, $\forall\ i \in \{1, \ldots, m\}$, então $\gamma = \sum_{i=1}^{m} x_i\alpha_i$. Logo

$$\begin{cases} \sigma_1(\gamma) &= x_1\sigma_1(\alpha_1) + \cdots + x_m\sigma_1(\alpha_m) \\ & \cdots \\ \sigma_m(\gamma) &= x_1\sigma_m(\alpha_1) + \cdots + x_m\sigma_m(\alpha_m). \end{cases}$$

Resolvendo o sistema linear anterior via regra de Cramer, obtemos $x_i = \frac{y_i}{\delta}$, onde $\delta = |\sigma_s(\alpha_i)|$ e y_i é obtido de δ trocando a i-ésima coluna por $\sigma_s(\gamma)$. Como cada $\sigma_s(\alpha_i)$ é um inteiro algébrico, assim como cada $\sigma_s(\gamma)$, então tanto δ quanto os y_i são também inteiros algébricos e $\delta^2 = \text{disc}(K)$. Segue que $\text{disc}(K)x_i = \frac{\text{disc}(K)y_i}{\delta} = \delta y_i \Rightarrow \text{disc}(K)x_i$ é um inteiro algébrico, $\forall\ i \in \{1, \ldots, m\}$.

Assim, $\text{disc}(K)x_i = \sum_{j=1}^{n} \frac{\text{disc}(K)m_{ij}}{r}\beta_j \in \mathcal{O}_{\mathbb{C}} \cap L = \mathcal{O}_L$, $\forall\ i \in \{1, \ldots, m\}$. Agora, como $\{\beta_1, \ldots, \beta_n\}$ é uma base integral de $\mathcal{O}_L$ sobre $\mathbb{Z}$, os números racionais

$\frac{\text{disc}(K)m_{ij}}{r}$ na realidade são inteiros. Logo $r|\,\text{disc}(K)m_{ij}$. Mas como $\text{mdc}(r, m_{ij}) = 1$, devemos ter $r|\,\text{disc}(K)$. Analogamente mostramos que $r|\,\text{disc}(L) \Rightarrow r|d$, como queríamos. □

Corolário 1.8.7. *Sejam K e L dois corpos de números de graus m e n sobre $\mathbb{Q}$, respectivamente. Se $\text{mdc}(\text{disc}(K), \text{disc}(L)) = 1$ e $[KL : \mathbb{Q}] = mn$, então $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$.*

Demonstração: O teorema anterior nos dá $\mathcal{O}_{KL} \subseteq \mathcal{O}_K\mathcal{O}_L$. Como a outra inclusão é trivial, o corolário está demonstrado. □

Teorema 1.8.8. *Se $m \in \mathbb{N}^*$, então $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.*

Demonstração: Nós já provamos este resultado para o caso no qual m é uma potência de um número primo. O que vamos fazer agora é supor que o teorema vale para dois inteiros positivos m_1 e m_2 primos entre si e mostrar que o mesmo vale para m_1m_2. Assim, o teorema seguirá por indução no número de fatores primos distintos de m.

Dessa forma, sejam m_1 e m_2 são dois inteiros positivos primos entre si e suponha que $\mathcal{O}_{\mathbb{Q}(\zeta_{m_1})} = \mathbb{Z}[\zeta_{m_1}]$ e $\mathcal{O}_{\mathbb{Q}(\zeta_{m_2})} = \mathbb{Z}[\zeta_{m_2}]$.

Como $\text{mdc}(m_1, m_2) = 1$, existem $r,\ s \in \mathbb{Z}$ tais que $sm_1 + rm_2 = 1$. Então $\zeta_{m_1}^r\zeta_{m_2}^s = e^{2\pi ir/m_1}e^{2\pi is/m_2} = e^{2\pi i/m_1m_2} = \zeta_{m_1m_2} \Rightarrow \mathbb{Q}(\zeta_{m_1m_2}) \subseteq \mathbb{Q}(\zeta_{m_1})\mathbb{Q}(\zeta_{m_2})$. Como a outra inclusão é trivial, temos $\mathbb{Q}(\zeta_{m_1m_2}) = \mathbb{Q}(\zeta_{m_1})\mathbb{Q}(\zeta_{m_2})$. Analogamente mostramos que $\mathbb{Z}[\zeta_{m_1m_2}] = \mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}]$. Além disso,

$$\begin{aligned}[\mathbb{Q}(\zeta_{m_1})\mathbb{Q}(\zeta_{m_2})/\mathbb{Q}] &= [\mathbb{Q}(\zeta_{m_1m_2})/\mathbb{Q}] = \varphi(m_1m_2) = \varphi(m_1)\varphi(m_2) = \\ &= [\mathbb{Q}(\zeta_{m_1})/\mathbb{Q}] \cdot [\mathbb{Q}(\zeta_{m_2})/\mathbb{Q}].\end{aligned}$$

Como $\text{disc}(\mathbb{Q}(\zeta_{m_1})) = \text{disc}(\zeta_{m_1})$ e $\text{disc}(\mathbb{Q}(\zeta_{m_2})) = \text{disc}(\zeta_{m_2})$, se $d|\,\text{disc}(\mathbb{Q}(\zeta_{m_1}))$ e $d|\,\text{disc}(\mathbb{Q}(\zeta_{m_2}))$, então $d|\,\text{disc}(\zeta_{m_1})$ e $d|\,\text{disc}(\zeta_{m_2})$. Pela proposição 1.6.14, $d|m_1^{\varphi(m_1)}$ e $d|m_2^{\varphi(m_2)}$. Como $\text{mdc}(m_1, m_2) = 1$, então $d = 1$. Pelo corolário 1.8.7, $\mathcal{O}_{\mathbb{Q}(\zeta_{m_1})\mathbb{Q}(\zeta_{m_2})} = \mathcal{O}_{\mathbb{Q}(\zeta_{m_1})}\mathcal{O}_{\mathbb{Q}(\zeta_{m_2})}$. Finalmente,

$$\mathcal{O}_{\mathbb{Q}(\zeta_{m_1m_2})} = \mathcal{O}_{\mathbb{Q}(\zeta_{m_1})\mathbb{Q}(\zeta_{m_2})} = \mathcal{O}_{\mathbb{Q}(\zeta_{m_1})}\mathcal{O}_{\mathbb{Q}(\zeta_{m_2})} = \mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}] = \mathbb{Z}[\zeta_{m_1m_2}].$$

□

1.9 Apêndice

Esta é uma seção que contempla alguns resultados básicos da Álgebra, que são usados no decorrer do texto. Por isso, não nos delongaremos muito nesta seção.

Lema 1.9.1. *Sejam A um domínio e $K = Frac(A)$. Se B é um subanel de $K[x]$ tal que $K \subseteq B \subseteq K[x]$, então B é um DIP (domínio de ideais principais).*

Demonstração: Seja $\mathfrak{i}$ um ideal de B. Se $\mathfrak{i} = (0)$, o resultado é trivial.

Caso contrário, $\exists\ p(x) \in \mathfrak{i},\ p(x) \neq 0$. Suponha sem perda de generalidade $p(x)$ de grau mínimo e mônico (é aqui que usamos a hipótese de que $B \supseteq K$; o lema é falso se considerarmos $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$). Afirmo então que $\mathfrak{i} = (p(x))$.

De fato, seja $f(x) \in \mathfrak{i}$. Dividindo $f(x)$ por $p(x)$ em $K[x]$, existem polinômios $q(x),\ r(x) \in K[x]$ tais que $f(x) = p(x)q(x) + r(x)$, onde $r(x) = 0$ ou $\partial(r) < \partial(p)$.

Como $f(x),\ p(x) \in \mathfrak{i}$, então $r \in \mathfrak{i}$. Da minimalidade do grau de $p(x)$, $r(x) = 0 \Rightarrow f(x) \in (p(x))$. Como a outra inclusão é trivial, o lema está demonstrado. □

Lema 1.9.2. *Todo ideal próprio* $\mathfrak{i}$ *de um anel noetheriano* A *está contido num ideal maximal.*

Demonstração: Seja S o conjunto de todos os ideais próprios de A que contém $\mathfrak{i}$. Então $S \neq \emptyset$, pois $\mathfrak{i} \in S$. Como A é noetheriano, então S admite um ideal maximal $\mathfrak{i}_{max}$. Então $\mathfrak{i} \subseteq \mathfrak{i}_{max} \subsetneq A$. Pela maximalidade de $\mathfrak{i}_{max},\ \mathfrak{i}_{max}$ é um ideal maximal de A. □

A hipótese de que o anel A seja noetheriano é supérflua. Entretanto, a demonstração sem esta hipótese faz uso do Lema de Zorn.

Lema 1.9.3. *Sejam* A *um anel e* $\mathfrak{i},\ \mathfrak{j}$ *ideais de* A *tais que* $\mathfrak{i} + \mathfrak{j} = A$. *Se* $m,\ n \in \mathbb{N}^*$, *então* $\mathfrak{i}^m + \mathfrak{j}^n = A$.

Demonstração: Como $1 \in \mathfrak{i} + \mathfrak{j}$, então $\exists\ \alpha \in \mathfrak{i},\ \beta \in \mathfrak{j}$ tais que $1 = \alpha + \beta$. Então

$$\begin{aligned} 1 &= (\alpha+\beta)^{m+n} = \sum_{i=0}^{n} \binom{m+n}{i} \alpha^{m+n-i}\beta^i + \sum_{i=n+1}^{m+n} \binom{m+n}{i} \alpha^{m+n-i}\beta^i = \\ &= \alpha^m \sum_{i=0}^{n} \binom{m+n}{i} \alpha^{n-i}\beta^i + \beta^n \sum_{i=n+1}^{m+n} \binom{m+n}{i} \alpha^{m+n-i}\beta^{i-n} \in \mathfrak{i}^m + \mathfrak{j}^n \end{aligned}$$

Logo $\mathfrak{i}^m + \mathfrak{j}^n = A$. □

Lema 1.9.4. *Sejam* A *um anel e* $\mathfrak{i}, \mathfrak{j}_1, \ldots, \mathfrak{j}_n$ *ideais de* A. *Se* $\mathfrak{i} + \mathfrak{j}_i = A,\ \forall\ i \in \{1, \ldots, n\}$, *então* $\mathfrak{i} + \mathfrak{j}_1 \cdot \ldots \cdot \mathfrak{j}_n = A$.

Demonstração: Por indução em n, é suficiente provarmos o resultado para $n = 2$. Suponha então que $\mathfrak{i} + \mathfrak{j}_1 = \mathfrak{i} + \mathfrak{j}_2 = A$.

Como $A = \mathfrak{i} + \mathfrak{j}_1,\ \exists\ i_1 \in \mathfrak{i},\ j_1 \in \mathfrak{j}_1$ tais que $1 = i_1 + j_1$.

Analogamente, $\exists\ i_2 \in \mathfrak{i},\ j_2 \in \mathfrak{j}_2$ tais que $1 = i_2 + j_2$.

Multiplicando tais equações, $1 = \underbrace{i_1 i_2 + i_1 j_2 + i_2 j_1}_{\in \mathfrak{i}} + \underbrace{j_1 j_2}_{\in \mathfrak{j}_1\mathfrak{j}_2} \in \mathfrak{i} + \mathfrak{j}_1\mathfrak{j}_2$. □

Lema 1.9.5. *Seja* A *um anel e* $\mathfrak{i}$ *um ideal maximal de* A. *Se* $\mathfrak{j}$ *é um ideal de* A *tal que* $\mathfrak{j} \nsubseteq \mathfrak{i}$, *então* $\mathfrak{i} + \mathfrak{j} = A$.

Demonstração: Note inicialmente que $\mathfrak{i} \subseteq \mathfrak{i} + \mathfrak{j} \subseteq A$. Como $\mathfrak{i}$ é maximal, então $\mathfrak{i} = \mathfrak{i} + \mathfrak{j}$ ou $\mathfrak{i} + \mathfrak{j} = A$. Suponha por absurdo que $\mathfrak{i} = \mathfrak{i} + \mathfrak{j}$. Como $\mathfrak{j} \nsubseteq \mathfrak{i}$, então $\exists\, x \in \mathfrak{j} - \mathfrak{i}$. Mas $x = 0 + x \in \mathfrak{i} + \mathfrak{j} = \mathfrak{i}$, absurdo. Logo $\mathfrak{i} + \mathfrak{j} = A$. □

Lema 1.9.6. *Seja f um polinômio mônico com coeficientes em $\mathbb{Z}$ e suponha que $f = gh$, onde g e h são polinômios mônicos com coeficientes em $\mathbb{Q}$. Então g e h têm, na verdade, coeficientes em $\mathbb{Z}$.*

Demonstração: Seja m (respectivamente n) o menor inteiro positivo tal que mg (respectivamente nh) tem coeficientes em $\mathbb{Z}$. Como g é mônico, os coeficientes de mg não têm fator comum, o mesmo ocorrendo com nh.

Afirmo então que $m = n = 1$. De fato, se $mn > 1$, seja $p \in \mathbb{Z}$ um primo tal que p divide mn e considere a equação $mnf = (mg)(nh)$. Reduzindo os coeficientes módulo p, obtemos $\overline{0} = \overline{mg} \cdot \overline{nh}$, onde a barra indica que os coeficientes dos referidos polinômios estão reduzidos módulo p. Como $\mathbb{Z}_p[x]$ é um domínio de integridade, então $\overline{mg} = \overline{0}$ ou $\overline{nh} = \overline{0}$. Assim, p divide todos os coeficientes de mg ou de nh, contradição. Logo $m = n = 1 \Rightarrow g,\ h \in \mathbb{Z}[x]$. □

Teorema 1.9.7. *Seja α um inteiro algébrico e seja f o polinômio mônico sobre $\mathbb{Z}$ de menor grau tendo α como raiz. Então f é irredutível sobre $\mathbb{Q}$. Equivalentemente, o polinômio minimal de α sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.*

Demonstração: Suponha por absurdo que f seja redutível sobre $\mathbb{Q}$. Então $f = gh$, onde g e h são polinômios não constantes em $\mathbb{Q}[x]$. Sem perda de generalidade podemos assumir que g e h são mônicos. Segue do lema anterior que $g,\ h \in \mathbb{Z}[x]$. Como α é raiz de f, então α deve ser raiz de g ou de h. Isto é um absurdo, pois contraria o fato de que f é o polinômio mônico sobre $\mathbb{Z}$ de menor grau tendo α como raiz. □

Capítulo 2

O teorema de Scholz-Reichardt

2.1 O problema inverso de Galois

Existe um famoso problema na Álgebra que pergunta se todo grupo finito G é grupo de Galois de alguma extensão galoisiana de $\mathbb{Q}$. Este problema é conhecido como *problema inverso de Galois*, e permanece em aberto até hoje. Entretanto, temos o seguinte resultado parcial:

Teorema 2.1.1 (Shafarevich)**.** *Todo grupo finito e solúvel é grupo de Galois de alguma extensão galoisiana de* $\mathbb{Q}$*.*

O objetivo deste capítulo não é dar uma demonstração do teorema de Shafarevich (que pode ser encontrada em [13], capítulo 9), mas sim mostrar um esboço da prova de um teorema um pouco mais fraco, mas ainda muito significativo na direção da solução do problema inverso de Galois:

Teorema 2.1.2 (Scholz-Reichardt)**.** *Todo l-grupo finito, com l primo ímpar, é grupo de Galois de alguma extensão galoisiana de* $\mathbb{Q}$*.*

Para isto, vamos precisar de alguns preparativos.

2.2 O problema inverso de Galois para grupos abelianos

O primeiro passo para a demonstração do teorema de Scholz-Reichardt é mostrar que o problema inverso de Galois tem solução se G for abeliano. Para isto precisamos do seguinte lema:

Lema 2.2.1. *Se n é um inteiro positivo, então existe um número primo p tal que* $p \equiv 1 \pmod{n}$.

Demonstração: Suponha por absurdo que não exista um primo satisfazendo a condição do enunciado e seja $f_n(x)$ o n-ésimo polinômio ciclotômico. Como $f_n(x)$ é mônico, existe $a \in \mathbb{N}$ tal que $f_n(an) > 1$. Seja $t = an$ e seja p um divisor primo de $f_n(t)$.

Como $f_n(t)$ divide $t^n - 1$, então p divide $t^n - 1 \Rightarrow t^n \equiv 1 \pmod{p}$. Afirmo que n é a ordem de t módulo p. Com efeito, seja r a ordem de t módulo p e suponha por absurdo que $r < n$. Como r divide n, então o polinômio $(x^r - 1)f_n(x)$ divide $x^n - 1$. Isto implica que $\overline{t}$ é raiz dupla de $x^n - \overline{1} \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}[x]$.

Note agora que $p \nmid n$. De fato, se $p|n$, então $p|t$. Como $p|t^n - 1$, então $p = 1$, absurdo, pois p é primo. Isto implica que o mdc do polinômio $x^n - \overline{1}$ com sua derivada $\overline{n}x^{n-1}$ em $\dfrac{\mathbb{Z}}{p\mathbb{Z}}[x]$ é $\overline{1}$, ou seja, que $x^n - \overline{1}$ não tem raízes repetidas em $\dfrac{\mathbb{Z}}{p\mathbb{Z}}[x]$, absurdo. Logo $r = n$.

Segue do Pequeno Teorema de Fermat que $n|p - 1 \Rightarrow p \equiv 1 \pmod{n}$. □

Corolário 2.2.2. *Se n é um inteiro positivo, então existem infinitos primos p tais que $p \equiv 1 \pmod{n}$.*

Demonstração: Basta supor por absurdo que existam finitos primos $p_1, \ldots, p_m$ satisfazendo a condição do enunciado, tomar $t = anp_1 \cdots p_m$ e repetir a prova anterior. □

Com o lema 2.2.1 podemos provar que o problema inverso de Galois tem solução se G for um grupo finito abeliano.

Teorema 2.2.3. *Se G é um grupo finito abeliano, então existe um corpo de números K tal que a extensão $K/\mathbb{Q}$ é galoisiana e $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$.*

Demonstração: Pelo teorema fundamental dos grupos abelianos finitamente gerados, existem $n_1, \ldots, n_k \in \mathbb{N}$ tais que $G \simeq \dfrac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{n_k\mathbb{Z}}$.

Pelo lema anterior, sejam $p_1, \ldots, p_k$ primos distintos tais que $p_i \equiv 1 \pmod{n_i}$, $\forall\, i \in \{1, \ldots, k\}$, e seja $n = p_1 \cdots p_k$. Da teoria básica dos grupos abelianos,

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times} \simeq \left(\frac{\mathbb{Z}}{p_1\mathbb{Z}}\right)^{\times} \times \cdots \times \left(\frac{\mathbb{Z}}{p_k\mathbb{Z}}\right)^{\times} \simeq \frac{\mathbb{Z}}{(p_1 - 1)\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{(p_k - 1)\mathbb{Z}},$$

onde não há risco de confundir as operações de multiplicação e adição.

Como $n_i|p_i - 1$, o grupo $\dfrac{\mathbb{Z}}{(p_i - 1)\mathbb{Z}}$ possui um subgrupo H_i de ordem $\dfrac{p_i - 1}{n_i}$, pois sabemos que vale a recíproca do teorema de Lagrange para grupos abelianos. Em particular, $\dfrac{\dfrac{\mathbb{Z}}{(p_i - 1)\mathbb{Z}}}{H_i} \simeq \dfrac{\mathbb{Z}}{n_i\mathbb{Z}}$. Se $H = H_1 \times \cdots \times H_k$, então

$$\frac{\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}}{H} \simeq \frac{\dfrac{\mathbb{Z}}{(p_1 - 1)\mathbb{Z}}}{H_1} \times \cdots \times \frac{\dfrac{\mathbb{Z}}{(p_k - 1)\mathbb{Z}}}{H_k} \simeq \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}} \simeq G.$$

Se K é o corpo fixo de $\mathbb{Q}(\zeta_n)$ por H, segue do teorema 1.5.2 e da teoria básica de Galois (veja teorema 58 de [16])que a extensão $K/\mathbb{Q}$ é galoisiana e satisfaz

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \frac{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)} \simeq \frac{\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}}{H} \simeq G.$$

□

Para estendermos o teorema anterior até o teorema de Scholz-Reichardt vamos agora estudar mais alguns conceitos sobre corpos de números.

2.3 Ramificação

Iniciamos esta seção com o seguinte lema:

Lema 2.3.1. *Sejam L/K uma extensão de corpos de números e $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$. Então $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$.*

Demonstração: Pelo lema 1.4.5, existe $\gamma \in K - \mathcal{O}_K$ tal que $\gamma\mathfrak{p} \subseteq \mathcal{O}_K$. Assim, $\gamma\mathfrak{p}\mathcal{O}_L \subseteq \mathcal{O}_K\mathcal{O}_L = \mathcal{O}_L$. Se $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, então $1 \in \mathfrak{p}\mathcal{O}_L \Rightarrow \gamma = \gamma \cdot 1 \in \mathcal{O}_L$. Como $\gamma \in K$, então $\gamma \in \mathcal{O}_L \cap K = \mathcal{O}_K$, absurdo. □

Demonstramos tal lema pelo seguinte: sejam L/K uma extensão de corpos de números e $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$. Pelo teorema da fatoração única de ideais em domínios de Dedekind (que exige ideais *próprios* em seu enunciado), o ideal $\mathfrak{p}\mathcal{O}_L$ de $\mathcal{O}_L$ se escreve como um produto $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$, onde $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ são todos ideais primos distintos de $\mathcal{O}_L$ e $e_1, \ldots, e_r$ são todos inteiros positivos.

Definição 2.3.2. *Sejam L/K uma extensão de corpos de números, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e considere $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ a fatoração do ideal $\mathfrak{p}\mathcal{O}_L$ de $\mathcal{O}_L$ como produto de ideais primos de $\mathcal{O}_L$. Definimos o índice de ramificação de $\mathfrak{p}_i$ sobre $\mathfrak{p}$ como sendo $e(\mathfrak{p}_i/\mathfrak{p}) = e_i$. Dizemos que o ideal $\mathfrak{p}$ se ramifica em L/K se algum dos $e_i > 1$. Dizemos ainda que um elemento primo π de $\mathcal{O}_K$ se ramifica em L/K se o ideal primo $\pi\mathcal{O}_K$ de $\mathcal{O}_K$ se ramifica em L/K.*

Apenas um número finito de ideais primos se ramificam em uma extensão de corpos de números ([6], p. 71 - 73). Pelo corolário 1.2.14, o corpo $\frac{\mathcal{O}_K}{\mathfrak{p}}$ é isomorfo a um subcorpo do corpo $\frac{\mathcal{O}_L}{\mathfrak{p}_i}$. Como ambos os corpos são finitos (corolário 1.5.6), $\frac{\mathcal{O}_L}{\mathfrak{p}_i}$ é um espaço vetorial de dimensão finita sobre $\frac{\mathcal{O}_K}{\mathfrak{p}}$, $\forall\, i \in \{1, \ldots, r\}$.

