

teoria dos números algébricos

Endler, Otto

Teoria dos números algébricos / Otto Endler. 2.ed.
Rio de Janeiro : IMPA, 2014.

199 p.; (Projeto Euclides)

ISBN 978-85-244-0026-1

I. Teoria dos números. I. Título. II. Série.

CDD-512

otto endler

**teoria dos
números algébricos**

Segunda edição



INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA

Copyright © 2014 by Otto Endler

Impresso no Brasil / Printed in Brazil

Capa: Noni Geiger / Sérgio R. Vaz

Projeto Euclides

Comissão Editorial:

Elon Lages Lima (Editor)
S. Collier Coutinho
Paulo Sad

Títulos Publicados:

- Curso de Análise, Volume 1 - *Elon Lages Lima*
- Medida e Integração - *Pedro Jesus Fernandez*
- Aplicações da Topologia à Análise - *Chaim Samuel Hönl*
- Espaços Métricos - *Elon Lages Lima*
- Análise de Fourier e Equações Diferenciais Parciais - *Djairo Guedes de Figueiredo*
- Introdução aos Sistemas Dinâmicos - *Jacob Palis Junior e Wellington C. de Melo*
- Introdução à Álgebra - *Adilson Gonçalves*
- Aspectos Teóricos da Computação - *Cláudio L. Lucchesi, Imre Simon, Istvan Simon, Janos Simon e Tomasz Kowaltowski*
- Teoria Geométrica das Folhações - *Alcides Lins Neto e César Camacho*
- Geometria Riemanniana - *Manfredo P. do Carmo*
- Lições de Equações Diferenciais Ordinárias - *Jorge Sotomayor*
- Probabilidade: Um Curso em Nível Intermediário - *Barry R. James*
- Curso de Análise, Volume 2 - *Elon Lages Lima*
- Teoria Ergódica - *Ricardo Mañé*
- Teoria dos Números Algébricos - *Otto Endler*
- Operadores Auto-Adjuntos e Equações Diferenciais Parciais - *Javier Thayer*
- Equações Diferenciais Parciais: Uma Introdução - *Rafael Iório Jr. e Valéria Iório*
- Álgebra: Um Curso de Introdução - *Arnaldo Leite P. Garcia e Yves Albert E. Lequain*
- Grupo Fundamental e Espaços de Recobrimento - *Elon Lages Lima*
- Funções de uma Variável Complexa - *Alcides Lins Neto*
- Elementos de Álgebra - *Arnaldo Garcia e Yves Lequain*
- Introdução à Geometria Analítica Complexa - *Marcos Sebastiani*
- Curso de Teoria da Medida - *Augusto Armando de Castro Júnior*
- Introdução à Teoria da Medida - *Carlos Isnard*
- Introdução à Teoria de Controle e Programação Dinâmica - *Johann Baumeister e Antonio Leitão*
- Homologia Básica - *Elon Lages Lima*
- Teoria dos Números: um Passeio com Primos e outros Números Familiares pelo Mundo Inteligente - *Fabio Brochero Martínez, Carlos Gustavo Moreira, Nicolau Saldanha e Eduardo Tengan*
- Introdução à Análise Funcional - *César R. de Oliveira*

Distribuição:

IMPA
Estrada Dona Castorina, 110
22460-320 Rio de Janeiro, RJ
e-mail: ddic@impa.br
<http://www.impa.br>

A segunda edição deste livro deve-se a uma sugestão do Prof. João Lucas Barbosa, presidente da Sociedade Brasileira de Matemática. Seu lançamento coincidiu com a realização, no Instituto de Matemática, Estatística e Computação Científica da UNICAMP, do *Workshop in Valuation Theory and its Applications*, no qual se homenageou o Prof. Otto Endler (1929-1988).

CONTEÚDO

Prólogo	VII
CAPÍTULO I – CORPOS DE NÚMEROS ALGÉBRICOS	1
§0. Noções básicas sobre corpos, anéis e módulos	1
§1. O anel I_L dos inteiros algébricos	9
§2. Corpos quadráticos	19
§3. Corpos ciclotômicos	28
§4. Discriminante	39
§5. Bases integrais	47
CAPÍTULO II – ANÉIS NOETHERIANOS E DOMÍNIOS DE DEDEKIND.....	55
§6. O Teorema Chinês de Restos	55
§7. Anéis noetherianos e módulos noetherianos	62
§8. Domínios de Dedekind	69
CAPÍTULO III – CLASSES DE IDEAIS	82
§9. Norma de ideais	82
§10. Finitude do número de classes.....	88
CAPÍTULO IV – EXTENSÕES DE DOMÍNIOS DE DEDEKIND	95
§11. Anéis de frações de um domínio.....	95
§12. Decomposição de ideais primos	102
§13. Um teorema de Kummer. Ramificação	108
CAPÍTULO V – DECOMPOSIÇÃO EM CORPOS CICLOTÔMICOS E QUADRÁTICOS	117
§14. Decomposição em corpos ciclotômicos	117
§15. Decomposição em corpos quadráticos	122
§16. Reciprocidade quadrática	127
CAPÍTULO VI – O MÉTODO GEOMÉTRICO.....	144
§17. Redes no $\mathbb{R}^n$	145
§18. Representações geométricas de números algébricos.....	151
§19. Invertíveis em corpos quadráticos	162
CAPÍTULO VII – EXTENSÕES GALOISIANAS	173
§20. Grupo e corpo de decomposição.....	173
§21. Grupos e corpos de inércia e de ramificação	179
Prólogo	191
Referências	193
Índice de notações	195
Índice alfabético	197

PRÓLOGO

A Teoria dos Números é, em princípio, uma teoria dos números *racionais* e *inteiros* e, em grande parte, está ligada ao problema de resolver equações diofantinas, isto é, encontrar soluções inteiras para equações algébricas $F(X_1, \dots, X_n) = 0$. Os números *algébricos* surgem, de maneira natural, como ferramenta para tratar este problema. Ilustramos isto por meio de dois exemplos:

I) Para tratar a equação $X^p + Y^p - Z^p = 0$ que, pelo famoso mas ainda não provado “Último Teorema de Fermat”, não possui nenhuma solução de números inteiros no caso em que p é um primo ímpar, convém escrever $X^p + Y^p$ como produto $(X + Y) \cdot (X + \zeta_p \cdot Y) \cdot \dots \cdot (X + \zeta_p^{p-1} \cdot Y)$, sendo uma raiz p -ésima da unidade $\zeta_p \neq 1$. Prova-se que o teorema será válido para p quando o domínio $\mathbb{Z}[\zeta_p]$ for fatorial (veja Borevich-Shafarevich [6], Chapter 3, §1).

II) Para determinar as soluções inteiras da “equação de Pell” $X^2 - d \cdot Y^2 - 1 = 0$ ($d > 1$, livre de quadrados), convém escrever $X^2 - d \cdot Y^2$ como produto $(X - \sqrt{d} \cdot Y) \cdot (X + \sqrt{d} \cdot Y)$. As soluções inteiras (a, b) desta equação correspondem aos elementos invertíveis $a + b \cdot \sqrt{d}$ do anel $[\sqrt{d}]$, com norma igual a 1, os quais podem ser obtidos como potências do “invertível fundamental” $\varepsilon_1 = a_1 + b_1 \cdot \sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$ (veja §19).

Vê-se nestes exemplos a importância dos anéis $\mathbb{Z}[\zeta_p]$ e $\mathbb{Z}[\sqrt{d}]$, respectivamente. Em geral, para qualquer número algébrico α , considera-se além do corpo $L = \mathbb{Q}(\alpha)$ um certo subanel distinguido I_L de L , o “anel dos inteiros algébricos de L ”, que entretanto nem sempre é da forma $\mathbb{Z}[\alpha]$. O estudo deste anel, cujo papel relativo a L é análogo ao de $\mathbb{Z} = I_{\mathbb{Q}}$ em relação a $\mathbb{Q}$, pode ser considerado o objetivo principal da *Teoria dos Números Algébricos*, a qual, embora surgida como ferramenta, tem se tornado uma teoria independente com vida própria.

Uma boa parte do estudo dos anéis I_L estende-se facilmente a domínios de Dedekind quaisquer. Por isto, desenvolveremos neste livro a teoria dos anéis noetherianos e dos domínios de Dedekind, que pertence à Álgebra Comutativa, na medida que for necessário para aplicá-la aos

anéis I_L . Não fazemos questão de alcançar o maior grau de generalidade. Pelo contrário, procuramos simplificar os enunciados e as demonstrações, restringindo-nos, onde convém, ao caso que mais nos interessa (evitando, por exemplo, extensões inseparáveis).