Definição 2.3.3. *Sejam L/K uma extensão de corpos de números, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e considere $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ a fatoração do ideal $\mathfrak{p}\mathcal{O}_L$ de $\mathcal{O}_L$ como produto de ideais primos de $\mathcal{O}_L$. Definimos o grau inercial de $\mathfrak{p}_i$ sobre o ideal $\mathfrak{p}$, denotado por $f(\mathfrak{p}_i/\mathfrak{p})$, como sendo o grau da extensão de corpos $\frac{\mathcal{O}_L}{\mathfrak{p}_i} \Big/ \frac{\mathcal{O}_K}{\mathfrak{p}}$.*

Os índices de ramificação e graus inerciais se relacionam da seguinte forma:

Teorema 2.3.4. *1. Sejam L/K uma extensão de corpos de números de grau n, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e considere $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ a fatoração do ideal $\mathfrak{p}\mathcal{O}_L$ de $\mathcal{O}_L$ como produto de ideais primos de $\mathcal{O}_L$. Então $\sum_{i=1}^{r} e_i f_i = n$. Se L/K for galoisiana, então $e_1 = \cdots = e_r \doteq e$, $f_1 = \cdots = f_r \doteq f$ e, consequentemente, $efr = n$.*

2. Seja $M/L/K$ uma torre de corpos de números e sejam $(0) \neq \mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \mathfrak{p}_3$ três ideais primos tais que $\mathfrak{p}_1 \subseteq \mathcal{O}_K$, $\mathfrak{p}_2 \subseteq \mathcal{O}_L$ e $\mathfrak{p}_3 \subseteq \mathcal{O}_M$. Então

$$e(\mathfrak{p}_3/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_2)e(\mathfrak{p}_2/\mathfrak{p}_1) \qquad e \qquad f(\mathfrak{p}_3/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_2)f(\mathfrak{p}_2/\mathfrak{p}_1).$$

Uma prova deste teorema (que não é dificil, mas é um pouco longa) encontra-se em [6], p. 65 - 71.

Definição 2.3.5. *Sejam L/K uma extensão de corpos de números, $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ e $\mathfrak{q}$ um ideal primo de $\mathcal{O}_L$. Dizemos que $\mathfrak{p}$ está sob $\mathfrak{q}$, ou que $\mathfrak{q}$ está sobre $\mathfrak{p}$, se $\mathfrak{p} \subseteq \mathfrak{q}$.*

Para a definição um pouco mais específica de ramificação (definição 2.3.7), precisamos do seguinte teorema:

Teorema 2.3.6. *Seja L/K uma extensão de corpos de números. Então:*

1. *cada ideal primo não nulo $\mathfrak{q}$ de $\mathcal{O}_L$ está sobre um único ideal primo não nulo de $\mathcal{O}_K$, a saber, $\mathfrak{q} \cap \mathcal{O}_K$.*
2. *cada ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_K$ está sob pelo menos um ideal primo não nulo $\mathfrak{q}$ de $\mathcal{O}_L$.*

Demonstração: 1. Seja $\mathfrak{q}$ um ideal primo não nulo de $\mathcal{O}_L$. Pelo corolário 1.2.14, $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ é um ideal primo de $\mathcal{O}_K$. Como $\mathcal{O}_L$ é um domínio de Dedekind, então $\mathfrak{q}$ é um ideal maximal de $\mathcal{O}_L$. Ainda pelo corolário 1.2.14, $\mathfrak{p}$ é um ideal maximal de $\mathcal{O}_K$. Se $\mathfrak{p} = (0)$, então $\mathcal{O}_K$ é corpo, absurdo. Logo $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ é um ideal primo não nulo de $\mathcal{O}_K$.

Se $\mathfrak{q}$ está sobre dois ideais primos não nulos distintos $\mathfrak{p}_1$ e $\mathfrak{p}_2$ de $\mathcal{O}_K$, então $\mathfrak{q}$ está sobre $\mathfrak{p}_1 + \mathfrak{p}_2$. Como $\mathcal{O}_K$ é domínio de Dedekind, então tanto $\mathfrak{p}_1$ quanto $\mathfrak{p}_2$ são ideais maximais $\Rightarrow \mathfrak{p}_1 + \mathfrak{p}_2 = A$. Logo $1 \in \mathfrak{p}_1 + \mathfrak{p}_2 \subseteq \mathfrak{q} \Rightarrow 1 \in \mathfrak{q}$, absurdo.

2. Seja $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e considere $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ a fatoração do ideal $\mathfrak{p}\mathcal{O}_L$ de $\mathcal{O}_L$ como produto de ideais primos de $\mathcal{O}_L$. Então $\mathfrak{p}\mathcal{O}_L \subseteq \bigcap_{i=1}^{r} \mathfrak{p}_i$. Em particular, $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{p}_1 \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}_1$. Como $\mathfrak{p} \neq (0)$, então $\mathfrak{p}_1 \neq (0)$. □

Definição 2.3.7. *Sejam L/K uma extensão galoisiana de corpos de números de grau n, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$, $p \in \mathbb{Z}$ o (único) número primo tal que $p\mathbb{Z} \subseteq \mathfrak{p}$ (pelo teorema anterior) e considere $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e}$ a fatoração do ideal $\mathfrak{p}\mathcal{O}_L$ de $\mathcal{O}_L$ como produto de ideais primos de $\mathcal{O}_L$. Se f denota o grau inercial de cada $\mathfrak{p}_i$ sobre $\mathfrak{p}$, então*

- *Dizemos que $\mathfrak{p}$ se decompõe totalmente em L/K se $e = 1,\ f = 1$ e $r = n$.*
- *Dizemos que $\mathfrak{p}$ é totalmente ramificado em L/K se $e = n,\ f = 1$ e $r = 1$.*
- *Dizemos que $\mathfrak{p}$ fica inerte em L/K se $e = 1,\ f = n$ e $r = 1$.*
- *Dizemos que $\mathfrak{p}$ se ramifica suavemente em L/K se $e > 1$ e se $\mathrm{mdc}(e, p) = 1$.*

Se π for um elemento primo do domínio $\mathcal{O}_K$, dizemos que π se decompõe totalmente (ou é totalmente ramificado, ou fica inerte, ou se ramifica suavemente) em L/K se o ideal primo $\pi\mathcal{O}_K$ de $\mathcal{O}_K$ se decompõe totalmente (ou é totalmente ramificado, ou fica inerte, ou se ramifica suavemente, respectivamente) em L/K.

Como o compósito de duas extensões galoisianas é uma extensão galoisiana, temos o seguinte resultado, que será usado mais à frente e cuja prova pode ser encontrada em [7], p. 24:

Teorema 2.3.8. *Sejam K, L corpos de números tais que as extensões $K/\mathbb{Q}$ e $L/\mathbb{Q}$ sejam galoisianas, e seja p um número primo. Então p se decompõe totalmente em $KL/\mathbb{Q}$ se, e somente se, p se decompõe totalmente em $K/\mathbb{Q}$ e em $L/\mathbb{Q}$.*

Caso a extensão L/K de corpos de números seja galoisiana, podemos definir outros dois conceitos, que também serão úteis mais à frente:

Definição 2.3.9. *Seja L/K uma extensão galoisiana de corpos de números com grupo de Galois G. Seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ e fixe $\mathfrak{q}$ um ideal primo de $\mathcal{O}_L$ sobre $\mathfrak{p}$. Definimos o grupo de decomposição e o grupo inercial de $\mathfrak{q}$ sobre $\mathfrak{p}$ por, respectivamente:*

$$\begin{aligned} D(\mathfrak{q}/\mathfrak{p}) &= \{\sigma \in G :\ \sigma(\mathfrak{q}) = \mathfrak{q}\} \\ I(\mathfrak{q}/\mathfrak{p}) &= \{\sigma \in G :\ \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}},\ \forall\ \alpha \in \mathcal{O}_L\} \end{aligned}$$

É claro que ambos são subgrupos de $\mathrm{Gal}(L/K)$, satisfazendo $I(\mathfrak{q}/\mathfrak{p}) \subseteq D(\mathfrak{q}/\mathfrak{p})$. Em particular, $K \subseteq L^{D(\mathfrak{q}/\mathfrak{p})} \subseteq L^{I(\mathfrak{q}/\mathfrak{p})} \subseteq L$. Chamamos o corpo $L^{D(\mathfrak{q}/\mathfrak{p})}$ de *corpo de decomposição* de $\mathfrak{q}/\mathfrak{p}$ e o corpo $L^{I(\mathfrak{q}/\mathfrak{p})}$ de *corpo de inércia* de $\mathfrak{q}/\mathfrak{p}$.

Para fechar esta seção, apresentamos o seguinte resultado, cuja prova está em [6], p. 98 - 101.

Proposição 2.3.10. *Sejam L/K uma extensão galoisiana de corpos de números de grau n, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e considere $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i^e$ a fatoração do ideal $\mathfrak{p}\mathcal{O}_L$ de $\mathcal{O}_L$ como produto de ideais primos de $\mathcal{O}_L$ (veja teorema 2.3.4). Se f denota o grau inercial de cada $\mathfrak{p}_i$ sobre $\mathfrak{p}$, então*

1. $[L^{D(\mathfrak{p}_i/\mathfrak{p})} : K] = r$. *Em particular,* $|D(\mathfrak{p}_i/\mathfrak{p})| = ef$.
2. $[L : L^{I(\mathfrak{p}_i/\mathfrak{p})}] = e$. *Em particular,* $|I(\mathfrak{p}_i/\mathfrak{p})| = e$.
3. $[L^{I(\mathfrak{p}_i/\mathfrak{p})} : L^{D(\mathfrak{p}_i/\mathfrak{p})}] = f$.

Veremos agora uma breve introdução às teorias de homologia e de cohomologia de grupos.

2.4 Homologia e cohomologia de grupos

Nesta seção, faremos uma breve explanação dos conceitos de homologia e cohomologia de grupos a serem usados neste capítulo. A maioria dos resultados será apresentada sem demosntração, embora sua prova não seja difícil. Se uma determinada demonstração não for trivial, indicamos uma referência que a contenha.

Definição 2.4.1. *Se G é um grupo e Λ é um anel comutativo com unidade, definimos o anel de grupo de G com coeficientes em Λ como sendo o conjunto formado por todas as combinações lineares formais de elementos de G com coeficientes em Λ, cujos elementos são da forma $\sum_{\sigma \in G} n_\sigma \sigma$, onde $n_\sigma \in \Lambda$.*

Se definirmos a soma e o produto de elementos de $\Lambda[G]$ da maneira natural, $\Lambda[G]$ torna-se um anel com unidade $1e$, que será comutativo caso G o seja.

Exemplo 2.4.2. *Se $G = \dfrac{\mathbb{Z}}{3\mathbb{Z}}$ é o grupo de 3 elementos gerado pelo elemento a, então*

$$\mathbb{C}[G] = \{z_0 + z_1 a + z_2 a^2 : \ z_1, z_2, z_3 \in \mathbb{C}\}.$$

Se $\lambda_1 = z_0 + z_1 a + z_2 a^2$, $\lambda_2 = w_0 + w_1 a + w_2 a^2 \in \mathbb{C}[G]$, então

$$\lambda_1 + \lambda_2 = (z_0 + w_0) + (z_1 + w_1)a + (z_2 + w_2)a^2$$

e

$$\lambda_1 \lambda_2 = (z_0 w_0 + z_1 w_2 + z_2 w_1) + (z_0 w_1 + z_1 w_0 + z_2 w_2)a + (z_0 w_2 + z_1 w_1 + z_2 w_0)a^2.$$

Devemos notar que se G não for abeliano, então devemos preservar a ordem na qual os fatores aparecem na multiplicação.

Daremos mais atenção ao caso onde $\Lambda = \mathbb{Z}$.

Definição 2.4.3. *Definimos o mapa de aumento de $\mathbb{Z}[G]$ como sendo o homomorfismo sobrejetor*

$$\begin{array}{rccc} \epsilon: & \mathbb{Z}[G] & \to & \mathbb{Z} \\ & \displaystyle\sum_{\sigma\in G} n_\sigma \sigma & \mapsto & \displaystyle\sum_{\sigma\in G} n_\sigma \end{array}$$

Se $I = \ker(\epsilon)$, então I é um ideal bilateral de $\mathbb{Z}[G]$, chamado de *ideal de aumento* de $\mathbb{Z}[G]$. Neste caso, a sequência $0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ é exata, e se $\widetilde{A} = \mathbb{Z}[G]$, então $I\widetilde{A} = \{\alpha_1 a_1 + \cdots \alpha_n a_n : \ \alpha_i \in I, \ a_i \in \widetilde{A}\}$ é um submódulo de $\widetilde{A}$.

Lembramos aqui que se G for um grupo, então um G-módulo é um grupo abeliano $(A, +)$, juntamente com uma função

$$\begin{array}{rccc} \rho: & G \times A & \to & A \\ & (g, a) & \mapsto & g \cdot a \end{array}$$

tal que $g \cdot (a + b) = g \cdot a + g \cdot b$.

Definição 2.4.4. *Sejam G um grupo e A um G-módulo à esquerda. Definimos $A^G = \{a \in A : \ \sigma a = a, \ \forall\ \sigma \in G\}$.*

Claramente A^G é um $\mathbb{Z}$-módulo. Além disso, se $\psi : A \to B$ é um homomorfismo entre G-módulos, então para todo $a \in A^G$ temos $\psi(a) \in B^G$, dado que $\psi(\sigma a) = \sigma\psi(a), \ \forall\ a \in A, \ \sigma \in G$.

Proposição 2.4.5. *Existe um $\mathbb{Z}$-isomorfismo entre A^G e $Hom_G(\mathbb{Z}, A)$.*

Demonstração: Basta tomarmos $F : A^G \to \mathrm{Hom}_G(\mathbb{Z}, A)$, que a cada $a \in A^G$ corresponde o homomorfismo $f_a \in \mathrm{Hom}_G(\mathbb{Z}, A)$ tal que $f_a(1) = a$. □

Definição 2.4.6. *Sejam G um grupo e A um G-módulo à esquerda. Se IA é como acima, então definimos $A_G = \dfrac{A}{IA}$.*

Note que vale uma proposição análoga à proposição 2.4.5 para o G-módulo A^G:

Proposição 2.4.7. *Sejam G um grupo e A um G-módulo à esquerda. Se $\overline{a}$ denota a classe de equivalência de a em A_G e $\mathbb{Z} \otimes_G A$ denota o produto tensorial entre G-módulos , então a função*

$$\begin{array}{rccc} F: & \mathbb{Z} \otimes_G A & \to & A_G \\ & n \otimes a & \mapsto & \overline{a} \end{array}$$

é um $\mathbb{Z}$-isomorfismo.

Proposição 2.4.8. *Sejam G e G' dois grupos. Se $\phi : G' \to G$ é um homomorfismo, então ϕ induz um homomorfismo injetor $\phi_1 : A^G \to A^{G'}$ e um homomorfismo sobrejetor $\phi_2 : A_{G'} \to A_G$.*

Entretanto, a prova destas duas proposições não é trivial. Recomendamos [14] para a demonstração. Agora estamos prontos para definir G-módulos projetivos e injetivos:

Definição 2.4.9. *Sejam G um grupo e A, B, C três G-módulos. Dizemos que A é um G-módulo projetivo se toda vez em que tivermos um diagrama*

$$\begin{array}{ccccc} & & A & & \\ & & \downarrow & & \\ B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

no qual a sequência $B \to C \to 0$ é exata e todos os mapas são G-homomorfismos, então existe um G-homomorfismo $A \to B$ tal que o seguinte diagrama comuta:

$$\begin{array}{ccccc} & & A & & \\ & \swarrow & \downarrow & & \\ B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

Definição 2.4.10. *Sejam G um grupo e A, B, C três G-módulos. Dizemos que A é um G-módulo injetivo se toda vez em que tivermos um diagrama*

$$\begin{array}{ccccc} 0 & \longrightarrow & B & \longrightarrow & C \\ & & \downarrow & & \\ & & A & & \end{array}$$

no qual a sequência $0 \to B \to C$ é exata e todos os mapas são G-homomorfismos, então existe um G-homomorfismo $C \to A$ tal que o seguinte diagrama comuta:

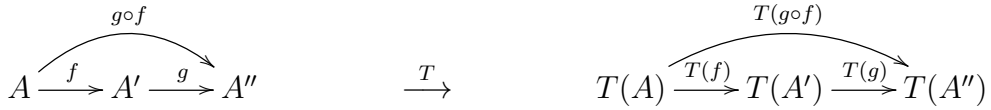
$$\begin{array}{ccccc} 0 & \longrightarrow & B & \longrightarrow & C \\ & & \downarrow & \swarrow & \\ & & A & & \end{array}$$

Outro objeto importante que precisamos definir são as sequências exatas conexas de funtores (tanto à direita quanto à esquerda). Para isto, precisamos explicar o que é um funtor. Vale notar que a definição de funtor pode ser feita num contexto bem mais amplo, mas isto não é necessário no momento.

Definição 2.4.11. *Um funtor é uma função T que*

1. *a cada G-módulo A associa um outro G-módulo $T(A)$; e*
2. *a cada G-homomorfismo entre G-módulos $f : A \to A'$ associa um outro G-homomorfismo entre G-módulos $T(f) : T(A) \to T(A')$ tal que*
   - *$T(\mathrm{id}_A) = \mathrm{id}_{T(A)}$; e*
   - *$T(g \circ f) = T(g) \circ T(f)$, $\forall$ $f : A \to A'$ e $g : A' \to A''$ G-homomorfismos entre G-módulos.*

Note então que um funtor preserva a composição de G-homomorfismos, assim como preserva o G-homomorfismo identidade.



Definição 2.4.12. *Seja $0 \to A' \to A \to A'' \to 0$ uma sequência exata de G-módulos, e seja $\{T^n\}_{n\geq 0}$ uma sequência de funtores. Dizemos que a sequência $\{T^n\}_{n\geq 0}$ é uma sequência exata conexa à direita se a sequência*

$$T^0(A') \to T^0(A) \to T^0(A'') \to T^1(A') \to \cdots \to T^n(A') \to T^n(A) \to T^n(A'') \to \cdots$$

for exata.

Definição 2.4.13. *Seja $0 \to A' \to A \to A'' \to 0$ uma sequência exata de G-módulos, e seja $\{T^n\}_{n\geq 0}$ uma sequência de funtores. Dizemos que a sequência $\{T^n\}_{n\geq 0}$ é uma sequência exata conexa à esquerda se a sequência*

$$\cdots \to T^n(A') \to T^n(A) \to T^n(A'') \to T^{n-1}(A') \to \cdots \to T^0(A') \to T^0(A) \to T^0(A'')$$

for exata.

Finalmente conseguimos definir as teorias de homologia e cohomologia de grupos:

Definição 2.4.14. *Seja G um grupo e A um G-módulo à esquerda. Definimos uma teoria de homologia para G como sendo uma sequência exata conexa à esquerda $\{H_n(G, A)\}_{n\geq 0}$ de funtores tal que:*

- $H_0(G, A) = A_G$
- *Se A é G-módulo projetivo, então $H_p(G, A) = 0$ sempre que $p > 0$.*

Dessa forma, se tivermos uma sequência exata $0 \to A' \to A \to A'' \to 0$ de G-módulos, a sequência

$$\begin{aligned}\cdots \to H_n(G, A') \to H_n(G, A) \to H_n(G, A'') \to H_{n-1}(G, A') \to \cdots \\ \cdots \to H_1(G, A'') \to H_0(G, A') \to H_0(G, A) \to H_0(G, A'')\end{aligned}$$

também será uma sequência exata de G-módulos. Caso tivermos um homomorfismo de grupos $\phi : G' \to G$, se colocarmos $\sigma' a = \phi(\sigma')a,\ \forall\ \sigma' \in G,\ a \in A$, o G-módulo A pode ser olhado como um G'-módulo. Assim, se pudermos definir uma teoria de homologia para G', então os grupos $H_n(G, A)$ formarão uma sequência exata conexa à esquerda.

A demonstração do seguinte teorema, conhecido como *teorema de unicidade das teorias de homologia*, pode ser encontrada em [14]:

Teorema 2.4.15. *Seja $\phi : G' \to G$ um homomorfismo de grupos e sejam $H_n(G', A)$, $H_n(G, A)$ teorias de homologia para G' e para G, respectivamente. Então existe um único homomorfismo da sequência conexa*

$$H_2(G', A),\ H_1(G', A),\ H_0(G', A)$$

na sequência conexa

$$H_2(G, A),\ H_1(G, A),\ H_0(G, A)$$

estendendo o homomorfismo sobrejetor $\phi_2 : A_{G'} \to A_G$ da proposição 2.4.8.

Corolário 2.4.16. *Se $\phi : G' \to G$ for um isomorfismo de grupos, então o isomorfismo $\phi_2 : A_{G'} \to A_G$ se estende de modo único a um isomorfismo das teorias de homologia para G e de G'. Em particular, se $\phi : G \to G$ for a identidade, duas torias de homologia quaisquer para G são sempre isomorfas com respeito ao isomorfismo $\phi_2 : A_G \to A_G$.*

Os dois últimos resultados nos permitem mostrar a existência de uma teoria de homologia para G em termos do conhecido funtor Tor:

Teorema 2.4.17. *Seja G um grupo. Então podemos obter uma teoria de homologia para G, definindo, para cada G-módulo à esquerda A,*

$$H_n(G, A) = \mathrm{Tor}_n^G(\mathbb{Z}, A),\ \forall\ n \geq 0.$$

Caso A seja um G-módulo à direita, podemos obter uma teoria de homologia para G, definindo

$$H_n(G, A) = \mathrm{Tor}_n^G(A, \mathbb{Z}),\ \forall\ n \geq 0.$$

Note que, em particular, $H_0(G, A) = \mathrm{Tor}_0^G(\mathbb{Z}, A) = \mathbb{Z} \otimes_G A \simeq A_G$, pela proposição 2.4.7.

Definição 2.4.18. *Seja G um grupo e A um G-módulo à esquerda. Definimos uma teoria de cohomologia para G como sendo uma sequência exata conexa à direita $\{H^n(G, A)\}_{n\geq 0}$ de funtores tal que:*

- $H^0(G, A) = A^G$
- *Se A é G-módulo injetivo, então $H^p(G, A) = 0$ sempre que $p > 0$.*

Da mesma forma que as teorias de homologia para grupos, as teorias de cohomologia para grupos também têm seu teorema de unicidade (e seu respectivo corolário), cujo enunciado é análogo. Sendo assim, podemos exibir uma teoria de cohomologia para um grupo G em termos do funtor Ext:

Teorema 2.4.19. *Seja G um grupo. Então podemos obter uma teoria de cohomologia para G, definindo, para cada G-módulo à esquerda A,*

$$H^n(G, A) = \mathrm{Ext}_n^G(\mathbb{Z}, A),\ \forall\ n \geq 0.$$

Note que, em particular, $H^0(G, A) = \mathrm{Ext}_0^G(\mathbb{Z}, A) = \mathrm{Hom}_G(\mathbb{Z}, A) \simeq A^G$, pela proposição 2.4.7.