Por outro lado, a finitude do número de classes h_L e o teorema de invertíveis de Dirichlet são dois fatos cruciais da Teoria dos Números que não se generalizam a domínios de Dedekind arbitrários. Provaremos o teorema de Dirichlet usando métodos geométricos, os quais são indispensáveis também num estudo mais profundo em torno de h_L .

Quanto aos pré-requisitos necessários para a leitura deste livro, fizemos força para reduzi-los aos conhecimentos mais básicos da Álgebra em nível da "Introdução à Álgebra", de Adilson Gonçalves, [10], publicada neste Projeto Euclides. As noções básicas sobre corpos, anéis e módulos que serão usadas neste livro, encontram-se sem demonstração (mas às vezes com referências) no §0. Resultados adicionais, inclusive os usualmente abordados num curso de mestrado em Álgebra, serão demonstrados nos parágrafos onde forem utilizados.

É difícil justificar a publicação de mais um livro sobre Número Algébricos, uma vez que já existem vários livros excelentes sobre esta matéria, como por exemplo Samuel [30], Ribenboim [27], Borevich Shafarevich [6], Stewart-Tall [33], para mencionar apenas os que mais foram utilizados pelo autor na preparação das notas de aula que deram origem a este livro. Mesmo assim, esperamos que, sendo escrito em português, este livro possa ser útil para divulgar os números algébricos no Brasil e estimular estudos mais profundos na Teoria dos Números, que costuma ser chamada a "Rainha da Matemática". Ele pode servir também como uma introdução suave e bem motivada a alguns tópicos de Álgebra Comutativa, pois nele as noções abstratas desta teoria são introduzidas para serem imediatamente aplicadas ao caso concreto de números algébricos.

Finalmente, queremos mencionar que existe outra opção, diferente da adotada neste livro, para apresentar a Teoria dos Números Algébricos. De fato, em lugar do "método clássico" aqui adotado, que se concentra no estudo do anel de Dedekind I_L , pode-se usar como base da teoria a noção de valorização (veja, por exemplo, Hasse [15] ou Weiss [37]) noção esta que aparece neste livro apenas de maneira implícita, no §8. Apesar da noção de valorização ser indispensável para estudos mais profundos, pois permite o uso do completamento e é mais adequada para extensões infinitas, demos preferência ao método clássico devido à sua maior transparência.

Agradeço a todos que contribuíram para a realização deste livro. Em primeiro lugar, sou grato a Elon Lages Lima por ter me convidado a escrever este livro para o Projeto Euclides. Valiosos estímulos e sugestões recebi de Yves Lequain, Karl-Otto Stöhr e José Felipe Voloch. A Maria de Conceição Vaz Pinto agradeço pela cuidadosa leitura e pela ajuda na correção do manuscrito. Finalmente, sou grato aos alunos do meu atual curso que, através de muitas sugestões, participaram no retoque final deste livro.

Rio de Janeiro, novembro de 1985
Otto Endler

CORPOS DE NÚMEROS ALGÉBRICOS

A noção central na Teoria dos Números Algébricos é a de anel dos inteiros algébricos, I_L , de um corpo de números algébricos, L . Este anel será introduzido no §1, num contexto mais geral, através da noção de elemento inteiro sobre um anel R , a qual generaliza a noção de elemento algébrico sobre um corpo K .

O fato de I_L ser sempre um $\mathbb{Z}$ -módulo livre será provado no §5. Na caracterização das suas bases, o discriminante, introduzido no §4, representa um papel importante.

Como exemplos mais simples de corpos de números algébricos serão estudados, nos §2 e §3, os corpos quadráticos e os corpos ciclotômicos, juntamente com os seus anéis dos inteiros algébricos.

Noções básicas da teoria dos corpos, dos anéis e dos módulos serão recordadas no §0.

§0. Noções básicas sobre corpos, anéis e módulos

Neste parágrafo reunimos alguns fatos básicos que serão utilizados neste livro e fixamos assim a terminologia básica nele adotada.

A) Corpos

Sejam L um corpo e K um subcorpo de L . Consideramos L como K -espaço, isto é, espaço vetorial sobre K (em relação à adição em L e à multiplicação com elementos de K); dizemos que L é uma *extensão* de K (ou $L|K$ é uma extensão). Diremos que L é uma *extensão finita* de K , de grau $[L:K] = n$, quando uma (e logo toda) base do K -espaço L tiver n elementos. Note-se que de $K \subseteq L \subseteq M$ decorre $[M:K] = [M:L] \cdot [L:K]$, e que $[L:K] = 1$ se e somente se $L = K$.