2.5 O problema de extensão de grupos

Definição 2.5.1. *Sejam A um grupo abeliano e G um grupo qualquer. Uma extensão de G por A é um par $(\widetilde{G}, \psi)$ tal que $\psi : \widetilde{G} \to G$ é um homomorfismo sobrejetor de grupos satisfazendo* $\ker(\psi) = A$. *A extensão $(\widetilde{G}, \psi)$ de G por A é chamada central se A for subgrupo do centro de $\widetilde{G}$.*

Duas extensões são ditas equivalentes se existe um isomorfismo $\rho : \widetilde{G}_1 \to \widetilde{G}_2$ tal que o seguinte diagrama comuta:

$$\begin{array}{ccccc} A & \hookrightarrow & \widetilde{G}_1 & \xrightarrow{\psi_1} & G \\ \| & & \downarrow \rho & & \| \\ A & \hookrightarrow & \widetilde{G}_2 & \xrightarrow{\psi_2} & G \end{array}$$

Em outras palavras, uma extensão de G por A é um par $(\widetilde{G}, \psi)$ tal que a sequência $1 \to A \to \widetilde{G} \xrightarrow{\psi} G \to 1$ de homomorfismos de grupos é exata e satisfaz $\ker(\psi) = A$. Em particular, $\dfrac{\widetilde{G}}{A} \simeq G$. Assim, o *problema de extensão de grupos* é descobrir quais (e quantas são) as extensões não equivalentes de G por A.

Lema 2.5.2. *Sejam A um grupo abeliano, G um grupo qualquer e $(\widetilde{G}, \psi)$ uma extensão de G por A. Então A tem uma estrutura de G-módulo a esquerda.*

Demonstração: Precisamos achar uma função $G \times A \to A,\ (\sigma, a) \mapsto a^\sigma$ tal que

1. $a^{\sigma\cdot\tau} = (a^\tau)^\sigma,\ \forall\ a \in A,\ \sigma, \tau \in G$;
2. $a^1 = a,\ \forall\ a \in A$; e,
3. $(a + b)^\sigma = a^\sigma + b^\sigma,\ \forall\ a, b \in A,\ \sigma \in G$.

Para isto, seja inicialmente $\sigma \in G$. Como ψ é sobrejetora, existe $\eta_\sigma \in \widetilde{G}$ tal que $\psi(\eta_\sigma) = \sigma$. Como $A \lhd \widetilde{G}$, então a função $a \mapsto \eta_\sigma a \eta_\sigma^{-1}$ é um automorfismo de A. Além disso, se η'_σ é um outro elemento de $\widetilde{G}$ tal que $\psi(\eta'_\sigma) = \sigma$, então existe $\alpha \in A$ tal que $\eta'_\sigma = \alpha\eta_\sigma$, pois $A = \ker(\psi)$. Assim,

$$\eta'_\sigma a \eta'^{-1}_\sigma = \alpha\eta_\sigma a \eta_\sigma^{-1}\alpha^{-1} = \eta_\sigma a \eta_\sigma^{-1}$$

pois A é abeliano e $\eta_\sigma a \eta_\sigma^{-1} \in A$ por normalidade. Assim, a função

$$(\sigma, a) \mapsto a^\sigma = \eta_\sigma a \eta_\sigma^{-1}$$

está bem definida e dá a A uma estrutura de G-módulo, pois satisfaz os três itens acima. □

O lema 2.5.2 é um passo essencial na prova do seguinte teorema (que pode ser encontrada em [7], p. 9 - 13), e permite-nos contar o numero de extensões não equivalentes de G por A:

Teorema 2.5.3. *Sejam A um grupo abeliano e G um grupo qualquer. Suponha que A tenha a estrutura de G-módulo descrita no lema 2.5.2. Então a cada extensão de G por A existe associado a ela um elemento de $H^2(G, A)$. Além disso, esta associação é uma bijeção entre as classes de extensões equivalentes e os elementos de $H^2(G, A)$. Mais ainda, uma extensão de grupos é trivial (isto é, $\widetilde{G} \simeq G \times A$) se, e somente se, a extensão correponde ao elemento neutro de $H^2(G, A)$.*

2.6 O teorema de Scholz-Reichardt

Definição 2.6.1. *Seja G um grupo finito. Definimos o expoente de G como sendo o mínimo múltiplo comum das ordens dos elementos de G.*

Claramente o expoente de um grupo finito G divide a ordem de G.

Inicialmente, seja L um corpo de números tal que a extensão $L/\mathbb{Q}$ seja galoisiana e tenha grupo de Galois G, onde G é um l-grupo, com l primo ímpar. Seja N um inteiro positivo tal que l^N é um múltiplo do expoente de G.

Definição 2.6.2. *Seja L um corpo de números. Dizemos que a extensão $L/\mathbb{Q}$ satisfaz a condição de Scholz para N (ou que satisfaz (S_N)), se cada número primo p que se ramifica em $L/\mathbb{Q}$ satisfaz:*

1. $p \equiv 1 \pmod{l^N}$
2. *Se $\mathfrak{q}$ é um ideal primo de $\mathcal{O}_L$ que contém p, então $I(\mathfrak{q}/p\mathbb{Z}) = D(\mathfrak{q}/p\mathbb{Z})$.*

Descreveremos agora um esquema da prova do teorema de Scholz-Reichardt com as ferramentas que temos em mãos.

Seja G um l-grupo, com l um primo ímpar. Então $|G| = l^s$, para algum inteiro positivo s. O que faremos será contruir, por indução em s, uma torre de corpos de números $\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$ tal que a extensão $L_s/\mathbb{Q}$ é galoisiana, L_s satisfaz a condição (S_N) (para algum inteiro positivo N), $\mathrm{Gal}(L_s/\mathbb{Q}) \simeq G$ e L_s ramifica no máximo um ideal primo de $\mathcal{O}_{L_{s-1}}$ a mais que o número de ideais primos que se ramificam em L_{s-1}.

O caso $s = 1$ é decorre do seguinte teorema, cuja prova pode ser encontrada em [4]:

Teorema 2.6.3. *Sejam $m \in \mathbb{N} - \{0\}$ e p um número primo. Se p for ímpar, p se ramifica na extensão $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ se, e somente se, $p|m$. Se $p = 2$, p se ramifica na extensão $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ se, e somente se, $4|m$.*

Corolário 2.6.4. *Se l for um primo ímpar e $G \simeq \dfrac{\mathbb{Z}}{l\mathbb{Z}}$, então existe um corpo de números L_1 tal que a extensão $L_1/\mathbb{Q}$ é galoisiana, L_1 satisfaz a condição (S_N) (para todo inteiro positivo N), $\mathrm{Gal}(L_1/\mathbb{Q}) \simeq G$ e L_1 ramifica um único número primo $p \in \mathbb{Z}$.*

Demonstração: Seja N um inteiro positivo. O lema 2.2.1 garante a existência de um número primo $p \in \mathbb{Z}$ tal que $p \equiv 1 \pmod{l^N}$. Em particular, $p \equiv 1 \pmod{l}$. Procedendo como na prova do teorema 2.2.3, existe um corpo de números L_1 tal que $\mathbb{Q} \subseteq L_1 \subseteq \mathbb{Q}(\zeta_p)$, $\mathrm{Gal}(L_1/\mathbb{Q}) \simeq G$ e a extensão $L_1/\mathbb{Q}$ e galoisiana. Resta mostrar que L_1 satisfaz a condição (S_N) e que L_1 ramifica um único número primo $p \in \mathbb{Z}$.

Se q é um número primo que se ramifica em $L_1/\mathbb{Q}$, então q se ramifica em $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Pelo teorema anterior, $q = p$. Assim, o único primo que se ramifica em $L_1/\mathbb{Q}$ é o primo p, que já satisfaz a condição 1 de (S_N). Agora, seja $\mathfrak{q}$ um ideal primo de $\mathcal{O}_{L_1}$ que contém p.

Como a extensão $L_1/\mathbb{Q}$ é galoisiana, o teorema 2.3.4 nos diz que $efr = l$. Como l é primo e $e > 1$, então a única opção que temos é $e = l$ e $f = r = 1$. Portanto $|I(\mathfrak{q}/p\mathbb{Z})| = |D(\mathfrak{q}/p\mathbb{Z})|$. Como $I(\mathfrak{q}/p\mathbb{Z}) \subseteq D(\mathfrak{q}/p\mathbb{Z})$, então $I(\mathfrak{q}/p\mathbb{Z}) = D(\mathfrak{q}/p\mathbb{Z})$. □

Seja agora $\widetilde{G}$ um l-grupo de ordem l^{s+1}. Como o centro de todo l-grupo é não trivial, considere a sequência exata central

$$1 \to \frac{\mathbb{Z}}{l\mathbb{Z}} \to \widetilde{G} \to G \to 1.$$

Note então que $\widetilde{G}$ é a extensão de G por $\dfrac{\mathbb{Z}}{l\mathbb{Z}}$. Como $|G| = l^s$, por hipótese de indução existe um corpo de números L_s tal que a extensão $L_s/\mathbb{Q}$ é galoisiana, $\mathrm{Gal}(L_s/\mathbb{Q}) \simeq G$ e $L_s/\mathbb{Q}$ ramifica no máximo um ideal primo de $\mathcal{O}_{L_{s-1}}$ a mais que o número de ideais primos que se ramificam em $L_{s-1}/\mathbb{Q}$. O que faremos será encontrar uma extensão galoisiana L_{s+1} de $\mathbb{Q}$ contendo L_s tal que $\mathrm{Gal}(L_{s+1}/L) \simeq \dfrac{\mathbb{Z}}{l\mathbb{Z}}$, $\mathrm{Gal}(L_{s+1}/\mathbb{Q}) \simeq \widetilde{G}$ e $L_{s+1}/\mathbb{Q}$ ramifica no máximo um ideal primo de $\mathcal{O}_{L_s}$ a mais que o número de ideais primos que se ramificam em $L_{s-1}/\mathbb{Q}$.

Dividiremos agora a demonstração em dois casos: o caso onde $\widetilde{G} \simeq G \times \dfrac{\mathbb{Z}}{l\mathbb{Z}}$ e o caso onde $\widetilde{G} \not\simeq G \times \dfrac{\mathbb{Z}}{l\mathbb{Z}}$. O fato da extensão ter de satisfazer a condição (S_N) será usada apenas no caso em que $\widetilde{G} \not\simeq G \times \dfrac{\mathbb{Z}}{l\mathbb{Z}}$.

2.6.1 O caso $\widetilde{G} \simeq G \times \dfrac{\mathbb{Z}}{l\mathbb{Z}}$

Sejam $p_1, \ldots, p_m$ os primos que se ramificam em $L_s = L$, onde $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$. As proposições 3.41 - 3.46 de [7] mostram a existência de um número primo q tal que:

- $q \equiv 1 \pmod{l^N}$;
- q se decompõe totalmente em $L/\mathbb{Q}$; e,
- Cada primo p_i, $i \in \{1, \ldots, m\}$, é uma potência l-ésima no corpo $\dfrac{\mathbb{Z}}{q\mathbb{Z}}$.

A ideia básica por trás desta parte demonstração é a seguinte: inicialmente mostra-se que dado corpo de números K, então existem infinitos números primos $q \in \mathbb{Z}$ tal que q se decompõe totalmente em K. Em seguida, escolhemos um destes primos que se decompõe totalmente no corpo de números $L(\zeta_{l^N}, \sqrt[l]{p_1}, \ldots, \sqrt[l]{p_m})$ e mostramos que ele cumpre as condições anteriores.

Dessa forma, seja $\lambda' : \left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^{\times} \to \frac{\mathbb{Z}}{l\mathbb{Z}}$ um homomorfismo sobrejetivo de grupos, que existe pois $q \equiv 1 \pmod{l}$. Compondo λ' com o isomorfismo canônico $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq \left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^{\times}$, obtemos um homomorfismo sobrejetor

$$\lambda : \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \to \frac{\mathbb{Z}}{l\mathbb{Z}}.$$

Seja então $H = \ker(\lambda)$. Da teoria básica de Galois, o corpo $M = \mathbb{Q}(\zeta_q)^H$ é tal que $\mathrm{Gal}(M/\mathbb{Q}) \simeq \frac{\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta_q)/M)} = \frac{\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})}{H} \simeq \frac{\mathbb{Z}}{l\mathbb{Z}}$. Agora, como $\mathbb{Q} \subseteq M \subseteq \mathbb{Q}(\zeta_q)$, o único primo que se ramifica em $M/\mathbb{Q}$ é o primo q. Como q se decompõe totalmente em $L/\mathbb{Q}$, então q não se ramifica em $L/\mathbb{Q}$, o que implica $L \cap M = \mathbb{Q}$. De novo pela teoria básica de Galois, o compósito $L_{s+1} = ML$ é uma extensão galoisiana de $\mathbb{Q}$ com grupo de Galois $G \times \frac{\mathbb{Z}}{l\mathbb{Z}} \simeq \widetilde{G}$. Já a prova de que L_{s+1} satisfaz a condição S_N, para algum inteiro positivo N pode ser encontrada em [7], p. 26 - 29.

2.6.2 O caso $\widetilde{G} \not\simeq G \times \frac{\mathbb{Z}}{l\mathbb{Z}}$

Neste caso, $\widetilde{G}$ ainda é uma extensão de G por $\frac{\mathbb{Z}}{l\mathbb{Z}}$. Sejam $\mathbb{A}$ o corpo dos números algébricos, $L = L_s$ e denote por $G_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{A}/\mathbb{Q})$. Claramente L_s induz um homomorfismo sobrejetor

$$\begin{array}{rccc} \mathrm{res}_L : & G_{\mathbb{Q}} & \to & G \\ & \sigma & \mapsto & \sigma|_L \end{array}.$$

Note que $N = \ker(\mathrm{res}_L) = \mathrm{Gal}(\mathbb{A}/L)$. Suponha que consigamos levantar res_L a um homomorfismo sobrejetor $\widetilde{\phi} : G_{\mathbb{Q}} \to \widetilde{G}$, obtendo assim o seguinte diagrama comutativo:

$$\begin{array}{ccccccccc} & & & & G_{\mathbb{Q}} & & & & \\ & & & \overset{\widetilde{\phi}}{\swarrow} & \downarrow{\scriptstyle \mathrm{res}_L} & & & & \\ 1 & \longrightarrow & \frac{\mathbb{Z}}{l\mathbb{Z}} & \longrightarrow & \widetilde{G} & \xrightarrow{\psi} & G & \longrightarrow & 1 \end{array}$$

Se $H = \ker(\widetilde{\phi})$, então $H \subseteq N \subseteq G_{\mathbb{Q}}$. Pelo primeiro teorema do isomorfismo, $\frac{G_{\mathbb{Q}}}{H} \simeq \widetilde{G}$. Se $\widetilde{L}$ for o corpo fixo por H em $\mathbb{A}$, então pela teoria básica de

Galois teremos $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \simeq \dfrac{\mathrm{Gal}(\mathbb{A}/\mathbb{Q})}{\mathrm{Gal}(\mathbb{A}/\widetilde{L})} = \dfrac{\mathrm{Gal}(\mathbb{A}/\mathbb{Q})}{\mathrm{Gal}(\mathbb{A}/\mathbb{A}^H)} = \dfrac{G_{\mathbb{Q}}}{H} \simeq \widetilde{G}$, o que finaliza a demonstração.

É aqui que entram as teorias de homologia e cohomologia. Sabemos, pelo teorema 2.5.3, que existe uma bijeção entre as extensões $\widetilde{G}$ de G por $\dfrac{\mathbb{Z}}{l\mathbb{Z}}$ e os elementos de $H^2\left(G, \dfrac{\mathbb{Z}}{l\mathbb{Z}}\right)$. Seja $\xi \in H^2\left(G, \dfrac{\mathbb{Z}}{l\mathbb{Z}}\right)$ o elemento correspondente à extensão $\widetilde{G}$. Pelo teorema de unicidade das teorias de cohomologia, ϕ induz um homomorfismo $\phi^* : H^2\left(G, \dfrac{\mathbb{Z}}{l\mathbb{Z}}\right) \to H^2\left(G_{\mathbb{Q}}, \dfrac{\mathbb{Z}}{l\mathbb{Z}}\right)$. Neste passo nos restringiremos a mostrar que o fato de $\phi^*(\xi) = 0$ implica a existência do levantamento $\widetilde{\phi}$. Para isto, precisamos antes da definição de produto fibrado sobre grupos.

Definição 2.6.5. *Sejam G um grupo e $i : X \to G,\ j : Y \to G$ dois homomorfismos sobrejetores de grupos. Um produto fibrado de X por Y sobre G é um grupo $X \times_G Y$, junto com dois homomorfismo (denominados "projeções") $p_1 : X \times_G Y \to X$ e $p_2 : X \times_G Y \to Y$, tais que, para cada grupo Z juntamente com homomorfismos $q_1 : Z \to X$ e $q_2 : Z \to Y$ tais que $i \circ q_1 = j \circ q_2$, existe um único homomorfismo $\rho : Z \to X \times_G Y$ tal que o seguinte diagrama comuta:*

$$\begin{array}{ccccc}
Z & \xrightarrow{q_1} & X & \xrightarrow{i} & G \\
\| & & \uparrow{\scriptstyle p_1} & & \\
Z & \xrightarrow{\rho} & X \times_G Y & & \\
\| & & \downarrow{\scriptstyle p_2} & & \\
Z & \xrightarrow{q_2} & Y & \xrightarrow{j} & G
\end{array}$$

É fácil ver que o conjunto

$$X \times_G Y = \{(x, y) \in X \times Y :\ i(x) = j(y)\},$$

junto com as projeções canônicas

$$p_1 : \begin{array}{ccc} X \times_G Y & \to & X \\ (x, y) & \mapsto & x \end{array} \qquad \text{e} \qquad p_2 : \begin{array}{ccc} X \times_G Y & \to & Y \\ (x, y) & \mapsto & y \end{array}$$

é um produto fibrado de X por Y sobre G, munido das operações respectivas coordenada a coordenada. Este produto fibrado, chamado de *produto subdireto de X e Y por G*, é usado logo abaixo. Considere o seguinte diagrama comutativo:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \dfrac{\mathbb{Z}}{l\mathbb{Z}} & \longrightarrow & \widetilde{G} \times_G G_{\mathbb{Q}} & \xrightarrow{p_2} & G_{\mathbb{Q}} & \longrightarrow & 1 \\
 & & & & \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle \mathrm{res}_L} & & \\
1 & \longrightarrow & \dfrac{\mathbb{Z}}{l\mathbb{Z}} & \longrightarrow & \widetilde{G} & \xrightarrow{\psi} & G & \longrightarrow & 1
\end{array}$$

onde p_1 e p_2 são as projeções canônicas. Note que a linha de cima do diagrama ainda é uma extensão de grupos, e suponha que $\phi^*(\xi) = 0$. Ainda pelo teorema 2.5.3, tal extensão de grupos é trivial, ou seja, $\widetilde{G} \times_G G_{\mathbb{Q}} \simeq G_{\mathbb{Q}} \times \dfrac{\mathbb{Z}}{l\mathbb{Z}}$, e pertence à classe de cohomologia de $\phi^*(\xi)$. Pela propriedade do produto subdireto, existe um homomorfismo $\rho : G_{\mathbb{Q}} \to \widetilde{G} \times_G G_{\mathbb{Q}}$ tal que $p_2 \circ \rho : G_{\mathbb{Q}} \to G_{\mathbb{Q}}$ é a identidade em $G_{\mathbb{Q}}$. Tomando $\widetilde{\phi} = p_1 \circ \rho : G_{\mathbb{Q}} \to \widetilde{G}$, obtemos

$$\psi(\widetilde{\phi}(y)) = \psi(p_1(\rho(y))) = \mathrm{res}_L(p_2(\rho(y))) = \mathrm{res}_L(y), \ \forall \ y \in G_{\mathbb{Q}}.$$

Assim, conseguimos o requerido levantamento $\widetilde{\phi}$. O fato de $\widetilde{\phi}$ ser sobrejetora segue diretamente do fato de que p_1 é sobrejetora.

Capítulo 3

Lei de reciprocidade local de Artin

O objetivo deste capítulo é provar a lei de reciprocidade local de Artin. Para isto, além dos conceitos já estudados nos capítulos precedentes, usaremos uma ferramenta conhecida como *lei de grupo formal*, que é definida sobre o anel $A[[X]]$ das séries de potências de um anel A. Vamos inicialmente fazer uma breve revisão de algumas propriedades desse anel.

3.1 Algumas propriedades do anel $A[[X]]$

Definição 3.1.1. *Seja A um anel. Uma série de potências em A é uma sequência $f = (a_0,\ a_1,\ a_2,\ \ldots)$ de elementos de A. O conjunto de todas as séries de potências do anel A é denotado por $A[[X]]$.*

Assim, se A é um anel, podemos definir uma adição e uma multiplicação de elementos de $A[[X]]$ da seguinte forma:

$$\begin{aligned} (a_0,\ a_1,\ \ldots) + (b_0,\ b_1,\ \ldots) &= (a_0 + b_0,\ a_1 + b_1,\ \ldots) \\ (a_0,\ a_1,\ \ldots) \cdot (b_0,\ b_1,\ \ldots) &= \left(a_0 b_0,\ \ldots,\ \sum_{i+j=k} a_i b_j,\ \ldots \right) \end{aligned}$$

Dessa forma, a tripla $(A[[X]], +, \cdot)$ assim definida é um anel, conhecido como *anel das séries de potências em uma variável sobre A*. Geralmente escrevemos um elemento de $A[[X]]$ como $f(x) = \sum_{i=0}^{\infty} a_i X^i$. Da mesma forma como definimos o anel de polinômios em duas ou mais variáveis sobre um anel A podemos definir o anel das séries de potências em duas ou mais variáveis sobre um anel A.

Entretanto, precisamos de um certo cuidado ao trabalharmos com o anel $A[[X]]$. Um exemplo disso é que, geralmente, não podemos avaliar um elemento $a \in A$ numa série de potência $f(X)$, assim como fazemos no anel de polinômios

$A[X]$, pois estaremos somando infinitos elementos de A. Pela mesma razão, nós só podemos avaliar uma série de potências $g(X)$ em outra $f(X)$ se o termo constante de $g(X)$ é 0 (o que é o mesmo que dizer que $g(x) \in XA[[X]]$). Neste caso $f(g(X))$ estará definida e será denotada por $f \circ g$. Este mesmo cuidado deve ser tomado no anel $A[[X_1, \ldots, X_n]]$: se $f(X_1, \ldots, X_n) \in A[[X_1, \ldots, X_n]]$ e $g_1, \ldots, g_n \in A[[Y_1, \ldots, Y_m]]$, então $f(g_1, \ldots, g_n)$ estará bem definida como um elemento de $A[[Y_1, \ldots, Y_m]]$ se os termos constantes de todas as séries de potêcias g_i forem iguais a 0.

Lema 3.1.2. *Seja A um anel.*

1. *Se $f \in A[[X]]$ e $g,\ h \in XA[[X]]$, então $f \circ (g \circ h) = (f \circ g) \circ h$.*
2. *Seja $f = \sum_{i=1}^{\infty} a_i X^i \in XA[[X]]$. Existe $g \in XA[[X]]$ tal que $f \circ g = X$ se, e somente se, $a_1 \in A^\times$. Neste caso, g é única e satisfaz também $g \circ f = X$.*

Demonstração: 1. Sabemos que, em geral, $(f_1 f_2) \circ g = (f_1 \circ g)(f_2 \circ g)$. Assim, se n for um inteiro positivo, $f^n \circ g = (f \circ g)^n$.

Se $f(X) = X^n$, então $f \circ (g \circ h) = (g \circ h)^n$ e $(f \circ g) \circ h = g^n \circ h = (g \circ h)^n$, ou seja, a fórmula vale neste caso.

Para o caso geral $f(X) = \sum_{i=1}^{\infty} a_i X^i$, temos

$$\begin{aligned} f \circ (g \circ h) &= \left(\sum_{i=1}^{\infty} a_i X^i \right) \circ (g \circ h) = \sum_{i=1}^{\infty} a_i [X^i \circ (g \circ h)] = \sum_{i=1}^{\infty} a_i [(X^i \circ g) \circ h] = \\ &= \left[\sum_{i=1}^{\infty} a_i (X^i \circ g) \right] \circ h = \left[\left(\sum_{i=1}^{\infty} a_i X^i \right) \circ g \right] \circ h = (f \circ g) \circ h. \end{aligned}$$

2. Queremos mostrar que existe $g(X) = \sum_{i=1}^{\infty} b_i X^i$ tal que $\sum_{i=1}^{\infty} a_i g(X)^i = X$, isto é, queremos encontrar $b_1,\ b_2,\ b_3,\ \ldots \in A$ tais que

$$\begin{cases} a_1 b_1 = 1 \\ a_1 b_2 + a_2 {b_1}^2 = 0 \\ \ldots \\ a_1 b_n + (\text{polinômio em } a_2, \ldots, a_n,\ b_1, \ldots,\ b_{n-1}) = 0 \\ \ldots \end{cases}$$

Assim, se uma tal $g \in A[[X]]$ existe, então a primeira equação nos informa que $a_1 \in A^\times$. Reciprocamente, se $a_1 \in A^\times$, então cada b_i é unicamente determinado, mostrando assim a existência de uma única série de potências $g(X)$ tal que $f \circ g = X$.

Por fim, como $b_1 \in A^\times$, então existe $h \in XA[[X]]$ tal que $g \circ h = X$. Assim,

$$f = f \circ X = f \circ (g \circ h) = (f \circ g) \circ h = X \circ h = h \Rightarrow g \circ f = g \circ h = X.$$

□

3.2 Leis de grupo formais

Definição 3.2.1. *Seja A um anel. Uma lei de grupo formal sobre A é uma série de potências $F \in A[[X,Y]]$ tal que:*

1. $F(X,Y) = X + Y +$ *termos de grau* ≥ 2;
2. $F(X, F(Y,Z)) = F(F(X,Y), Z)$;
3. $F(X,Y) = F(Y,X)$.

Proposição 3.2.2. *Se $F(X,Y)$ é uma lei de grupo formal, então*

$$F(X,Y) = X + Y + \sum_{\substack{1 \leq i < \infty \\ 1 \leq j < \infty}} a_{i,j} X^i Y^j.$$

Demonstração: Note que o item *1.* implica que o termo constante de $F(X,Y)$ é 0. Além disso, tomando $Y = Z = 0$ nos itens *1.* e *2.*, obtemos

$$F(X,0) = X + (\text{termos de grau} \geq 2 \text{ em } X) \qquad \text{e} \qquad F(X,0) = F(F(X,0),0).$$

Seja $F(X,0) = f(X) \in XA[[X]]$. Pelo lema 3.1.2, existe uma única $g(X) \in XA[[X]]$ tal que $f \circ g = X$. Assim,

$$f(f(X)) = F(f(X),0) = F(F(X,0),0) = F(X,0) = f(X) \Rightarrow f \circ f = f.$$

Logo $f = f \circ X = f \circ (f \circ g) = (f \circ f) \circ g = f \circ g = X \Rightarrow F(X,0) = f(X) = X$.

Analogamente $F(0,Y) = Y$. Assim, $F(X,Y) = X + Y + \sum_{\substack{1 \leq i < \infty \\ 1 \leq j < \infty}} a_{i,j} X^i Y^j$. $\square$

Pode ser provado (veja [9], p.34) que para cada série de potência $F(X,Y) \in A[[X,Y]]$ tal que $F(X,0) = X$ e $F(0,Y) = Y$ existe uma única série de potência $i_F(X) \in XA[[X]]$ tal que $F(X, i_F(X)) = 0$. Assim, pela proposição 3.2.2, para cada lei de grupo formal $F(X,Y)$ existe uma única $i_F(X) \in XA[[X]]$ tal que $F(X, i_F(X)) = 0$.

A mais simples lei de grupo formal é $F(X,Y) = X + Y$. Uma lei de grupo formal um pouco mais elaborada é $F(X,Y) = X + Y + XY$. Com efeito, precisamos mostrar apenas que vale o item *2.* da definição 3.2.1, pois os outros são óbvios. Para isto, basta notar que

$$\begin{aligned} F(X, F(Y,Z)) &= F(X, Y + Z + YZ) = X + Y + Z + YZ + XY + XZ + XYZ \\ &\text{e} \\ F(F(X,Y), Z) &= F(X + Y + XY, Z) = X + Y + XY + Z + XZ + YZ + XYZ. \end{aligned}$$

Vejamos agora a noção de homomorfismo entre duas leis de grupos formais.

Definição 3.2.3. *Sejam $F(X,Y)$ e $G(X,Y)$ duas leis de grupos formais. Um homomorfismo $h : F \to G$ é uma série de potências $h(T) \in TA[[T]]$ tal que*

$$h(F(X,Y)) = G(h(X), h(Y)).$$

Caso exista um homomorfismo $h' : G \to F$ tal que $(h \circ h')(T) = T = (h' \circ h)(T)$, dizemos que h é um isomorfismo, cujo inverso é h'. Um homomorfismo $h : F \to F$ é chamado um endomorfismo de F.

Exemplo 3.2.4. *Considere a lei de grupo formal*

$$F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1.$$

Então $h(T) = (1+T)^n - 1$ é um endomorfismo de F, $\forall\ n \in \mathbb{N} - \{0\}$. De fato:

$$\begin{aligned} F(h(X), h(Y)) &= (1+h(X))(1+h(Y)) - 1 = (1+X)^n(1+Y)^n - 1 = \\ &= [(1+X)(1+Y)]^n - 1 = [1+F(X,Y)]^n - 1 = h(F(X,Y)). \end{aligned}$$

Proposição 3.2.5. *Seja G uma lei de grupo formal. Para $f,\ g \in TA[[T]]$, definimos*

$$f +_G g = G(f(T), g(T)).$$

Então $(TA[[T]],\ +_G)$ é um grupo abeliano.

Demonstração: O fato de $f +_G g \in TA[[T]]$ segue diretamente da proposição 3.2.2: se $f,\ g \in TA[[T]]$, então

$$f +_G g = G(f(T), g(T)) = f(T) + g(T) + \sum_{\substack{1 \le i < \infty \\ 1 \le j < \infty}} a_{i,j} f(T)^i g(T)^j \in TA[[T]].$$

- $+_G$ é associativa: como $G(X, G(Y,Z)) = G(G(X,Y), Z)$, então

$$\begin{aligned} f +_G (g +_G h) &= f +_G G(g(T), h(T)) = G(f(T), G(g(T), h(T))) = \\ &= G(G(f(T), g(T)), h(T)) = G(f(T), g(T)) +_G h = \\ &= (f +_G g) +_G h. \end{aligned}$$

- $+_G$ é comutativa: como $G(X,Y) = G(Y,X)$, então

$$f +_G g = G(f(T), g(T)) = G(g(T), f(T)) = g +_G f.$$

- $f +_G 0 = G(f(T), 0) = f(T)$, pela proposição 3.2.2.
- O elemento inverso de f é $i_G \circ f$. De fato,

$$f +_G (i_G \circ f) = G(f(T), (i_G \circ f)(T)) = G(f(T), i_G(f(T))) = 0.$$

□

Teorema 3.2.6. *Sejam F e G duas leis de grupo formais.*

1. *O conjunto $Hom(F,G)$ dos homomorfismos de F em G é um grupo abeliano sob a operação $f +_G g$.*

2. *O conjunto $End(F)$ dos endomorfismos de F é um anel (não necessariamente comutativo) com a multiplicação $f \circ g$.*

Demonstração: 1. Claramente $\mathrm{Hom}(F,G)$ é um subconjunto de $TA[[T]]$. Como $0 \in \mathrm{Hom}(F,G)$, é suficiente mostrar que $\mathrm{Hom}(F,G)$ é fechado pela soma e pelo inverso. Sejam $f,\ g \in \mathrm{Hom}(F,G)$ e considere $h = f +_G g \in TA[[T]]$. Então

$$\begin{aligned}
h(F(X,Y)) &= (f +_G g)(F(X,Y)) = \\
&= G(f(F(X,Y)), g(F(X,Y))) = \\
&= G(G(f(X), f(Y)), G(g(X), g(Y))) = \\
&= G(f(X), f(Y)) +_G G(g(X), g(Y)) = \\
&= (f(X) +_G f(Y)) +_G (g(X) +_G g(Y)) = \\
&= (f(X) +_G g(X)) +_G (f(Y) +_G g(Y)) = \\
&= G(f(X), g(X)) +_G G(f(Y), g(Y)) = \\
&= G(G(f(X), g(X)), G(f(Y), g(Y))) = \\
&= G((f +_G g)(X), (f +_G g)(Y)) = \\
&= G(h(X), h(Y)).
\end{aligned}$$

Logo $h \in \mathrm{Hom}(F,G)$. Agora, para mostrarmos que $i_G \circ f \in \mathrm{Hom}(F,G)$, note inicialmente que

$$\begin{aligned}
G(G(f(X), f(Y)), G((i_G \circ f)(X), (i_G \circ f)(Y))) &= \\
G(f(X), f(Y)) +_G G((i_G \circ f)(X), (i_G \circ f)(Y)) &= \\
(f(X) +_G f(Y)) +_G ((i_G \circ f)(X) +_G (i_G \circ f)(Y)) &= \\
(f(X) +_G (i_G \circ f)(X)) +_G (f(Y) +_G (i_G \circ f)(Y)) &= \ 0 +_G 0 = 0.
\end{aligned}$$

Pela unicidade de i_G, temos

$$\begin{aligned}
G((i_G \circ f)(X), (i_G \circ f)(Y)) &= i_G(G(f(X), f(Y))) \\
&= i_G(f(F(X,Y))) = (i_G \circ f)(F(X,Y)).
\end{aligned}$$

Logo $i_G \circ f \in \mathrm{Hom}(F,G)$.

2. De início, temos que mostrar que se $f,\ g \in \mathrm{End}(F)$, então $f \circ g \in \mathrm{End}(F)$. De fato,

$$\begin{aligned}
(f \circ g)(F(X,Y)) &= f(g(F(X,Y))) = f(F(g(X), g(Y))) = \\
&= F(f(g(X)), f(g(Y))) = F((f \circ g)(X), (f \circ g)(Y)).
\end{aligned}$$

Nós também já mostramos no lema 3.1.2 que a composição é associativa. Como $f(T) = T \in \mathrm{End}(F)$ é claramente o elemento neutro da operação $\circ$, resta mostrar que $\circ$ é distributiva com relação à adição $+_F$. Se $f,\ g,\ h \in \mathrm{End}(F)$, então

$$\begin{aligned} f \circ (g +_F h) &= f(F(g(T), h(T))) = F(f(g(T)), f(h(T))) = \\ &= F((f \circ g)(T), (f \circ h)(T)) = (f \circ g) +_F (f \circ h). \end{aligned}$$

e

$$\begin{aligned} (f +_F g) \circ h &= F(f(T), g(T)) \circ h = F(f(h(T)), g(h(T))) = \\ &= F((f \circ h)(T), (g \circ h)(T)) = (f \circ h) +_F (g \circ h). \end{aligned}$$

□

3.3 Leis de grupo de Lubin-Tate

Antes de continuar, alertamos o leitor que toda a teoria desenvolvida até aqui (extensões integrais de anéis, anel de inteiros, bases integrais, ramificação, etc...) pode ser estendida para os corpos p-ádicos, sendo a extensa maioria dos resultados válidos para tais corpos (e, mais geralmente, para corpos de frações de domínios de integridade de característica zero). A demonstração de quase todos os resultados generalizados não é tão difícil uma vez entendida claramente as demonstrações que temos em mãos, e supor-se-á feita.

A partir de agora, estudaremos mais detalhadamente algumas leis de grupo formais, a saber, as *leis de grupo formais de Lubin-Tate*. Para isto, é recomendável ter alguma familiaridade com a álgebra existente por trás dos corpos p-ádicos. Dessa forma, colocamos aqui um breve resumo dos fatos a serem utilizados posteriormente. As demonstrações dos resultados abaixo enunciados podem ser encontradas no capítulo 7 de [8] e nos capítulos 1 e 2 de [12].

Sejam p um número primo e K uma extensão finita do corpo dos números p-ádicos $\mathbb{Q}_p$. Seu anel de inteiros, assim como antes, é denotado por $\mathcal{O}_K$. Neste caso, $\mathcal{O}_K$ é um DIP e tem um único ideal maximal (em particular, primo) não nulo, o qual deve ser, obrigatoriamente, o complementar das unidades $\mathcal{O}_K - \mathcal{O}_K^\times$. Denotaremos tal ideal por $\mathfrak{m}_K = \mathfrak{m}$. Como $\mathcal{O}_K$ é um DIP, $\mathfrak{m}_K = \pi\mathcal{O}_K$, para algum $\pi \in \mathfrak{m}_K$. Tal elemento π é chamado de *uniformizador de* $\mathcal{O}_K$, ou de *primo de* K. Assim, cada elemento não nulo $a \in \mathcal{O}_K$ se escreve de uma maneira única $a = u\pi^m$, onde $u \in \mathcal{O}_K^\times$ e $m \in \mathbb{N}$. Em particular, cada elemento não nulo $a \in K$ se escreve de maneira única $a = u\pi^m$, onde $u \in \mathcal{O}_K^\times$ e $m \in \mathbb{Z}$.

Definimos o *corpo residual* de K como sendo o corpo $\dfrac{\mathcal{O}_K}{\mathfrak{m}_K}$, que será denotado por k. É fato que k é um corpo finito de característica p. Denotaremos sua cardinalidade por q. Neste caso, definimos a *valorização normalizada* de um elemento não nulo $a = u\pi^m$ de K por $|a| = q^{-m}$.

Se L for uma extensão não ramificada de K cujo corpo residual tem cardinalidade q, então a extensão L/K é galoisiana e $\mathrm{Gal}(L/K)$ é um grupo cíclico, gerado

por, digamos, σ. Tal elemento σ, chamado de *elemento de Frobenius* da extensão L/K, tem a propriedade de que

$$\sigma(\alpha) \equiv \alpha^q \pmod{\mathfrak{m}_L},\ \forall\ \alpha \in \mathcal{O}_L,$$

e é denotado por $\mathrm{Frob}_{L/K}$.

Fixadas as notações acima (que valerão até o fim deste capítulo), podemos prosseguir nosso estudo. Para simplificar a notação, colocamos $A = \mathcal{O}_K$.

Definição 3.3.1. *Definimos $\mathcal{F}_\pi$ como sendo o conjunto de todos os $f(X) \in A[[X]]$ tais que:*

1. *$f(X) = \pi X + (\text{termos de grau } \geq 2)$;*
2. *$f(X) \equiv X^q \ (mod\ \pi)$.*

Exemplo 3.3.2. 1. *O polinômio $f(X) = \pi X + X^q \in \mathcal{F}_\pi$.*

2. *Se $K = \mathbb{Q}_p$ e $\pi = p$, então*

$$f(X) = (1+X)^p - 1 = pX + \binom{p}{2}X^2 + \cdots + pX^{p-1} + X^p \in \mathcal{F}_p.$$

Definição 3.3.3. *Seja R um anel. Um polinômio $p(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ é dito homogêneo se todos os seus monômios têm o mesmo grau.*

Lema 3.3.4. *Sejam $f,\ g \in \mathcal{F}_\pi$ e seja $\phi_0(X_1, \ldots, X_n)$ uma forma linear com coeficientes em A. Então existe uma única $\phi \in A[[X_1, \ldots, X_n]]$ tal que*

$$\begin{cases} \phi(X_1, \ldots, X_n) &= \phi_0(X_1, \ldots, X_n) + \text{termos de grau } \geq 2 \\ f(\phi(X_1, \ldots, X_n)) &= \phi(g(X_1), \ldots, g(X_n)) \end{cases}$$

Demonstração: Inicialmente vamos mostrar por indução em $r \in \mathbb{N}^*$ que para cada $r \in \mathbb{N}^*$ existe um único polinômio $\phi_r(X_1, \ldots, X_n)$ de grau r tal que

$$\begin{cases} \phi_r(X_1, \ldots, X_n) &= \phi_0(X_1, \ldots, X_n) + \text{termos de grau } \geq 2 \\ f(\phi_r(X_1, \ldots, X_n)) &= \phi_r(g(X_1), \ldots, g(X_n)) + \text{termos de grau} \geq r+1. \end{cases}$$

Vamos para o caso $r = 1$. Pela primeira equação e sabendo que $\deg(\phi_1) = 1$, a única opção que temos é tomar $\phi_1 = \phi_0$. Claramente ϕ_1 satisfaz a primeira equação e, se escrevermos $\phi_0(X_1, \ldots, X_n) = \sum_{i=1}^{n} a_i X_i$, obtemos

$$\begin{aligned} f(\phi_1(X_1, \ldots, X_n)) &= f(\phi_0(X_1, \ldots, X_n)) = \pi\phi_0(X_1, \ldots, X_n) + \text{termos de grau} \geq 2 \\ &= \pi \sum_{i=1}^{n} a_i X_i + \text{termos de grau} \geq 2 \\ &= \sum_{i=1}^{n} a_i(\pi X_i) + \text{termos de grau} \geq 2 \\ &= \phi_1(g(X_1), \ldots, g(X_n)) + \text{termos de grau} \geq 2. \end{aligned}$$

Suponha então que $r \geq 1$ e que já temos definido o único ϕ_r.

Como ϕ_r é único, $\phi_{r+1} = \phi_r + Q(X_1, \ldots, X_n)$, onde $Q(X_1, \ldots, X_n)$ é um polinômio homogêneo de grau $r+1$ em $A[X_1, \ldots, X_n]$. É fácil ver que este polinômio satisfaz as condições acima, e, portanto, temos definido ϕ_r, $\forall\ r \in \mathbb{N}^*$. Além disso,

$$\phi_{r+1} = \phi_r + \text{termos de grau } \geq r+1.$$

Dessa forma, podemos definir ϕ como sendo a única série de potências que satisfaz $\phi = \phi_r + \text{termos de grau } \geq r+1$, $\forall\ r \in \mathbb{N}^*$. Pelas relações satisfeitas pelas ϕ_r, ϕ satisfaz as condições desejadas. □

Proposição 3.3.5. *Para cada $f \in \mathcal{F}_\pi$, existe uma única lei de grupo formal $F_f \in A[[X,Y]]$ admitindo f como endomorfismo.*

Demonstração: Tomando $g = f$ e $\phi_0(X,Y) = X + Y$ no lema anterior, existe uma única $F_f \in A[[X,Y]]$ satisfazendo

$$\begin{cases} F_f(X,Y) &= X + Y + \text{termos de grau } \geq 2 \\ f(F_f(X,Y)) &= F_f(f(X), f(Y)). \end{cases}$$

Assim, precisamos apenas mostrar que F_f é uma lei de grupo formal. Note que F_f já satisfaz a primeira condição para ser uma lei de grupo formal, de modo que precisamos mostrar apenas as outras duas.

2. Mostremos que $F_f(X, F_f(Y,Z)) = F_f(F_f(X,Y), Z)$. Note que

$$\begin{aligned} F_f(X, F_f(Y,Z)) &= X + F_f(Y,Z) + \text{termos de grau } \geq 2 \\ &= X + Y + Z + \text{termos de grau } \geq 2. \end{aligned}$$

Seja agora $G_1(X,Y,Z) = F_f(X, F_f(Y,Z))$. Então

$$\begin{aligned} f(G_1(X,Y,Z)) &= f(F_f(X, F_f(Y,Z))) = F_f(f(X), f(F_f(Y,Z))) \\ &= F_f(f(X), F_f(f(Y), f(Z))) = G_1(f(X), f(Y), f(Z)). \end{aligned}$$

Analogamente mostra-se que $G_2(X,Y,Z) = F_f(F_f(X,Y), Z)$ satisfaz estas mesmas equações. Tomando $\phi_0(X,Y,Z) = X + Y + Z$ e $f = g$ no lema anterior, deve existir uma única série de potências satisfazendo tais equações. Logo $G_1 = G_2$, ou seja, $F_f(X, F_f(Y,Z)) = F_f(F_f(X,Y), Z)$.

3. Mostremos agora que $F_f(X,Y) = F_f(Y,X)$. Seja $G(X,Y) = F_f(Y,X)$. Precisamos mostrar que $G(X,Y) = F_f(X,Y)$. Note que

$$\begin{cases} G(X,Y) &= X + Y + \text{termos de grau } \geq 2 \\ f(G(X,Y)) &= f(F_f(Y,X)) = F_f(f(Y), f(X)) = G(f(X), f(Y)). \end{cases}$$

Como $F_f(X,Y)$ é a única série de potências que satisfaz estas propriedades, então $G(X,Y) = F_f(X,Y)$. □

Exemplo 3.3.6. *Seja $K = \mathbb{Q}_p$ e $\pi = p$. Então $f(T) = (1+T)^p - 1 \in \mathcal{F}_p$ e $F(X,Y) = X + Y + XY$ admite f como endomorfismo (pelo exemplo 3.2.4). Logo $F = F_f$.*

Proposição 3.3.7. *Sejam $f,\ g \in \mathcal{F}_\pi$ e $a \in A$. Denote por $[a]_{g,f}$ o único elemento de $A[[T]]$ tal que*

$$\begin{cases} [a]_{g,f}(T) &= aT + \text{termos de grau } \geq 2 \\ g([a]_{g,f}(T)) &= [a]_{g,f}(f(T)). \end{cases}$$

Então $[a]_{g,f}$ é um homomorfismo $F_f \to F_g$.

Demonstração: Seja $h = [a]_{g,f}$. A existência e a unicidade de h são garantidas pelo lema 3.3.4. Precisamos então mostrar que $h(F_f(X,Y)) = F_g(h(X), h(Y))$. Temos

$$\begin{aligned} h(F_f(X,Y)) &= aF_f(X,Y) + \text{termos de grau } \geq 2 \\ &= aX + aY + \text{termos de grau} \geq 2 \end{aligned}$$

e

$$\begin{aligned} F_g(h(X), h(Y)) &= F_g(aX + \text{termos de grau } \geq 2, aY + \text{termos de grau } \geq 2) \\ &= aX + aY + \text{termos de grau } \geq 2. \end{aligned}$$

Além disso,

$$\begin{aligned} g(h(F_f(X,Y))) &= (g \circ h)(F_f(X,Y)) = (h \circ f)(F_f(X,Y)) = \\ &= h(f(F_f(X,Y))) = h(F_f(f(X), f(Y))) \end{aligned}$$

e

$$\begin{aligned} g(F_g(h(X), h(Y))) &= F_g((g \circ h)(X), (g \circ h)(Y)) = \\ &= F_g((h \circ f)(X), (h \circ f)(Y)) = F_g(h(f(X)), h(f(Y))). \end{aligned}$$

Pela unicidade do lema 3.3.4 obtemos $h(F_f(X,Y)) = F_g(h(X), h(Y))$. □

Assim, para cada $a \in A$ existe um único endomorfismo $[a]_f : F_f \to F_f$ tal que $[a]_f = aT +$ termos de grau ≤ 2 e $[a]_f$ comuta com f. Basta tomar $[a]_f = [a]_{f,f}$. A proposição anterior implica também os três seguintes corolários, que encerram nosso estudo sobre séries de grupos formais:

Corolário 3.3.8. *Se $a,\ b \in A$, então $[a+b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}$ e $[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}$.*

Demonstração: Basta ver que, em cada caso, as séries de potências satisfazem as condições do lema 3.3.4. Pela unicidade deste mesmo lema, elas são iguais. □

Corolário 3.3.9. *Se $f,\ g \in \mathcal{F}_\pi$, então $F_f \simeq F_g$.*

Demonstração: Seja $u \in A^\times$. Analogamente à demonstração anterior, provamos que $[u]_{g,f}$ é um homomorfismo de F_f em F_g e que $[u^{-1}]_{f,g}$ é um homomorfismo de F_g em F_f. Agora, como

$$[u]_{g,f} \circ [u^{-1}]_{f,g} = [uu^{-1}]_{g,g} = [1]_{g,g} = T = [1]_{f,f} = [u^{-1}u]_{f,f} = [u^{-1}]_{f,g} \circ [u]_{g,f},$$

o corolário está demonstrado. □

Corolário 3.3.10. *A função $\Upsilon : A \to End(F_f)$ dada por $\Upsilon(a) = [a]_f$ é um homomorfismo injetor de anéis.*

Demonstração: Se $a,\ b \in A$, então

$$\Upsilon(a+b) = [a+b]_f = [a+b]_{f,f} = [a]_{f,f} +_{F_f} [b]_{f,f} = [a]_f +_{F_f} [b]_f = \Upsilon(a) +_{F_f} \Upsilon(b)$$

e

$$\Upsilon(ab) = [ab]_f = [ab]_{f,f} = [a]_{f,f} \circ [b]_{f,f} = [a]_f \circ [b]_f = \Upsilon(a) \circ \Upsilon(b).$$

Finalmente, se $\Upsilon(a) = \Upsilon(b)$, então $[a]_f = [b]_f \Rightarrow a = b$. □

3.4 A lei de reciprocidade local

Nesta seção, ainda manteremos a notação da seção anterior: K será uma extensão finita de $\mathbb{Q}_p$, $A = \mathcal{O}_K$, π é um uniformizador de $\mathcal{O}_K$ e $k = \dfrac{A}{\mathfrak{m}}$ é o corpo residual de K contendo q elementos, onde q é uma potência de p. Quando for necessário, escreveremos $\mathfrak{m} = \mathfrak{m}_K$.

Seja $\mathbb{K}$ um corpo. Fixado um fecho algébrico $\overline{\mathbb{K}}$ de $\mathbb{K}$, defina $\mathbb{K}^{ab}$ como sendo o compósito de todas as extensões abelianas de $\mathbb{K}$ (contidas em $\overline{\mathbb{K}}$). Como o compósito de extensões abelianas de um corpo qualquer é ainda uma extensão abeliana de tal corpo, $\mathbb{K}^{ab}$ pode ser visto como a máxima extensão abeliana de $\mathbb{K}$ contida em $\overline{\mathbb{K}}$. O que faremos nesta seção será construir duas extensões K_π e K^{un} de K de tal forma que $K^{ab} = K_\pi \cdot K^{un}$, onde K_π é uma extensão totalmente ramificada de K e K^{un} é a maior extensão não ramificada de K contida em $\overline{K}$.

A construção de K^{un} não é longa: se $m \in \mathbb{N}$, denote por μ_m o conjunto das raízes m-ésimas de 1 em $\overline{K}$. Se m não for um múltiplo de p, então a extensão $K[\mu_m]/K$ será não ramificada. Como o compósito de extensões não ramificadas é ainda não ramificada, o compósito de todas as extensões $K[\mu_m]$ de K onde $p \nmid m$ será uma extensão não ramificada de K de tal forma que seu corpo residual é um fecho algébrico de k. Assim, podemos definir K^{un} como sendo o compósito de todas as extensões $K[\mu_m]$ de K tais que $p \nmid m$.

Vamos agora construir o corpo K_π, tal que $K^{ab} = K_\pi \cdot K^{un}$.

Seja $f(T) = \pi T + T^q \in \mathcal{F}_\pi$ e denote $f^{(n)} = \underbrace{f \circ \cdots \circ f}_{n \text{ vezes}},\ \forall\ n \in \mathbb{N}$. Note que $f^{(n)}(T) = \pi^n T + \pi g_n(T) + T^{q^n}$, para algum polinômio $g_n(T) \in A[T]$. Seja também Λ_n o conjunto das raízes de $f^{(n)}$. Fixadas estas notações, temos o seguinte teorema, cuja prova pode ser encontrada em [9], p. 35 - 38:

Teorema 3.4.1. *Seja* $K_{\pi,n} = K[\Lambda_n]$.

1. *Para cada número natural* $n \in \mathbb{N}^*$, *a extensão* $K_{\pi,n}/K$ *é totalmente ramificada de grau* $(q-1)q^{n-1}$.
2. *Existe um isomorfismo* $g : \left(\frac{A}{\mathfrak{m}^n}\right)^\times \to \mathrm{Gal}(K_{\pi,n}/K)$. *Em particular, a extensão* $K_{\pi,n}/K$ *é abeliana.*
3. *Para cada* $n \in \mathbb{N}^*$, π *é uma norma em* $K_{\pi,n}$.

Dessa forma, podemos tomar K_π como sendo o compósito de todos os corpos $K[\Lambda_n]$. Assim, em face do que foi feito até agora, podemos definir um homomorfismo

$$\phi_\pi : K^\times \to \mathrm{Gal}(K_\pi \cdot K^{un}/K)$$

da seguinte forma:

Seja $a \in K^\times$. Como $K_\pi \cap K^{un} = K$, é suficiente descrever as ações de $\phi_\pi(a)$ em K_π e em K^{un} separadamente. Escreva $a = u\pi^m$, onde $u \in \mathcal{O}_K^\times$ e $m \in \mathbb{Z}$. Definimos que $\phi_\pi(a)$ age como $\mathrm{Frob}_{L/K}$ em qualquer extensão não ramificada L de K, enquanto que em K_π ele age da seguinte forma:

$$\phi_\pi(a)(\lambda) = [u^{-1}]_f(\lambda),\ \forall\ \lambda \in \bigcup_{n\in\mathbb{N}} \Lambda_n.$$

Deve ser enfatizado, entretanto, que tanto ϕ_π quanto K_π, na verdade, não dependem do elemento primo π que escolhemos, ou seja, se π' é um elemento primo de A associado a π, então $\phi_\pi = \phi_{\pi'}$ e $K_\pi = K_{\pi'}$. (veja [9], p. 39 - 42). Assim, $K^{ab} = K_\pi \cdot K^{un}$. Com isto obtemos a lei de reciprocidade local de Artin:

Teorema 3.4.2 (Lei de reciprocidade local de Artin)**.** *Se* K *for uma extensão finita de* $\mathbb{Q}_p$, *então existe um único homomorfismo*

$$\phi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$$

que satisfaz:

1. *Se* π *é um elemento primo de* K *e se* L *é uma extensão finita não ramificada de* K, *então* $\phi_K(\pi)|_L = Frob_{L/K}$;
2. *Se* L *é uma extensão finita abeliana de* K, *então* $N_{L/K}(L^\times)$ *é o kernel do homomorfismo*

$$\begin{array}{rccc} \phi_{L/K} : & K^\times & \to & \mathrm{Gal}(L/K) \\ & a & \mapsto & \phi_K(a)|_L \end{array}$$

e ϕ_K *induz um isomorfismo*

$$\overline{\phi_{L/K}} : \frac{K^\times}{N_{L/K}(L^\times)} \xrightarrow{\simeq} \mathrm{Gal}(L/K)$$

Em particular, $(K^\times : N_{L/K}(L^\times)) = [L : K]$.

Chamamos a função $\phi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ de *lei de reciprocidade local de Artin* de K. Já o isomorfismo $\overline{\phi_{L/K}} : \dfrac{K^\times}{N_{L/K}(L^\times)} \to \mathrm{Gal}(L/K)$ será chamado de *lei de reciprocidade local de Artin de K com relação a L.*

Do teorema já segue rapidamente que se L é uma extensão finita abeliana de K, então o seguinte diagrama é comutativo:

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{ab}/K) \\ \downarrow{\scriptstyle \mathrm{can}} & & \downarrow{\scriptstyle \mathrm{rest}_L} \\ \dfrac{K^\times}{N_{L/K}(L^\times)} & \xrightarrow[\simeq]{\overline{\phi_{L/K}}} & \mathrm{Gal}(L/K) \end{array}$$

onde $\mathrm{can}(a) = \overline{a} = a \cdot N_{L/K}(L^\times)$ e $\mathrm{rest}_L(\tau) = \tau|_L$.

De fato, se $a \in K^\times$, então $\overline{\phi_{L/K}} \circ \mathrm{can}(a) = \overline{\phi_{L/K}}(\overline{a}) = \phi_{L/K}(a) = \phi_K(a)|_L$.

Definição 3.4.3. *Seja K um corpo. Os subgrupos de $K^\times$ da forma $N_{L/K}(L^\times)$ para alguma extensão abeliana L de K são chamados de grupos de normas de K.*

Vejamos algumas consequências da lei de reciprocidade de Artin:

Corolário 3.4.4. *Sejam K uma extensão finita de $\mathbb{Q}_p$, $\phi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ sua lei de reciprocidade local e L, L' extensões finitas abelianas de K. Então:*

1. $N_{LL'/K}((LL')^\times) = N_{L/K}(L^\times) \cap N_{L'/K}(L'^\times)$.
2. $L \subseteq L' \Leftrightarrow N_{L'/K}(L'^\times) \subseteq N_{L/K}(L^\times)$.
3. *A função $L \mapsto N_{L/K}(L^\times)$ é uma bijeção do conjunto das extensões finitas abelianas de K no conjunto dos grupos de normas de $K^\times$.*
4. *Todo subgrupo de $K^\times$ contendo um grupo de normas é ele mesmo um grupo de normas.*
5. $N_{L\cap L'/K}((L \cap L')^\times) = N_{L/K}(L^\times) \cdot N_{L'/K}(L'^\times)$.

Demonstração: 1. Sabemos, pelo teorema da transitividade das normas, que se $L \subseteq L'$, então $N_{L'/K} = N_{L/K} \circ N_{L'/L}$. Assim, $N_{L'/K}(L'^\times) \subseteq N_{L/K}(L^\times)$. Agora, como $L \cup L' \subseteq LL'$, então $N_{LL'/K}((LL')^\times) \subseteq N_{L/K}(L^\times) \cap N_{L'/K}(L'^\times)$.

Reciprocamente, se $a \in N_{L/K}(L^\times) \cap N_{L'/K}(L'^\times)$, então $a \in \ker(\phi_{L/K}) \cap \ker(\phi_{L'/K}) \Rightarrow \phi_{L/K}(a) = 1 = \phi_{L'/K}(a)$. Mas

$$\overline{\phi_{LL'/K}}(\overline{a})|_L = \phi_{LL'/K}(a)|_L = \phi_K(a)|_{LL'}|_L = \phi_K(a)|_L = \phi_{L/K}(a) = 1.$$

Analogamente, $\overline{\phi_{LL'/K}}(\overline{a})|_{L'} = 1$. Como a função

$$\begin{array}{rccc} \rho : & \mathrm{Gal}(LL'/K) & \to & \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K) \\ & \sigma & \mapsto & (\sigma|_L,\ \sigma|_{L'}) \end{array}$$

é injetora, segue que $\overline{\phi_{LL'/K}}(\overline{a}) = 1 \Rightarrow a \in N_{LL'/K}((LL')^\times)$.

2. A implicação $\Rightarrow$ já foi feita no item anterior. Façamos a outra direção. Suponha que $N_{L'/K}(L'^\times) \subseteq N_{L/K}(L^\times)$. Pelo item *1.*, $N_{LL'/K}((LL')^\times) = N_{L'/K}(L'^\times)$.

Pelo item *2.* da lei de reciprocidade local de Artin,

$$[LL' : K] = (K^\times : N_{LL'/K}(LL'^\times)) = (K^\times : N_{L'/K}(L'^\times)) = [L' : K].$$

Como $LL' \supseteq L'$, então $LL' = L' \Rightarrow L \subseteq L'$.

3. É claro que a função $L \mapsto N_{L/K}(L^\times)$ é sobrejetiva. Provemos então sua injetividade. Se $N_{L/K}(L^\times) = N_{L'/K}(L'^\times)$, então $N_{L/K}(L^\times) \subseteq N_{L'/K}(L'^\times)$ e $N_{L'/K}(L'^\times) \subseteq N_{L/K}(L^\times)$. Pelo item anterior, $L \subseteq L'$ e $L' \subseteq L \Rightarrow L = L'$.

4. Seja $N = N_{L/K}(L^\times)$ um grupo de normas e seja I um subgrupo de $K^\times$ contendo N. Então $N \subseteq I \subseteq K^\times$. Como ϕ_K é homomorfismo, então $\phi_K(I)$ é subgrupo de $\mathrm{Gal}(K^{ab}/K)$. Seja M o corpo fixo por $\phi_K(I)$. Como $I \supseteq N$, então M também é uma extensão abeliana finita de K, satisfazendo $M \subseteq L$. Segue que

$$\overline{\phi_{L/K}}\left(\frac{I}{N}\right) = \phi_{L/K}(I) = \phi_K(I)|_L = \mathrm{Gal}(L/M).$$

Considere agora o seguinte diagrama comutativo:

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \\ \downarrow{\scriptstyle \mathrm{can}} & & \downarrow{\scriptstyle \mathrm{rest}_M} \\ \dfrac{K^\times}{N_{M/K}(M^\times)} & \xrightarrow[\simeq]{\overline{\phi_{M/K}}} & \mathrm{Gal}(M/K) \end{array}$$

Por um lado, $\ker(\overline{\phi_{M/K}} \circ \mathrm{can}) = N_{M/K}(M^\times)$. Por outro lado, o kernel de

$$K^\times \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/K) \xrightarrow{\mathrm{rest}_M} \mathrm{Gal}(M/K)$$

é ${\phi_{L/K}}^{-1}(\mathrm{Gal}(L/M)) = I$, pela teoria de Galois. Logo $I = N_{M/K}(M^\times)$ é um grupo de normas.

5. Pelos itens *2.* e *3.*, a função $L \mapsto N_{L/K}(L^\times)$ é uma bijeção que inverte as inclusões entre as extensões finitas abelianas de K e os grupos de normas de $K^\times$. Dessa forma, como $L \cap L'$ é a maior extensão de K contida em L e em L', e $N_{L/K}(L^\times) \cdot N_{L'/K}(L'^\times)$ é um grupo de normas (pelo item anterior) que é o menor subgrupo de $K^\times$ contendo $N_{L/K}(L^\times)$ e $N_{L'/K}(L'^\times)$, segue que $N_{L\cap L'/K}((L \cap L')^\times) = N_{L/K}(L^\times) \cdot N_{L'/K}(L'^\times)$. □

Assim, se L e M são duas extensões finitas abelianas de K satisfazendo $M \subseteq L$, então o seguinte diagrama é comutativo:

$$\begin{array}{ccc}
K^\times & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{ab}/K) \\
\Big\downarrow{\scriptstyle \mathrm{can}} & & \Big\downarrow{\scriptstyle \mathrm{rest}_L} \\
\dfrac{K^\times}{N_{L/K}(L^\times)} & \xrightarrow[\simeq]{\overline{\phi_{L/K}}} & \mathrm{Gal}(L/K) \\
\Big\downarrow{\scriptstyle \mathrm{can}} & & \Big\downarrow{\scriptstyle \mathrm{rest}_M} \\
\dfrac{K^\times}{N_{M/K}(M^\times)} & \xrightarrow[\simeq]{\overline{\phi_{M/K}}} & \mathrm{Gal}(M/K)
\end{array}$$

De fato,

$$\overline{\phi_{L/K}}(a \cdot N_{L/K}(L^\times))|_M = \phi_{L/K}(a)|_M = \phi_K(a)|_L|_M = \phi_K(a)|_M.$$

Por outro lado,

$$\begin{aligned}
\overline{\phi_{M/K}}((a \cdot N_{L/K}(L^\times)) \cdot N_{M/K}(M^\times)) &= \overline{\phi_{M/K}}(a \cdot N_{M/K}(M^\times)) \\
&= \phi_{M/K}(a) = \phi_K(a)|_M.
\end{aligned}$$

3.5 Os teoremas de Kronecker-Weber

A igualdade $K^{ab} = K_\pi \cdot K^{un}$ claramente implica o teorema de Kronecker-Weber local, abaixo enunciado.

Teorema 3.5.1 (Teorema de Kronecker-Weber local)**.** *Seja p um número primo e K uma extensão abeliana do corpo dos números p-ádicos $\mathbb{Q}_p$. Então K está contido em uma extensão ciclotômica de $\mathbb{Q}_p$.*

Seja agora K uma extensão galoisiana de $\mathbb{Q}$ com grupo de Galois G. Se $\mathfrak{p}$ for um ideal primo não nulo de $\mathcal{O}_K$, sabemos que existe um único número primo $p \in \mathbb{Z}$ tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Também já temos definido o grupo inercial de $\mathfrak{p}$ sobre $p\mathbb{Z}$ como sendo

$$I(\mathfrak{p}/p\mathbb{Z}) = \{\sigma \in G : \ \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}}, \ \forall\ \alpha \in \mathcal{O}_K\}.$$

Vamos denotar $I(\mathfrak{p}/p\mathbb{Z})$ simplesmente por $I_\mathfrak{p}$. Com apenas mais um lema acerca dos grupos inerciais podemos obter o teorema de Kronecker-Weber global.

Lema 3.5.2. *Seja K uma extensão galoisiana de $\mathbb{Q}$. Se $G = \mathrm{Gal}(K/\mathbb{Q})$, então G é gerado pelos subgrupos de inércia dos ideais primos $\mathfrak{p}$ de $\mathcal{O}_K$ que se ramificam na extensão $K/\mathbb{Q}$.*

Demonstração: Seja H o subgrupo de G gerado por tais subgrupos, e seja M o corpo fixo por H em K. Então $K^{I_\mathfrak{p}} \supseteq M$, qualquer que seja o ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$. Como $\mathfrak{p}$ se ramifica na extensão $K/\mathbb{Q}$, então $\mathfrak{p} \cap \mathcal{O}_M$ não se ramifica na extensão $M/\mathbb{Q}$. Assim, M é uma extensão não ramificada de $\mathbb{Q}$. Como toda extensão própria

de $\mathbb{Q}$ ramifica pelo menos um primo (veja o teorema 34 e o corolário 3 do teorema 37 de [6]), segue que $M = \mathbb{Q} \Rightarrow H = G$. □

Agora podemos enunciar e demonstrar o teorema de Kronecker-Weber global:

Teorema 3.5.3 (Teorema de Kronecker-Weber global)**.** *Se K for uma extensão abeliana de $\mathbb{Q}$, então K está contido em algum corpo ciclotômico.*

Demonstração: Seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ e seja p um número primo tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Denote por $K_\mathfrak{p}$ o completamento de K com respeito a alguma valorização $|\cdot|_\mathfrak{p}$ em $\mathfrak{p}$. Então $K_\mathfrak{p}$ é uma extensão abeliana de $\mathbb{Q}_p$. Pelo Teorema de Kronecker-Weber local, $K_\mathfrak{p}$ está contido em algum corpo ciclotômico de $\mathbb{Q}_p$. Denote tal corpo ciclotômico por $\mathbb{Q}_p(u_p, v_p)$, onde u_p é uma raiz p^{s_p}-ésima da unidade e v_p é uma raiz da unidade de ordem prima com p.

Como apenas um número finito de primos se ramifica numa extensão finita de $\mathbb{Q}$, seja L a extensão ciclotômica de $\mathbb{Q}$ gerada por todas as raízes p^{s_p}-ésimas da unidade, onde p é um primo que se ramifica na extensão $K/\mathbb{Q}$. Seja também $M = KL$. Como o compósito de extensões abelianas é ainda uma extensão abeliana, então $M/\mathbb{Q}$ é uma extensão abeliana de corpos e, da mesma forma que antes, $M_\mathfrak{q} \subseteq \mathbb{Q}_p(u_p, w_p)$, onde $\mathfrak{q}$ é um ideal de $\mathcal{O}_M$ e w_p é uma raiz da unidade de ordem prima com p. Assim, é suficiente provar o teorema para K no lugar de M, de onde podemos assumir sem perda de generalidade que $K \supseteq L$.

Note inicialmente que $[K : \mathbb{Q}] \geq [L : \mathbb{Q}] = \prod_p \varphi(p^{s_p})$, onde o produtório percorre todos os primos que se ramificam na extensão $K/\mathbb{Q}$ e φ é a função de Euler. Por outro lado, como K é uma extensão abeliana de $\mathbb{Q}$, o grupo inercial $I_\mathfrak{p}$ de um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$ depende unicamente do número primo $p \in \mathbb{Z}$ tais que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Dessa forma, podemos denotá-lo simplesmente por I_p. Como, pelo lema anterior, $\mathrm{Gal}(K/\mathbb{Q})$ é gerado pelos subgrupos de inércia dos ideais primos $\mathfrak{p}$ de $\mathcal{O}_K$ que se ramificam na extensão $K/\mathbb{Q}$, então

$$[K : \mathbb{Q}] = |\operatorname{Gal}(K/\mathbb{Q})| \leq \prod_p |I_p| \leq \prod_p \varphi(p^{s_p}) = [L : \mathbb{Q}].$$

Então $K = L$ e o teorema está demonstrado. □

Deve ser notado que o teorema de Kronecker-Weber global é um teorema específico do corpo dos números racionais, não valendo geralmente para corpos de números arbitrários, mesmo que a extensão seja abeliana de grau 2. De fato, seja d um inteiro livre de quadrados e considere a torre de corpos $\mathbb{Q}(\sqrt[4]{d})/\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Claramente as extensões $\mathbb{Q}(\sqrt[4]{d})/\mathbb{Q}(\sqrt{d})$ e $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ são abelianas de grau 2. Entretanto, o corpo de números $\mathbb{Q}(\sqrt[4]{d})$ não está contido em nenhum corpo ciclotômico. Com efeito, como todo corpo ciclotômico é uma extensão abeliana dos racionais, todo subcorpo dos corpos ciclotômicos é uma extensão galoisiana de $\mathbb{Q}$. Se $\mathbb{Q}(\sqrt[4]{d})$ estivesse contido em algum corpo ciclotômico, então a extensão $\mathbb{Q}(\sqrt[4]{d})/\mathbb{Q}$ seria galoisiana, absurdo.

Capítulo 4

Lei de reciprocidade global de Artin

Iniciamos a demonstração da lei de reciprocidade global de Artin com um estudo um pouco mais profundo da cohomologia dos grupos cíclicos.

4.1 Cohomologia de grupos cíclicos

Seja $G =< \sigma >$ um grupo cíclico de ordem n e seja A um G-módulo. Defina

$$\Delta = 1 - \sigma \qquad \text{e} \qquad N = 1 + \sigma + \cdots + \sigma^{n-1}.$$

Proposição 4.1.1. *Seja A um G-módulo. Se A é escrito aditivamente, então as ações*

$$\Delta: \begin{array}{ccc} A & \to & A \\ a & \mapsto & a - \sigma(a) \end{array} \quad e \quad N: \begin{array}{ccc} A & \to & A \\ a & \mapsto & \mapsto a + \sigma(a) + \cdots + \sigma^{n-1}(a) \end{array}$$

são endomorfismos de A.

Demonstração: Se $a,\ b \in A$, então:

$$\Delta(a+b) = (a+b) - \sigma(a+b) = a + b - \sigma(a) - \sigma(b) = \Delta(a) + \Delta(b)$$

e

$$\begin{aligned} N(a+b) &= (a+b) + \sigma(a+b) + \cdots + \sigma^{n-1}(a+b) \\ &= a + b + \sigma(a) + \sigma(b) + \cdots + \sigma^{n-1}(a) + \sigma^{n-1}(a) \\ &= N(a) + N(b). \end{aligned}$$

□

Claramente, se A é escrito multiplicativamente,

$$\Delta(a) = a \cdot \sigma(a)^{-1} \qquad \text{e} \qquad N(a) = a \cdot \sigma(a) \cdot \ \cdots \ \cdot \sigma^{n-1}(a).$$

Exemplo 4.1.2. *Seja L/K uma extensão galoisiana de corpos de números com grupo de Galois cíclico (escrito multiplicativamente). Neste caso, $N = N_{L/K}$.*

Quando for necessário, escreveremos $\Delta = \Delta_A$ e $N = N_A$. Note que se A é um G-módulo, então $\Delta \circ N = N \circ \Delta = 0$, pois se $a \in A$,

$$\begin{aligned} \Delta(N(a)) &= \Delta(a + \sigma(a) + \cdots + \sigma^{n-1}(a)) \\ &= (a + \sigma(a) + \cdots + \sigma^{n-1}(a)) - (\sigma(a) + \sigma^2(a) + \cdots + a) = 0 \end{aligned}$$

e

$$N(\Delta(a)) = N(a - \sigma(a)) = (a - \sigma(a)) + (\sigma(a) - \sigma^2(a)) + \cdots + (\sigma^{n-1}(a) - a) = 0.$$

Assim, $\mathrm{img}(N) \subseteq \ker(\Delta)$ e $\mathrm{img}(\Delta) \subseteq \ker(N)$. Dessa forma, faz sentido a seguinte definição.

Definição 4.1.3. *Seja A um G-módulo. Definimos os grupos de cohomologia $H^0(A)$ e $H^1(A)$ por*

$$H^0(A) = \frac{\ker(\Delta)}{N(A)} \qquad e \qquad H^1(A) = \frac{\ker(N)}{\Delta(A)}.$$

Definimos também a noção de G-homomorfismo entre G-módulos.

Definição 4.1.4. *Se A e B são G-módulos, um G-homomorfismo é um homomorfismo $f : A \to B$ entre os grupos abelianos A e B tal que $f(\sigma(a)) = \sigma(f(a))$, $\forall\ a \in A$.*

Lema 4.1.5. *Se $f : A \to B$ é um G-homomorfismo de G-módulos, então existem homomorfismos $f_1 : H^1(A) \to H^1(B)$ e $f_2 : H^2(A) \to H^2(B)$.*

Demonstração: Afirmo inicialmente que $f(\Delta_A(a)) = \Delta_B(f(a))$ e que $f(N_A(a)) = N_B(f(a))$, $\forall\ a \in A$. De fato, seja $a \in A$. Então:

- $f(\Delta_A(a)) = f(a - \sigma(a)) = f(a) - f(\sigma(a)) = f(a) - \sigma(f(a)) = \Delta_B(f(a))$.
- $f(N_A(a)) = f(a + \sigma(a) + \cdots + \sigma^{n-1}(a)) = f(a) + f(\sigma(a)) + \cdots + f(\sigma^{n-1}(a)) = = f(a) + \sigma(f(a)) + \cdots + \sigma^{n-1}(f(a)) = N_B(f(a))$.

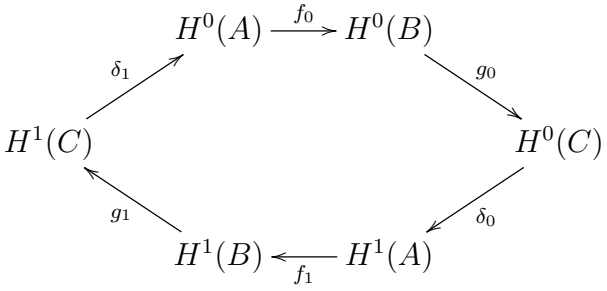
Em particular, $f(\ker(\Delta_A)) \subseteq \ker(\Delta_B)$ e $f(N_A(A)) \subseteq N_B(B)$. Sabendo disto, podemos definir (e estarão bem definidos) os homomorfismos

$$f_0 : \begin{array}{ccc} H^0(A) & \to & H^0(B) \\ a + N_A(A) & \mapsto & f(a) + N_B(B) \end{array} \quad \text{e} \quad f_1 : \begin{array}{ccc} H^1(A) & \to & H^1(B) \\ a + \Delta_A(A) & \mapsto & f(a) + \Delta_B(B). \end{array}$$

□

O lema anterior admite o seguinte corolário, conhecido como *lema do hexágono exato*. Ele será usado logo mais à frente.

Lema 4.1.6. *Seja* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *uma sequência exata de G-módulos e G-homomorfismos. Então existem homomorfismos* δ_0 *e* δ_1 *(denominados homomorfismos de conexão) tal que o hexágono abaixo é exato em cada grupo:*



Demonstração: Seja $c \in \ker(\Delta_C)$. Pela exatidão da sequência, existe $b \in B$ tal que $g(b) = c$. Logo $g(\Delta_B(b)) = \Delta_C(g(b)) = \Delta_C(c) = 0 \Rightarrow \Delta_B(b) \in \ker(g)$. Como $\ker(g) = \mathrm{img}(f)$, existe $a \in A$ tal que $\Delta_B(b) = f(a)$. Como $f(N_A(a)) = N_B(f(a)) = N_B(\Delta_B(b)) = 0$, então $N_A(a) \in \ker(f)$. De novo pela exatidão da sequência, $N_A(a) = 0 \Rightarrow a \in \ker(N_A)$. Dessa forma, podemos assim definir δ_0 por

$$\delta_0(c + N_C(C)) = a + \Delta_A(A).$$

Mostremos que δ_0 está bem definida. Suponha que $c + N_C(C) = c' + N_C(C)$ e que $g(b') = c'$. Afirmo inicialmente que existe $a' \in A$ tal que $\Delta_B(b') = f(a')$. De fato, como $c - c' \in N_C(C)$, existe $c'' \in C$ tal que $c - c' = N_C(c'')$. Logo $0 = \Delta_C(N_C(c'')) = \Delta_C(c - c') = \Delta_C(g(b) - g(b')) = \Delta_C(g(b - b')) = g(\Delta_B(b - b')) \Rightarrow \Delta_B(b - b') \in \ker(g)$. Como $\ker(g) = \mathrm{img}(f)$, existe $a'' \in A$ tal que $\Delta_B(b - b') = f(a'')$. Como $\Delta_B(b - b') = \Delta_B(b) - \Delta_B(b') = f(a) - \Delta_B(b')$, então $\Delta_B(b') = f(a) - f(a'') = f(a - a'')$. Basta agora tomar $a' = a - a''$.

Agora conseguimos mostrar que $a - a' \in \Delta_A(A)$. Como g é sobrejetora, existe $b'' \in B$ tal que $g(b'') = c''$. Assim, $g(b - b' - N_B(b'')) = g(b) - g(b') - g(N_B(b'')) = c - c' - N_C(g(b'')) = c - c' - N_C(c'') = 0 \Rightarrow b - b' - N_B(b'') \in \ker(g)$. Como $\ker(g) = \mathrm{img}(f)$, existe $\widetilde{a} \in A$ tal que $b - b' - N_B(b'') = f(\widetilde{a})$. Aplicando Δ_B de cada lado desta equação, obtemos $\Delta_B(b) - \Delta_B(b') - \Delta_B(N_B(b'')) = \Delta_B(f(\widetilde{a})) \Rightarrow f(a) - f(a') = f(\Delta_A(\widetilde{a})) \Rightarrow f(a - a') = f(\Delta_A(\widetilde{a}))$. Como f é injetora, $a - a' = \Delta_A(\widetilde{a}) \in \Delta_A(A)$ e, portanto, δ_0 está bem definida.

Claro que δ_0 é um homomorfismo, pois em cada passo usamos um homomorfismo da sequência. Analogamente definimos $\delta_1(c + \Delta_C(C)) = a + N_A(A)$, onde $g(b) = c$ e $f(a) = N_B(b)$. A exatidão segue diretamente das propriedades que δ_0 e δ_1 têm, e da hipótese. □

De posse dos grupos de cohomologia de um G-módulo A definimos o seguinte conceito, que nos acompanhará até o final deste capítulo.

Definição 4.1.7. *Seja A um G-módulo. O quociente de Herbrand de A é definido por*

$$q(A) = \frac{|H^1(A)|}{|H^0(A)|}$$

desde que os grupos $H^0(A)$ e $H^1(A)$ sejam ambos finitos. Neste caso dizemos que o quociente de Herbrand de A está definido.

Lema 4.1.8. *Seja $0 \to A \to B \to C \to 0$ uma sequência exata de G-módulos. Se quaisquer dois dos quocientes de Herbrand $q(A)$, $q(B)$ ou $q(C)$ estão definidos, então o terceiro também estará definido e $q(A)q(C) = q(B)$.*

Demonstração: Suponha sem perda de generalidade que $q(A)$ e $q(B)$ estão definidos e seja $i \in \{1, 2\}$. Pelo lema do hexágono exato, $\dfrac{H^i(C)}{\ker(\delta_i)} \simeq \text{img}(\delta_i)$. Como $\ker(\delta_i) = \text{img}(g_i)$, $\dfrac{H^i(C)}{\text{img}(g_i)} \simeq \text{img}(\delta_1)$. Como g_i está definida em um grupo finito e $\text{img}(\delta_i)$ está contida em um grupo finito, $q(C)$ está definido. Em particular, $|H^i(C)| = |\text{img}(g_i)| \cdot |img(\delta_i)|$.

Agora suponha que os seis grupos de cohomologia são finitos. Ainda pelo lema do hexágono exato, comparando as ordens das imagens e dos núcleos, obtemos

$$\begin{aligned} q(A)q(C) &= \frac{|H^1(A)|}{|H^0(A)|} \cdot \frac{|H^1(C)|}{|H^0(C)|} = \frac{|\text{img}(\delta_0)| \cdot |\text{img}(f_1)|}{|\text{img}(\delta_1)| \cdot |\text{img}(f_0)|} \cdot \frac{|\text{img}(g_1)| \cdot |\text{img}(\delta_1)|}{|\text{img}(g_0)| \cdot |\text{img}(\delta_0)|} = \\ &= \frac{|\text{img}(f_1)| \cdot |\text{img}(g_1)|}{|\text{img}(f_0)| \cdot |\text{img}(g_0)|} = \frac{|H^1(B)|}{|H^0(B)|} = q(B). \end{aligned}$$

□

Corolário 4.1.9. *Se $A \subseteq B$ são G-módulos tais que $C = B/A$ é finito. Se $q(A)$ ou $q(B)$ estiver definido, então o outro quociente de Herbrand também estará definido e $q(A) = q(B)$.*

Demonstração: Como, por hipótese, C é finito, pelo lema anterior basta mostrar que $q(C) = 1$. De fato: $q(C) = \dfrac{|H^1(C)|}{|H^0(C)|} = \dfrac{|\ker(N_C)|}{|\text{img}(\Delta_C)|} \cdot \dfrac{|\text{img}(N_C)|}{|\ker(\Delta_C)|} = \dfrac{|C|}{|C|} = 1.$ □

A seção abaixo dá um exemplo do cálculo do quociente de Herbrand.

4.2 O quociente de Herbrand de um módulo de permutação

Sejam d um divisor fixo de $n = |G|$, R um domínio de integridade de característica 0 e $A = \sum_{i=1}^{d} Ru_i$ o R-módulo livre gerado por $u_1, \ldots, u_d$. Suponha que G age em A permutando os elementos da base da seguinte maneira:

$$\sigma(u_i) = \begin{cases} u_{i+1} & \text{se } i < d \\ u_1 & \text{se } i = d. \end{cases}$$

Então σ^d age como a identidade em A. Se denotarmos por $G_A =< \sigma^d >$, então G_A é o subgrupo de índice d em G (lembre-se de que G é cíclico). Com estas notações temos a seguinte

Proposição 4.2.1. *Seja* $md = n$. *Se* $\dfrac{R}{mR}$ *é finito e* A *é como acima, então* $q(A)$ *está definido e* $q(A) = \dfrac{1}{[R : mR]}$. *Em particular, se* $R = \mathbb{Z}$, *então* $q(A) = \dfrac{1}{[\mathbb{Z} : m\mathbb{Z}]} = \dfrac{1}{|G_A|}$.

Demonstração: Calculando os grupos diretamente pela definição, obtemos

(a) $\ker(N) = \left\{ \sum_{i=1}^{d} r_i u_i : \sum_{i=1}^{d} r_i = 0 \right\}$;

(b) $\mathrm{img}(\Delta) = \ker(N)$;

(c) $\ker(\Delta) = R(u_1 + \cdots + u_d)$;

(d) $\mathrm{img}(N) = mR(u_1 + \cdots + u_n)$.

Portanto $H^0(A) \equiv \dfrac{R}{mR}$ e $H^1(A) = 0$, de onde segue a tese. □

Para continuarmos precisamos agora entender o conceito de módulus de um corpo de números, que será dado brevemente na próxima seção. Uma discussão mais aprofundada pode ser encontrada em [12], capítulo 2, seção 3, e em [5], capítulo 2.

4.3 Módulus e grupo ideal de um corpo de números

Começamos com o conceito de valorização em um corpo qualquer.

Definição 4.3.1. *Seja* K *um corpo. Uma valorização em* K *é uma função*

$$|\cdot| : K \to \mathbb{R}$$

que satisfaz:

- $|x| \geq 0, \ \forall\ x \in K$;
- $|x| = 0 \Leftrightarrow x = 0$;
- $|xy| = |x| \cdot |y|, \ \forall\ x,\ y \in K$;
- $|x + y| \leq |x| + |y|, \ \forall\ x,\ y \in K$.

Claramente todo corpo admite a valorização denominada *valorização trivial*, dada por $|x| = 1, \ \forall\ x \in K^{\times}, \ |0| = 0$. Note que se K for um corpo finito, esta é a única valorização possível. Ademais, se colocarmos $d(x, y) = |x - y|$, então o corpo K torna-se um espaço métrico.

Exemplo 4.3.2. *Seja D um domínio de ideais principais com um único ideal maximal $\mathfrak{p} = \pi D$ e corpo de frações K. Podemos definir a valorização $\mathfrak{p}$-ádica de K colocando*

$$|a\pi^k|_{\mathfrak{p}} = c^k,$$

onde $a \in D - \mathfrak{p}$, k é um número inteiro, $c = |\pi|_{\mathfrak{p}}$ é qualquer número real positivo estritamente menor que 1 e extendendo-a de maneira natural a K. Neste exemplo, costuma-se denotar por $K_{\mathfrak{p}}$ o completamento de K com respeito à métrica induzida por esta valorização.

Duas valorizações $|\cdot|_1$ e $|\cdot|_2$ em um corpo K são ditas equivalentes se $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$.

Definição 4.3.3. *Uma valorização $|\cdot|$ em um corpo K é chamada de não arquimediana se $|x+y| \leq \max\{|x|, |y|\}$, $\forall\ x,\ y \in K$. Caso contrário ela é dita arquimediana.*

Assim, uma classe de equivalência de valorizações $\mathfrak{p}$ em um corpo K é chamado de um *primo* de K, ou um *lugar* de K. Um primo é chamado *infinito* se ele contém uma valorização arquimediana. Caso contrário ele é chamado de primo *finito* de K. Como os completamentos de K com respeito a duas valorizações equivalentes são isomorfos, podemos falar então sem ambiguidades sobre o único (a menos de isomorfismo) completamento de K com respeito ao primo $\mathfrak{p}$. Um primo infinito é chamado de *real* se o completamento de K com respeito a $\mathfrak{p}$ for o corpo dos números reais. Caso o completamento de K com respeito ao primo $\mathfrak{p}$ seja isomorfo ao corpo dos números complexos, denominamos tal primo de primo *complexo*.

Assim, podemos apresentar agora a definição de módulus de um corpo K.

Definição 4.3.4. *Um módulus de um corpo K é um produto formal $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$, onde o produtório percorre todos os primos finitos ou reais infinitos de K, no qual o número $n(\mathfrak{p})$ é não negativo para todo primo $\mathfrak{p}$ de K, positivo apenas para um número finito deles e valendo no máximo 1 para os primos reais infinitos de K.*

Na prática,

- tomamos o primo real $\mathfrak{p}$ de K como sendo o ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$, consideramos o mergulho $x \mapsto x_{\mathfrak{p}}$ de K em $K_{\mathfrak{p}} = \mathbb{R}$, e escrevemos $a \equiv^* b \pmod{\mathfrak{p}}$ para indicar que a e b tem o mesmo sinal.
- tomamos o primo finito $\mathfrak{p}$ de K como sendo o ideal primo $\mathfrak{p}$ de K e escrevemos $a \equiv^* b \pmod{\mathfrak{p}^n}$, onde n é um inteiro positivo, se $a \in b(1 + \mathfrak{p}^n(\mathcal{O}_K)_{\mathfrak{p}})$, onde $(\mathcal{O}_K)_{\mathfrak{p}}$ representa a localização do anel de números $\mathcal{O}_K$ de K no ideal primo $\mathfrak{p}$.

Dessa forma, um módulus $\mathfrak{m}$ pode ser olhado como um produto $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$, onde $\mathfrak{m}_0 = \prod_{\mathfrak{p}\text{ finito}} \mathfrak{p}^{n(\mathfrak{p})}$ e $\mathfrak{m}_\infty = \prod_{\mathfrak{p}\text{ real}} \mathfrak{p}^{n(\mathfrak{p})}$. Note que no primeiro caso $\mathfrak{m}_0$ é um ideal

de $\mathcal{O}_K$ e no segundo os expoentes $n(\mathfrak{p})$ valem 0 ou 1, valendo 1 apenas um número finito de vezes.

No caso geral, escrevemos $\alpha \equiv^* \beta \pmod{\mathfrak{m}}$ para dois elementos $\alpha,\ \beta \in K^\times$ se $\alpha \equiv^* \beta \pmod{\mathfrak{p}^{n(\mathfrak{p})}}$ para todos os primos $\mathfrak{p}$ de K tais que $n(\mathfrak{p}) > 0$. Aproveitamos também para fixarmos a seguinte notação:

- $K_{\mathfrak{m}} = \{a/b \in K : a,\ b \in \mathcal{O}_K \text{ e } a\mathcal{O}_K,\ b\mathcal{O}_K \text{ são relativamente primos a } \mathfrak{m}_0\}$;
- $K_{\mathfrak{m},1} = \{\alpha \in K_{\mathfrak{m}} : \alpha \equiv^* 1 \pmod{\mathfrak{m}}\}$.

Vamos agora falar um pouco sobre ideais fracionários:

Definição 4.3.5. *Seja K um corpo de números e considere $\mathcal{O}_K$ seu anel de inteiros. Um ideal fracionário I de $\mathcal{O}_K$ é um $\mathcal{O}_K$-submódulo de K para o qual existe $d \in \mathcal{O}_K - \{0\}$ tal que $dI \subseteq \mathcal{O}_K$. Tal elemento d é chamado de denominador de I.*

Definimos também o produto de dois ideais fracionários I e I' de $\mathcal{O}_K$ como sendo o conjunto $II' = \left\{ \sum_{i=1}^{n} x_i y_i :\ x_i \in I,\ y_i \in I',\ n \in \mathbb{N} \right\}$. Claramente, se I e I' são dois ideais fracionários de $\mathcal{O}_K$ com denominadores d e d', respectivamente, então $I \cap I',\ I + I'$ e II' são todos ideais fracionários de $\mathcal{O}_K$ com denominadores d (ou d'), dd' e dd', respectivamente. Assim sendo, o conjunto de todos os ideais fracionários I de $\mathcal{O}_K$ é um grupo perante a multiplicação acima indicada, denominado *grupo ideal* de K, e denotado por $\mathbf{I}_K$. (Para uma prova deste fato, veja [17], capítulo 3.)

Existe um homomorfismo natural $\iota : K^\times \to \mathbf{I}_K$ dado por $\iota(\alpha) = \alpha\mathcal{O}_K$. Então $\ker(\iota) = \mathcal{O}_K^\times \doteq \mathbf{U}_K$.

Definição 4.3.6. *Seja $\iota : K^\times \to \boldsymbol{I}_K$ o homomorfismo natural acima indicado. Definimos o grupo de classe de K, denotado por $\boldsymbol{C}_K$, como sendo o cokernel de ι, isto é, $\boldsymbol{C}_K = \operatorname{coker}(\iota) = \dfrac{\boldsymbol{I}_K}{\iota(K^\times)}$.*

Pelo teorema 13.8 de [5], o grupo $\mathbf{C}_K$ é sempre finito, e assim temos a sequência exata

$$1 \to \mathbf{U}_K \to K^\times \xrightarrow{\iota} \mathbf{I}_K \to \mathbf{C}_K \to 1.$$

Fixado um módulus $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$, dentaremos por $\mathbf{I}^{\mathfrak{m}} = \mathbf{I}_K^{\mathfrak{m}}$ o subgrupo do grupo ideal de K gerado por todos os ideais primos de $\mathcal{O}_K$ primos com $\mathfrak{m}_0$.

4.4 S-unidades

Nesta seção, L denotará uma extensão galoisiana de um corpo de números K com grupo de Galois $G =< \sigma >$ cíclico.

Seja $\mathfrak{m}$ um módulus para K e assuma que qualquer primo de K que se ramifica em L tem um expoente positivo em $\mathfrak{m}$. Como cada primo de K pode ser visto como um produto de primos de L, o módulus $\mathfrak{m}$ de K pode ser visto como um módulus para L.

Como G opera nos ideais de $\mathcal{O}_L$, então $\mathbf{I}_L$ é um G-módulo. Os primos de L que estão sobre um primo de K são permutados transitivamente por G. Segue que o conjunto de primos de L que não dividem $\mathfrak{m}$ são permutados por G e, portanto, $\mathbf{I}_L^{\mathfrak{m}}$ também é um G-módulo. Calculando diretamente pela definição dos grupos de cohomologia, obtemos a seguinte proposição:

Proposição 4.4.1. *Se $\mathfrak{m}$ for um módulus para K divisível por todos os primos de K que se ramificam em L, então:*

- $H^0(\boldsymbol{I}_L^{\mathfrak{m}}) = \dfrac{\boldsymbol{I}_K^{\mathfrak{m}}}{N(\boldsymbol{I}_L^{\mathfrak{m}})}$;
- $H^1(\boldsymbol{I}_L^{\mathfrak{m}}) = 1$;
- $H^0(L^\times) = \dfrac{K^\times}{N(L^\times)}$;
- $H^1(L^\times) = 1$.

Considere agora o homomorfismo

$$j_{\mathfrak{m}} : \begin{array}{ccc} \mathbf{I}_L & \to & \mathbf{I}_{\mathfrak{m}}^L \\ \mathfrak{B} & \mapsto & \begin{cases} \mathfrak{B} & \text{se } \mathfrak{B} \nmid \mathfrak{m} \\ 1 & \text{se } \mathfrak{B} | \mathfrak{m}. \end{cases} \end{array}$$

A imagem de um elemento $\mathfrak{A} \in \mathbf{I}_L$ por $j_{\mathfrak{m}}$ é o produto de fatores primos relativamente primos a $\mathfrak{m}$. Lembrando que a função $\iota : L^\times \to \mathbf{I}_L$ é a função que associa α ao ideal fracionário $\iota(\alpha) = \alpha\mathcal{O}_L = (\alpha)$, seja $f_m : L^\times \to \mathbf{I}_L^{\mathfrak{m}}$ a composta $j_{\mathfrak{m}} \circ \iota$. Note que os grupos mencionados aqui são G-módulos e que as funções aqui descritas são G-homomorfismos. Agora seja S um conjunto finito de primos dividindo $\mathfrak{m}$ e seja $L^S = \ker(f_{\mathfrak{m}})$. Então é fácil ver que

$$L^S = \{\alpha \in L^\times : \iota(\alpha) \text{ e divisível apenas por primos em } S\}.$$

Caso $S \subseteq S_\infty$ (o conjunto dos primos infinitos de L), então $L^S = \mathbf{U}_L = \mathcal{O}_L^\times$.

Definição 4.4.2. *O conjunto L^S acima descrito é chamado de grupo das S-unidades de L.*

Com isto temos o seguinte lema:

Lema 4.4.3. *Se $q(\boldsymbol{U}_L)$ e $q(\ker(j_{\mathfrak{m}}))$ estão definidos, então $q(L^S) = q(\boldsymbol{U}_L)q(\ker(j_{\mathfrak{m}}))$.*

Demonstração: O fato de $1 = f_{\mathfrak{m}}(L^S) = j_{\mathfrak{m}}(\iota(L^S))$ nos dá uma sequência exata $1 \to \iota(L^S) \to \ker(j_{\mathfrak{m}}) \to C \to 1$, para algum grupo C, que é finito, pois

$$C \cong \frac{\ker(j_{\mathfrak{m}})}{\iota(L^S)} \cong \frac{\ker(j_{\mathfrak{m}})}{\iota(L^\times) \cap \ker(j_{\mathfrak{m}})} \cong \frac{\iota(L^\times)\ker(j_{\mathfrak{m}})}{\iota(L^\times)},$$

que é um subgrupo do grupo de classes de L, o qual nós sabemos ser finito. Pelo lema 4.1.8 e pelo corolário 4.1.9 concluímos que $q(\iota(L^S)) = q(\ker(j_{\mathfrak{m}}))$. Usando a sequência exata $1 \to \mathbf{U}_L \to L^S \to \iota(L^S) \to 1$, concluímos que

$$q(L^S) = q(\mathbf{U}_L)q(\iota(L^S)) = q(\mathbf{U}_L)q(\ker(j_{\mathfrak{m}})).$$

□

4.5 O quociente de Herbrand $q(\mathbf{U}_L)$

Para calcularmos o quociente de Herbrand $q(\mathbf{U}_L)$ precisamos antes da seguinte proposição técnica, cuja prova pode ser encontrada em [5], p. 175 - 176.

Proposição 4.5.1. *Seja L tendo s primos reais $\mathfrak{B}_1, \ldots, \mathfrak{B}_r$ e r primos complexos $\mathfrak{B}_{r+1}, \ldots, \mathfrak{B}_{r+s}$. Então existem elementos $w_1, \ldots, w_{r+s}$ de $\boldsymbol{U}_L$ em correspondência biunívoca com os primos infinitos $\mathfrak{B}_i$ tais que*

- *G permuta os w_i que correpondem aos primos $\mathfrak{B}_i$ que se estendem a um dado primo infinito $\mathfrak{p}$ de K;*
- $\prod_{i=1}^{r+s} w_i = 1$;
- *subgrupo $W =< w_1, \ldots, w_{r+s} >$ tem índice finito em $\boldsymbol{U}_L$.*

Com tal proposição em mãos podemos calcular o quociente de Herbrand de $q(\mathbf{U}_L)$.

Teorema 4.5.2. *Seja r_0 o número de primos infinitos de K que ramificam em L. Então $q(\boldsymbol{U}_L) = \dfrac{[L:K]}{2^{r_0}}$.*

Demonstração: Para um primo infinito $\mathfrak{p}$ de K e um primo $\mathfrak{B}$ de L contendo $\mathfrak{p}$, defina $d_{\mathfrak{p}} = [G : G(\mathfrak{B})]$. Seja também $A_{\mathfrak{p}} = \sum_{i=1}^{d_{\mathfrak{p}}} \mathbb{Z}u_{i,\mathfrak{p}}$, onde cada $u_{i,\mathfrak{p}}$ corresponde a um primo $\mathfrak{B}_i$ (como na proposição acima) estendendo $\mathfrak{p}$ de tal forma que G permuta os elementos da base assim como G permuta os $\mathfrak{B}_i$. Assim temos a sequência exata

$$0 \to \mathbb{Z} \xrightarrow{g} \sum_{\mathfrak{p}|\infty} A_{\mathfrak{p}} \xrightarrow{h} W \to 1,$$

onde $g(z) = \sum_i \sum_{\mathfrak{p}} u_{i,\mathfrak{p}}$ e h é definido como sendo o G-homomorfismo que manda cada elemento da base $u_{i,\mathfrak{p}}$ no w_j divisor de $\mathfrak{B}_j$. A exatidão da sequência segue do segundo item da proposição anterior.

Agora, sabemos que $q(W)q(\mathbb{Z}) = q\left(\sum_{\mathfrak{p}|\infty} A_{\mathfrak{p}}\right) = \prod_{\mathfrak{p}} q(A_{\mathfrak{p}})$.

Como a ação de G em $\mathbb{Z}$ é a trivial, segue da proposição 4.2.1 que $q(\mathbb{Z}) = \frac{1}{|G|}$. A mesma proposição nos dá $q(A_{\mathfrak{p}}) = \frac{1}{|G(\mathfrak{B})|}$ quando $\mathfrak{B}$ contém $\mathfrak{p}$.

Agora, se $\mathfrak{p}$ é um primo de K que não ramifica, então existem $[L:K]$ extensões de $\mathfrak{p}$ em L e então $G(\mathfrak{B}) = 1$. Quando $\mathfrak{p}$ ramifica em L, então existem $\frac{[L:K]}{2}$ extensões e, portanto, $G(\mathfrak{B})$ tem ordem 2. Segue que $q(W) = \frac{1}{2^{r_0}}$, onde r_0 é o número de primos de K que ramificam em L. Do fato de que W tem índice finito em $\mathbf{U}_L$ concluímos que $q(W) = q(\mathbf{U}_L)$. □

Calculamos também o quociente de Herbrand de $q(L^S)$.

Teorema 4.5.3. *Seja S o conjunto dos primos finitos de K dividindo o módulus $\mathfrak{m}$. Assuma que $\mathfrak{m}$ é divisível por todos os primos de K que ramificam em L. Então* $q(L^S) = \dfrac{[L:K]}{\prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}} f_{\mathfrak{p}}}$.

Demonstração: Para determinarmos $q(L^S)$ precisamos primeiramente determinar $q(\ker(j_{\mathfrak{m}}))$.

Sabemos que $\ker(j_{\mathfrak{m}})$ é o grupo abeliano livre dos primos finitos em S. Para cada primo finito $\mathfrak{p}$ de K que é divisível por algum primo em S, denote por $\mathbf{I}(\mathfrak{p})$ o subgrupo de $\ker(j_{\mathfrak{m}})$ gerado pelos divisores primos de $\mathfrak{p}$ em L. Então $\ker(j_{\mathfrak{m}}) = \prod_{\mathfrak{p}} \mathbf{I}(\mathfrak{p})$ e $q(\ker(j_{\mathfrak{m}})) = \prod_{\mathfrak{p}} q(\mathbf{I}(\mathfrak{p}))$.

Seja $\mathfrak{p}\mathcal{O}_L = (\mathfrak{B}_1 \cdots \mathfrak{B}_g)^e$ e $N_{L/K}(\mathfrak{B}_i) = \mathfrak{p}^f$. Como G age transitivamente nos $\mathfrak{B}_i$, temos

- $\ker(N_{\mathbf{I}_{\mathfrak{p}}}) = \left\{\prod \mathfrak{B}_i^{a_i} : \sum a_i = 0\right\}$;
- $\mathrm{img}(\Delta_{\mathbf{I}_p}) = \ker(N_{\mathbf{I}_{\mathfrak{p}}})$;
- $\ker(\Delta_{\mathbf{I}_{\mathfrak{p}}}) =< \mathfrak{D} >$, onde $\mathfrak{D} = \mathfrak{B}_1 \cdots \mathfrak{B}_g$;
- $\mathrm{img}(N_{\mathbf{I}_{\mathfrak{p}}}) =< \mathfrak{p}^f >=< \mathfrak{D}^{ef} >$.

Segue que $q(\mathbf{I}(\mathfrak{p})) = \frac{1}{ef} = \frac{1}{e_{\mathfrak{p}} f_{\mathfrak{p}}}$. Assim $q(\ker(j_{\mathfrak{m}})) = \dfrac{1}{\prod_{\mathfrak{p}|\mathfrak{m}_0} e_{\mathfrak{p}} f_{\mathfrak{p}}}$, onde $\mathfrak{m}_0$ é a parte finita de $\mathfrak{m}$. O resultado segue então do lema 4.4.3. □

4.6 A norma de um módulus

De novo, L será uma extensão galoisiana de um corpo de números K e com grupo de Galois $G =< \sigma >$ cíclico.

Definição 4.6.1. *Seja $\mathfrak{m}$ um módulus de K. Definimos $a(\mathfrak{m}) = [K^\times : N(L^\times)K_{\mathfrak{m},1}]$.*

Lema 4.6.2. *Se $\mathfrak{m}$ e $\mathfrak{n}$ são módulus relativamente primos, então $a(\mathfrak{mn}) = a(\mathfrak{m})a(\mathfrak{n})$.*

Demonstração: A função $\alpha \to (\alpha K_{\mathfrak{m},1},\ \alpha K_{\mathfrak{n},1})$ induz um isomorfismo

$$\frac{K^\times}{K_{\mathfrak{mn},1}} \to \frac{K^\times}{K_{\mathfrak{m},1}} \times \frac{K^\times}{K_{\mathfrak{n},1}},$$

o qual, por sua vez, induz o homomorfismo sobrejetor

$$f:\ \frac{K^\times}{K_{\mathfrak{mn},1}} \to \frac{K^\times}{N(L^\times)K_{\mathfrak{m},1}} \times \frac{K^\times}{N(L^\times)K_{\mathfrak{n},1}}.$$

Assim, basta mostrarmos que $\ker(f) = \dfrac{N(L^\times)K_{\mathfrak{mn},1}}{K_{\mathfrak{mn},1}}$.

Suponha que $\alpha K_{\mathfrak{mn},1} \in \ker(f)$. Então existem $\beta_1,\ \beta_2 \in L^\times$ tais que

$$\alpha \equiv N(\beta_1) \pmod{\mathfrak{m}}, \qquad \alpha \equiv N(\beta_2) \pmod{\mathfrak{n}}.$$

Olhando $\mathfrak{m}$ e $\mathfrak{n}$ como módulus para L, eles continuam sendo relativamente primos. Logo existe $\beta \in L^\times$ tal que

$$\beta \equiv \beta_1 (\mathrm{mod}\ \mathfrak{m}), \qquad \beta \equiv \beta_2 (\mathrm{mod}\ \mathfrak{n}).$$

Portanto $\beta\beta_1^{-1} \in L_{\mathfrak{m},1}$ e $\beta\beta_2^{-1} \in L_{\mathfrak{n},1}$. Como $N(L_{\mathfrak{m},1}) \subseteq K_{\mathfrak{m},1}$, para qualquer módulus $\mathfrak{m}$ de K, concluímos que $N(\beta)N(\beta_1)^{-1} \in K_{\mathfrak{m},1}$ e que $N(\beta)N(\beta_2)^{-1} \in K_{\mathfrak{n},1}$. Seguirá que $\alpha N(\beta)^{-1} \equiv 1 \pmod{\mathfrak{m}}$ e que $\alpha N(\beta)^{-1} \equiv 1 \pmod{\mathfrak{n}}$. Em particular, isto implica que $\alpha N(\beta)^{-1} \in K_{\mathfrak{mn},1}$, e, portanto, $\alpha \in N(L^\times)K_{\mathfrak{mn},1}$. □

Dessa forma, o lema provado agora reduz o cálculo de $a(\mathfrak{m})$ para um módulus $\mathfrak{m}$ divisível por apenas um primo. Assim, vamos considerar $\mathfrak{m} = \mathfrak{p}^n$ com $n \geq 1$. O caso no qual $\mathfrak{p}$ é um primo infinito será tratado agora:

Lema 4.6.3. *Se $\mathfrak{p}$ é um primo infinito de K, então $a(\mathfrak{p}) = e_\mathfrak{p}$, o índice de ramificação de $\mathfrak{p}$ em L.*

Demonstração: Seja $\mathfrak{B}_1, \ldots, \mathfrak{B}_g$ os primos de L estendendo $\mathfrak{p}$. Suponha que $\mathfrak{p}$ ramifica em L. Então todos os $\mathfrak{B}_i$ são primos complexos e, se $\alpha \in L^\times$, então $N_{L/K}(\alpha) = \prod_i N_{L_{\mathfrak{B}_i}/K_\mathfrak{p}}(\alpha)$, uma vez que a norma global é o produto das normas locais. Cada completamento de L é $\mathbb{C}$ e a norma no corpo real $K_\mathfrak{p}$ deve ser positiva. Logo $N_{L/K}(L^\times) \subseteq K_{\mathfrak{m},1}$ e portanto $\dfrac{K^\times}{K_{\mathfrak{m},1}}$ tem ordem $2 = e_\mathfrak{p}$.

Agora suponha que $\mathfrak{p}$ e real e tem apenas extensões reais a L. Então $K_{\mathfrak{m},1}$ é o conjunto dos elementos de K que são positivos em $\mathfrak{p}$ e todas as suas extensões locais têm grau 1; logo $N_{L_{\mathfrak{B}_i}/K_\mathfrak{p}}(\alpha) = \alpha_{\mathfrak{B}_i}$, a imagem de α em $\mathbb{R}$ pelo mergulho correspondente ao $\mathfrak{B}_i$. Como existe α tal que α é positivo em todos os primos $\mathfrak{B}_j$ com $j \neq 1$ e negativo em $\mathfrak{B}_1$, $N_{L/K}(\alpha) < 0$ e portanto $N(L^\times)K_{\mathfrak{m},1} = K^\times$. Segue que $a(\mathfrak{m}) = 1 = e_\mathfrak{p}$ neste caso. Caso $\mathfrak{p}$ seja complexo, $K_{\mathfrak{m},1} = K^\times$ e $a(\mathfrak{m}) = e_p = 1$. □

Seja agora $\mathfrak{m} = \mathfrak{p}^n$, onde $\mathfrak{p}$ é um primo finito de K e n é um inteiro positivo. Seja $\mathfrak{B}$ um dos primos de L acima de $\mathfrak{p}$.

Lema 4.6.4. *Seja $m = \mathfrak{p}^n$ um módulus para K com $\mathfrak{p}$ um primo finito. Então*

- $[K^\times : N(L^\times)K_\mathfrak{m}] = f_\mathfrak{p}$;
- $a(\mathfrak{m}) = f_\mathfrak{p}[K_\mathfrak{m} : (K_\mathfrak{m} \cap N(L^\times))K_{\mathfrak{m},1}]$.

Demonstração: Como $\mathfrak{m} = \mathfrak{p}^n$, segue que $K_\mathfrak{m}$ é o conjunto das unidades do anel local $R_\mathfrak{p}$. Seja π é um gerador do ideal maximal $\mathfrak{p}$ de $R_\mathfrak{p}$. Então todo elemento não nulo de K é da forma $\pi^a u$, onde $u \in K_\mathfrak{m}$.

Nós sabemos que $N(\mathfrak{B}) = (\pi^f)$. Portanto, elementos de $N(L^\times)$ têm a forma $\pi^{fb}u$, onde $u \in K_\mathfrak{m}$. Segue que

$$\frac{K^\times}{K_\mathfrak{m}N(L^\times)} \cong \frac{<\pi> K_\mathfrak{m}}{<\pi^f> K_\mathfrak{m}} \cong \frac{<\pi>}{<\pi^f>},$$

o qual tem ordem $f = f_\mathfrak{p}$, conforme diz a primeira parte.

Já a fatoração de $a(\mathfrak{m})$ pode ser obtida a partir dos índices da seguinte cadeia de subgrupos:

$$N(L^\times)K_{\mathfrak{m},1} \subseteq N(L^\times)K_\mathfrak{m} \subseteq K^\times.$$

O segundo índice é $f_\mathfrak{p}$ pela primeira parte. Para terminar, basta observar que existe um isomorfismo $\dfrac{K_\mathfrak{m}}{(K_\mathfrak{m} \cap N(l^\times))K_{\mathfrak{m},1}} \cong \dfrac{N(L^\times)K_\mathfrak{m}}{N(L^\times)K_{\mathfrak{m},1}}$, induzido pela inclusão de $K_\mathfrak{m}$ em $N(L^\times)K_\mathfrak{m}$. □

4.7 A lei de reciprocidade global

Seja L/K uma extensão galoisisana de corpos de números com grupo de Galois G. Para enunciarmos a lei de reciprocidade global de Artin, precisamos antes da definição da *função de Artin*.

Suponha que $\mathfrak{p}$ seja um primo de $\mathcal{O}_K$ que não se ramifica em L/K. Seja $\mathfrak{B}$ um primo de $\mathcal{O}_L$ acima de $\mathfrak{p}$. Como $\mathfrak{p}$ não se ramifica, o grupo de decomposição $D(\mathfrak{B}/\mathfrak{p})$ é um subgrupo cíclico de $\mathrm{Gal}(L/K)$ gerado por, digamos, σ. Tal elemento σ é denotado por $\left[\dfrac{L/K}{\mathfrak{B}}\right]$. Se $\mathfrak{B}$ e $\mathfrak{B}'$ são dois ideais primos de $\mathcal{O}_L$ contendo $\mathfrak{p}$,

então $\left[\frac{L/K}{\mathfrak{B}}\right] = \left[\frac{L/K}{\mathfrak{B}'}\right]$, de onde podemos definir o automorfismo de Frobenius da extensão de corpos globais L/K com relação ao primo $\mathfrak{p}$ de $\mathcal{O}_K$ como sendo $\left[\frac{L/K}{\mathfrak{B}}\right]$, para qualquer ideal primo $\mathfrak{B}$ de $\mathcal{O}_L$ acima de $\mathfrak{p}$. Tal elemento será denotado por $(L/K, \mathfrak{p})$.

Agora podemos definir a função de Artin como segue: seja inicialmente S um conjunto de ideais primos de $\mathcal{O}_K$ contendo todos os primos que ramificam na extensão L/K. Se denotarmos por $\mathbf{I}_K^S$ o subgrupo de $\mathbf{I}_K$ gerado por todos os ideais primos que não estão em S, segue que um elemento de $\mathbf{I}_K^S$ é da forma $\mathfrak{A} = \prod_{\substack{\mathfrak{p} \text{ primo} \\ p \notin S}} \mathfrak{p}^{a(\mathfrak{p})}$.

Assim, podemos definir a função de Artin por

$$\begin{array}{rccc} \varphi: & \mathbf{I}_K^S & \to & \mathrm{Gal}(L/K) \\ & \mathfrak{A} & \mapsto & \prod_{\substack{\mathfrak{p} \text{ primo} \\ p \notin S}} (L/K, \mathfrak{p})^{a(\mathfrak{p})}. \end{array}$$

Definição 4.7.1. *Diremos que a lei de reciprocidade vale para a tripla $(L, K, \mathfrak{m})$ se L é uma uma extensão abeliana de K e $\mathfrak{m}$ é um módulus para K tal que $\iota(K_{\mathfrak{m},1}) \subseteq \ker(\varphi_{L/K})$.*

Começemos com alguns lemas simples:

Lema 4.7.2. *Se a lei de reciprocidade vale para a tripla $(L, K, \mathfrak{m})$ e se $\mathfrak{m}$ é divisível por todos os primos de K que ramificam em L, então $\ker(\varphi_{L/K}) = N(\boldsymbol{I}_L^{\mathfrak{m}})\iota(K_{\mathfrak{m},1})$.*

Demonstração: Como $N(\mathbf{I}_L^{\mathfrak{m}}) \subseteq \ker(\varphi_{L/K})$, pela lei de reciprocidade $N(\mathbf{I}_L^{\mathfrak{m}})\iota(K_{\mathfrak{m},1}) \subseteq \ker(\varphi_{L/K}) \subseteq \mathbf{I}_K^{\mathfrak{m}}$.

Segue que o índice do primeiro grupo desta inclusão é pelo menos $[L : K]$, enquanto que o índice de $\ker(\varphi_{L/K})$ é exatamente $[L : K]$. Segue que os dois grupos são iguais. □

Lema 4.7.3. *Sejam a e r inteiros maiores que 1, e seja q um número primo. Então existe um número primo p tal que a ordem de a módulo p é q^r.*

Demonstração: Considere o polinômio $g(X) = \dfrac{X^q - 1}{X - 1} = X^{q-1} + X^{q-2} + \cdots + 1 = (X-1)^{q-1} + \cdots + \binom{q}{t}(X-1)^{t-1} + q$.

Note que se $n \geq 2$, então $g(n) \geq 3 \Rightarrow g(n)$ tem um divisor primo. Seja p um divisor primo de $g(a^{q^{r-1}}) = g$. Se p não divide o denominador $a^{q^{r-1}} - 1$, então r tem que ser o menor inteiro tal que $a^{q^r} \equiv 1 \pmod{p}$. Então esta escolha para p funciona.

Suponhamos agora que $p | a^{q^{r-1}} - 1$. Então (pela forma de como escrevemos $g(X)$), $p = q$. Vamos provar que g não é potência de primo, de onde poderemos escolher um outro primo divisor de g no qual podemos aplicar o primeiro caso.

Suponha inicialmente que $q > 2$. Então tanto $(X-1)^{q-1}$ quanto $\binom{q}{t}(X-1)^{t-1}$, $t \neq 1$ é divisível por t^2, dado que q divide o coeficiente binomial. Como $a \geq 2$, então $q \neq g$. Então g não é uma potência de q e poderemos fazer uma outra escolha de p.

Finalmente, suponha $q = 2$. Então $g = (a^{2^{r-1}}-1)+2 = a^{2^{r-1}}+1$. Precisamos mostrar que g não é uma potência de 2. Claro que a precisa ser ímpar para que g seja uma potência de 2. Mas neste caso $(a = 2k+1)$, obtemos $g = (2k+1)^{2^{r-1}}+1 \equiv 2(\text{mod } 4)$. Como $g \neq 2$ já que $r \geq 2$, g não é uma potência de 2 e o lema está provado. □

Definição 4.7.4. *Dizemos que dois elementos σ e τ de um grupo abeliano são independentes se $<\sigma> \cap <\tau> = 1$. Dizemos que dois inteiros a e b relativamente primos a m são independentes módulo m se as classes residuais de a e de b são independentes no grupo multiplicativo dos elementos invertíveis módulo m.*

Lema 4.7.5. *Seja $n = q_1^{r_1} \cdots q_s^{r_s}$ a fatoração do inteiro n como produto de primos distintos e seja $a > 1$ um inteiro. Então existem infinitos inteiros livre de quadrados $m = p_1 \cdots p_s p_1' \cdots p_s'$ tais que a ordem de a módulo m é divisível por n. Também existe um inteiro b cuja ordem módulo m é divisível por n e tal que a e b são independentes módulo m. Além disso, o menos divisor primo de m pode ser tomado tão grande quanto se queira.*

Demonstração: Para cada $r \geq r_1$ e $r \geq 2$, existe um primo p_i tal que a tem ordem $q_i^{r_i}$ módulo p_i pelo lema anterior. Se r cresce, p_i também cresce, e a ordem de a módulo p_i é divisível por $q_i^{r_i}$.

Agora sejam $p_1, \ldots, p_s$ primos distintos e suficientemente grandes tais que a ordem de a módulo p_i seja $q_i^{r_i'}$ com $r_i' \geq r_i$. Sejam $p_1', \ldots, p_s'$ primos distintos ainda maiores tais que a tem ordem $q_i^{r_i''}$ módulo p_i', com $r_i'' \geq r_i'$. Então $m = p_1 \cdots p_s p_1' \cdots p_s'$ é livre de quadrados e n divide a ordem de a módulo m. Seja b um inteiro tal que $b \equiv a \pmod{p_1 \cdots p_s}$ e tal que $b \equiv 1 \pmod{p_1' \cdots p_s'}$.

Então n divide a ordem de b módulo m Para mostrarmos que a e b são independentes , suponha que existem inteiros u e v tais que $a^u b^v \equiv 1(\text{mod } m)$. Então $1 \equiv a^u b^v \equiv a^u(\text{mod } p_1' \cdots p_s')$. Portanto $q_i^{r_i''}$ divide u e, logo, $a^u \equiv 1(\text{mod } m)$. Segue que $b^v \equiv 1(\text{mod } m)$ e, sendo assim, a e b são independentes módulo m. □

Assim conseguimos provar a seguinte proposição:

Proposição 4.7.6. *Seja L/K uma extensão abeliana de grau n e seja s um inteiro positivo. Seja $\mathfrak{p}$ um ideal primo em $\mathcal{O}_K$ que não se ramifica em L. Então existe um inteiro positivo m relativamente primo a s e a $\mathfrak{p}$ com as seguintes propriedades:*

- *Se θ_m é uma raiz primitiva m-ésima da unidade e $E = K(\theta_m)$, então $\varphi_{L/K}(\mathfrak{p})$ tem ordem divisível por n;*
- *$L \cap E = K$;*
- *existe um automorfismo $\tau \in \text{Gal}(E/K)$ cuja ordem é divisível por n e que é independente de $\varphi_{E/K}(\mathfrak{p})$.*

Demonstração: Nós aplicaremos o lema anterior usando $a = N_{K/\mathbb{Q}}(\mathfrak{p})$. O corpo L tem apenas um número finito de subcorpos. Logo existe uma raiz M-ésima da unidade θ_M tal que $\mathbb{Q}(\theta_M)$ contém todo subcorpo ciclotômico de L. Pelo lema anterior, existe m tal que todo divisor primo de m é maior que Ms. Assim $\mathbb{Q}(\theta_M) \cap \mathbb{Q}(\theta_m) = \mathbb{Q}$ e, portanto, $L \cap \mathbb{Q}(\theta_m) = \mathbb{Q}$.

Tomando-se $E = K(\theta_m)$, obtemos o item (b).

Escreva $\sigma = \varphi_{E/K}(\mathfrak{p})$. Então $\sigma(\theta_m) = \theta_m^{N(\mathfrak{p})} = \theta_m^a$, donde obtemos o item (a). Finalmente, tomando b como no lema anterior, o automorfismo $\tau(\theta_m) = \theta_m^b$ de $\mathbb{Q}(\theta_m)$ tem ordem divisível por n e é independente de σ. Desde que $K \cap \mathbb{Q}(\theta_m) = \mathbb{Q}$, o automorfismo τ se estende a um elemento de $\mathrm{Gal}(E/K)$ de mesma ordem, de onde obtemos o item (c). □

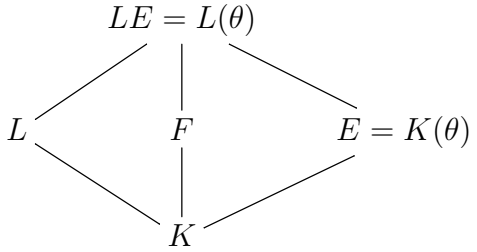
Este lema é o passo técnico crucial para a demonstração da lei de reciprocidade global para extensões cíclicas.

Lema 4.7.7 (Lema de Artin)**.** *Seja L uma extensão cíclica de K, s um inteiro positivo e $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ que não ramifica em L. Então existe um inteiro positivo m e uma extensão F de K tal que:*

- $L \cap F = K$;
- $L \cap K(\theta_m) = K$, *onde θ_m é uma raiz m-ésima da unidade;*
- $L(\theta_m) = F(\theta_m)$;
- $\mathfrak{p}$ *se decompõe completamente em F.*

Demonstração: Seja m como no resultado anterior e seja $E = K(\theta)$. Então $L(\theta) = LE$ e $L \cap E = K$. Dessa forma, o segundo item da proposição anterior também vale e $\mathrm{Gal}(L(\theta)/K) = \mathrm{Gal}(L/K) \times \mathrm{Gal}(E/K)$.

Seja σ um gerador de $\mathrm{Gal}(L/K)$ e seja τ um elemento satisfazendo o item c da proposição anterior. Assim, σ é idependente de $\varphi_{L/K}(\mathfrak{p})$. Seja H o subgrupo gerado por $\sigma \times \tau$ e por $\varphi_{L/K}(\mathfrak{p}) \times \varphi_{E/K}(\mathfrak{p})$, e seja F o subcorpo de LE fixo por H. Temos assim o seguinte diagrama:



Segue que $\varphi_{LE/K}(\mathfrak{p}) = \varphi_{L/K}(\mathfrak{p}) \times \varphi_{E/K}(\mathfrak{p})$. Este elemento gera o grupo de decomposição em $\mathrm{Gal}(LE/K)$ de um primo de LE sobre $\mathfrak{p}$ e então o grupo de decomposição está contido em H. O automorfismo de Frobenius de $\mathfrak{p}$ para a

extensão F/K é a identidade, desde que F é o corpo fixo por H e também porque $\mathrm{res}_F(\varphi_{LE/K}(\mathfrak{p})) = 1$.

Segue que $\mathfrak{p}$ se decompõe completamente em F, provando assim o quarto item.

O corpo $F(\theta) = FE$ é o corpo fixo por $H \cap (\mathrm{Gal}(L/K) \times 1)$. Afirmo que este grupo é a identidade e isto provará o terceiro item.

Suponha que tenhamos inteiros u e v tais que $(\sigma \times \tau)^u(\varphi_{L/K}(\mathfrak{p}) \times \varphi_{E/K}(\mathfrak{p}))^v \in \mathrm{Gal}(L/K) \times 1$.

Então $\tau^u \in < \varphi_{E/K}(\mathfrak{p}) > \Rightarrow \tau^u = 1$, pela hipótese de independência. Segue que $n|u$ e então $\sigma^u = 1$ pois a ordem de σ é $n = [L : K]$. Assim $\varphi_{E/K}(\mathfrak{p})^v = 1$ e portanto $n|v$. Logo $\varphi_{L/K}(\mathfrak{p})^v = 1$ e portanto o único elemento na interseção é a identidade.

Pela definição de H, temos o primeiro item, e como $L \cap F$ é a parte fixa por H e a restrição de H a L contém $\mathrm{res}_L\, \sigma \times \tau = \sigma$ que gera $\mathrm{Gal}(L/K)$, temos $L \cap F = K$. □

Teorema 4.7.8. *Seja L uma extensão cíclica de K e seja $\mathfrak{m}$ um módulus para K divisível por todos os primos que ramificam em L. Seja $\boldsymbol{C}^{\mathfrak{m}} = \dfrac{\boldsymbol{I}_K^{\mathfrak{m}}}{N_{L/K}(I_L^{\mathfrak{m}})\iota(K_{\mathfrak{m},1})}$. Suponha que $|\boldsymbol{C}^{\mathfrak{m}}| = [L : K]$. Então vale a lei de reciprocidade para $(L, K, \mathfrak{m})$.*

Demonstração: Mostraremos que $\ker(\varphi_{L/K}|_{\mathbf{I}_K^{\mathfrak{m}}}) \subseteq \iota(K_{\mathfrak{m},1})N(\mathbf{I}_L^{\mathfrak{m}})$. A igualdade valerá pois ambos os grupos tem índice $[L : K]$ em $\mathbf{I}_K^{\mathfrak{m}}$.

Seja $\mathfrak{A}$ um ideal em $\mathbf{I}_K^{\mathfrak{m}}$ tal que $\varphi_{L/K}(\mathfrak{A}) = 1$. Fatore $\mathfrak{A} = \prod_{i=1}^{r} \mathfrak{p}_1^{a_i}$.

Os primos $\mathfrak{p}_i$ são não ramificados em L, pois todos os primos que se ramificam dividem $\mathfrak{m}$ e $\mathfrak{A}$ é primo com $\mathfrak{m}$ por escolha. Pelo lema anterior aplicado a cada primo $\mathfrak{p}_i$, obtemos uma raíz da unidade θ_{m_i} tais que os inteiros m_i são primos dois a dois. Segue que $K \cap (\mathbb{Q}(\theta_{m_i})) = \mathbb{Q}$. Logo o grupo de Galois $G_i = \mathrm{Gal}(K(\theta_{m_i})/K) \cong \mathrm{Gal}(\mathbb{Q}(\theta_{m_i})/\mathbb{Q})$. Além disso, o grupo de Galois de $L(\theta_{m_1}, \ldots, \theta_{m_r})$ sobre K é o produto direto $\mathcal{G} = G \times G_1 \times \cdots \times G_r$, onde $G = \mathrm{Gal}(L/K) =< \sigma >$.

Seja τ_i o elemento que obtemos (segundo o lema anterior) usando $\mathfrak{p}_i$ no lugar de $\mathfrak{p}$. Seja H_i o subgrupo de $G \times G_i$ gerado por $\sigma \times \tau_i$ e por $\varphi_{L/K}(\mathfrak{p}_i) \times \varphi_{K(\theta_{m_i})/K}(\mathfrak{p}_i)$. Considere H_i como subgrupo de $\mathcal{G}$ segundo a inclusão canônica.

Seja F_i o subcorpo de $L(\theta_{m_1}, \ldots, \theta_{m_r})$ fixo por $H_i \times \prod_{i \neq j} G_j$, e seja $F = F_1F_2 \cdots F_r$. afirmo que $L \cap F = K$ e $\mathrm{Gal}(LF/F) = \mathrm{Gal}(L/K)$.

De fato, note que, para cada i, $\mathrm{Gal}(LF/F_i)$ contém um elemento $\lambda = \sigma \times \tau_1 \times \cdots \times \tau_r$. A interseção dos grupos $\mathrm{Gal}(LF/F_i)$ fixa F e contém λ. O corpo $L \cap F$ é fixo por este elemento e também por $1 \times \tau_1 \times \cdots \times \tau_r$. Então $L \cap F$ é fixo por σ e, dado que o subcorpo de L fixo por σ é K, temos $L \cap F = K$. Já a igualdade

$\mathrm{Gal}(LF/F) = \mathrm{Gal}(L/K)$ vale pelo fato de que a restrição a $\mathrm{Gal}(LF/F)$ a L é um isomorfismo em $\mathrm{Gal}(L/K)$. Agora seja $\varphi_{L/K}(\mathfrak{p}_i^{a_i}) = \sigma^{d_i}$, para algum $d_i \geq 0$. Então $\varphi_{L/K}(\mathfrak{A}) = \prod_i \sigma^{d_i} = 1$. Se $d = d_1 + \cdots + d_r$, e temos que $n|d$, pois $n = [L:K] = |G|$.

Sabemos que se $\mathfrak{m}'$ for um módulus com expoentes suficientemente grandes e com determinados divisores primos, então $\varphi_{LF/F}$ manda $\mathbf{I}_F^{\mathfrak{m}'}$ em $\mathrm{Gal}(LF/F)$ de maneira sobrejetora. Seja $\mathfrak{m}'$ divisível por $\mathfrak{m}$ e por todos os inteiros m_i. Então existe um ideal $\mathfrak{B}_0 \in \mathbf{I}_F^{\mathfrak{m}'}$ tal que $\varphi_{LF/F}(\mathfrak{B}_0) = \sigma$. Seja $\mathfrak{B} = N(L/F)(\mathfrak{B}_0) \in \mathbb{I}_K^{\mathfrak{m}}$. Como $\varphi_{LF/F} = \varphi_{L/K} \circ N_{F/K}$, concluímos que $\varphi_{L/K}(\mathfrak{B}) = \sigma$. Como $\mathfrak{B}$ é uma norma de F, então $\mathfrak{B}$ também é uma norma em cada F_j. Além disso cada $\mathfrak{p}_i$ se decompõe completamente em F_i, de onde tiramos que $\mathfrak{p}_i$ é uma norma de F_i. Logo existe um ideal $\mathfrak{C}_i$ primo com $\mathfrak{m}$ e com os inteiros m_j tais que $N_{F_i/K}(\mathfrak{C}_i) = \mathfrak{p}_i^{a_i}\mathfrak{B}^{-d_i}$. Assim

$$\varphi_{LF_i/F_i}(\mathfrak{C}_i) = \varphi_{L/K}(N_{F_i/K}(\mathfrak{C}_i)) = \varphi_{L/K}(\mathfrak{p}_i)^{a_i}\varphi_{L/K}(\mathfrak{B})^{-d_i} = \sigma^{d_i - d_i} = 1.$$

Como a extensão LF_i de F_i satisfaz $F_i \subseteq LF_i \subseteq F_i(\theta_{m_i})$, a lei de reciprocidade vale para $(LF_i, F_i, \mathfrak{m}'')$ desde que $\mathfrak{m}''$ seja divisível por $(\mathfrak{m}_i)\mathfrak{p}_\infty$. Pelo fato de $\mathfrak{C}_i$ ser primo com $\mathfrak{m}_i$ e $\mathfrak{m}$, temos que $\mathfrak{m}''$ é divisível por $\mathfrak{m}$ e $\mathfrak{C}_i \in \mathbf{I}_{F_i}^{\mathfrak{m}''}$. Pela lei de reciprocidade, existem $\gamma_i \in F_i$ tal que $\gamma_i \equiv 1 (\mathrm{mod}\ \ \mathfrak{m}'')$ e um ideal $\mathfrak{D}_i \in \mathbb{I}_{LF_i}^{\mathfrak{m}''}$ tal que $\mathfrak{C}_i = (\gamma_i)N_{LF_i/F_i}(F_i)(\mathfrak{D}_i)$. Tomando as normas em K obtemos $\mathfrak{p}_i^{a_i}\mathfrak{B}^{-d_i} = (N_{F_i/K}(\gamma_i))N(_{LF_i/K}(\mathfrak{D}_i))$.

Como $\mathfrak{m}''$ é divisível por $\mathfrak{m}$, sabemos que $\alpha_i = N_{F_i/K}(\gamma_i) \in K_{\mathfrak{m},1}$. Tomando o produto sobre todos os i, obtemos $\mathfrak{A}\mathfrak{B}^{-d} = \prod_i \mathfrak{p}_i^{a_i}\mathfrak{B}^{-di} = \prod_i \alpha_i \prod_i N_{LF_i/K}(\mathfrak{D}_i)$.

Se $\mathfrak{D}_i' = N_{LF_i/L}(\mathfrak{D}_i)$, então DD_i' é primo com $\mathfrak{m}$. Assim

$$\mathfrak{A} = \mathfrak{B}^d(\alpha_1 \cdots \alpha_r)N_{L/K}(\mathfrak{D}_1' \cdots \mathfrak{D}_r').$$

Como $n|d$ e $\mathfrak{B}^d$ é uma norma em L, temos $\mathfrak{A} \in \iota(K_{\mathfrak{m},1})N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})$. □

Agora podemos generalizar o teorema anterior para extensões abelianas:

Teorema 4.7.9. *Seja L uma extensão abeliana de um corpo de números K e seja $\mathfrak{m}$ um módulus para K divisível por cada primo que ramifica em L. Se os expoentes dos divisores primos de $\mathfrak{m}$ são suficientemente grandes, então a função de Artin $\varphi_{L/K}$ associa $\boldsymbol{I}_K^{\mathfrak{m}}$ de maneira sobrejetora a* $\mathrm{Gal}(L/K)$ *e satisfaz* $\ker(\varphi_{L/K}) = \iota(K_{\mathfrak{m},1})N(L/K)(\boldsymbol{I}_L^{\mathfrak{m}})$.

Demonstração: Escreva $G = \mathrm{Gal}(L/K) = C_1 \times \cdots C_s$ como o produto de grupos cíclicos.

Seja H_j tal que $G = C_j \times H_j$. Seja E_j o subcorpo de L fixo por H_j. Então E_j é uma extensão cíclica de K com grupo de Galois C_j. Logo existe um módulus $\mathfrak{m}_j$ para K tal que a lei de reciprocidade vale para $(E_j, K, \mathfrak{m}_j)$. Cada primo de K que ramifica em E_j também ramifica em L. Assim, podemos escolher $\mathfrak{m}_j$ como sendo divisível apenas pelos primos que se ramificam em E_j com expoentes suficientemente grandes tais que $\mathfrak{m}_j|\mathfrak{m}$. Assim valerá a lei de reciprocidade para $(E_j, K, \mathfrak{m})$. Isto implica $\iota(K_{\mathfrak{m},1}) \subseteq \bigcap_i \ker(\varphi_{E_j/K})$.

Para um ideal $\mathfrak{A} \in \mathbb{I}_K^{\mathfrak{m}}$, sabemos que $\mathrm{res}_{E_j}(\varphi_{L/K}(\mathfrak{A})) = \varphi_{E_j/K}(\mathfrak{A})$. Em particular, se $\mathfrak{A} \in \iota(K_{\mathfrak{m},1})$, então $\mathrm{res}_{E_j}(\varphi_{L/K}(\mathfrak{A})) = 1$. Lembrando que $L = E_1 \cdots E_s$ e qualquer automorfismo que é a identidade em E_j precisa ser a identidade em L, temos que $\varphi_{L/K}(\mathfrak{A}) = 1$ e $i(K_{\mathfrak{m},1}) \subseteq \ker(\varphi_{L/K})$. Logo a lei de reciprocidade vale para $(L, K, \mathfrak{m})$. Agora o resultado segue do primeiro lema desta seção. □

Referências Bibliográficas

[1] Emil Artin, John Tate ; "Class Field Theory"; AMS Chelsea Publishing.

[2] Nicolas Bourbaki; "Commutative Algebra"; Elements of Mathematics; Hermann.

[3] J. W. S. Cassels, A. Fröhlich; "Algebraic Number Theory" (Proceedings of an Instructional Conference Organized by the London Mathematical Society), Academic Press.

[4] Kenneth Ireland, Michael Rosen; "A Classical Introduction to Modern Number Theory", Second Edition; Spring-Verlag.

[5] Gerald J. Janusz; "Algebraic Number Fields", Second Edition; Graduate Studies in Mathematics, Volume 7; American Mathematical Society.

[6] Daniel A. Marcus; "Number Fields"; Universitext; Springer-Verlag.

[7] Adam Massey; "The inverse Galois problem for nilpotent groups of odd order", course notes available at `http://www.math.ucla.edu/~amassey3102/Thesis_02.pdf`

[8] J. Milne; "Algebraic Number Theory"; course notes available at `http://www.jsmilne.org/math/`

[9] J. Milne; "Class Field Theory"; course notes available at `http://www.jsmilne.org/math/`

[10] J. Milne; "Fields and Galois Theory"; course notes available at `http://www.jsmilne.org/math/`

[11] M. Ram Murty, Jody Esmonde; "Problems in Algebraic Number Theory", Second Edition; Graduate Texts in Mathematics 190; Springer-Verlag.

[12] Jürgen Neukirch; "Algebraic Number Theory"; Grundlehren Der Mathematischen Wissenschaften 322; Springer-Verlag.

[13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg; "Cohomology of number fields"; Grundlehren der Mathematischen Wissenschaften 323; Springer-Verlag.

[14] D. G. Northcott; "An Introduction to Homological Algebra"; Cambridge University Press.

[15] R. S. Pierce; “Associative Algebras”; Graduate Texts in Mathematics 88; Springer-Verlag.

[16] Joseph Rotman; “Galois Theory”, Second Edition; Springer-Verlag.

[17] Pierre Samuel; “Algebraic Theory of Numbers”; Dover Books on Mathematics.

[18] Jean-Pierre Serre; “Local fields”; Graduate Texts in Mathematics 67; Springer-Verlag.

[19] Jean-Pierre Serre; “Topics in Galois Theory”; Research Notes in Mathematics, A K Peters.

[20] J. H. Silverman; “Advanced Topics in the Arithmetic of Elliptic Curves”; Graduate Texts in Mathematics 151; Springer-Verlag.

[21] Ian Stewart, David Tall; “Algebraic Number Theory and Fermat’s Last Theorem”; B& T.