Dado um subconjunto $\mathcal{A}$ de L , denotamos por $K(\mathcal{A})$ o corpo obtido de K pela *adjunção* de $\mathcal{A}$, ou seja, o menor corpo entre K e L que contém $\mathcal{A}$. No caso $\mathcal{A} = \{\alpha_1, \dots, \alpha_s\}$ escrevemos $K(\alpha_1, \dots, \alpha_s)$ em lugar de $K(\mathcal{A})$.

Para qualquer $\alpha \in L$, seja $p_{\alpha, K}$ o conjunto dos polinômios $F \in K[X]$ tais que $F(\alpha) = 0$, isto é, que α seja uma *raiz* de F . Como $p_{\alpha, K}$ é o núcleo do homomorfismo $K[X] \rightarrow L$ definido por $F \mapsto F(\alpha)$ ($F \in K[X]$), $p_{\alpha, K}$ é um ideal primo de $K[X]$. O elemento α será chamado *algébrico* sobre K se e somente se $p_{\alpha, K} \neq (0)$, o que ocorrerá se e somente se $p_{\alpha, K}$ for um ideal maximal de $K[X]$, se e somente se $K[\alpha]$ for um corpo. Neste caso, temos $K[\alpha] = K(\alpha)$, e $p_{\alpha, K}$ é gerado por um polinômio irredutível e mônico $P_{\alpha|K}$, univocamente determinado, que é chamado o *polinômio minimal* de α sobre K ; além disto, os elementos $1, \alpha, \dots, \alpha^{n-1}$ formam uma base da extensão $K(\alpha)$ de K , sendo $n = \partial P_{\alpha|K}$ ($=$ grau do polinômio $P_{\alpha|K}$). Por outro lado, quando α for *transcendente*, isto é, não algébrico sobre K , o anel $K[\alpha]$ será K -isomorfo ao anel de polinômios $K[X]$, sob o homomorfismo acima indicado, e será um subanel próprio do corpo $K(\alpha)$, que é o seu corpo de frações.

Diremos que L é uma *extensão algébrica* de K se todo $\alpha \in L$ for algébrico sobre K ; neste caso, todo anel entre K e L é um subcorpo de L . O corpo $K(\mathcal{A})$, obtido de K pela adjunção de um conjunto $\mathcal{A}$ de elementos algébricos sobre K , é uma extensão algébrica de K . Uma extensão L de K será finita se existirem elementos $\alpha_1, \dots, \alpha_r$ algébricos sobre K tais que $L = K(\alpha_1, \dots, \alpha_r)$; neste caso, L é uma extensão algébrica de K .

Um corpo Ω será chamado *algebricamente fechado* se não possuir nenhuma extensão algébrica própria ou, equivalentemente, se todo polinômio irredutível em $\Omega[X]$ for linear (isto é, tiver grau 1). Neste caso, a fatoração (única) de qualquer polinômio não-nulo $F \in \Omega[X]$ é da forma $F = \omega \cdot (X - \alpha_1) \cdot \dots \cdot (X - \alpha_n)$, sendo $\alpha_1, \dots, \alpha_n \in \Omega$ as raízes de F , não necessariamente distintas, e $\omega \in \Omega \setminus \{0\}$.

No que se segue, Ω denotará sempre um corpo algebricamente fechado que contém o corpo K . Tal corpo Ω sempre existe, e os resultados serão independentes da escolha de Ω . Quando o corpo K for uma extensão algébrica de $\mathbb{Q}$, ele poderá ser considerado como subcorpo do corpo $\mathbb{C}$ dos números complexos, o qual é algebricamente fechado. As vezes convém escolher Ω como um *fecho algébrico* de K , isto é, um corpo algebricamente fechado que é algébrico sobre K . O fecho algébrico de K é univocamente determinado a menos de um K -isomorfismo. Dentro de um corpo algebricamente fechado Ω que contém K , existe um único fecho algébrico de K ; ele consiste dos elementos de Ω que são algébricos sobre K . Por exemplo, o fecho algébrico de $\mathbb{Q}$ em $\mathbb{C}$ é o corpo $\mathbb{A}$ de todos os números algébricos.

Para qualquer extensão algébrica L de K existem pelo menos um e, se a extensão é finita, no máximo $[L:K]$ K -isomorfismos de L em Ω .⁽¹⁾

Um polinômio mônico (não necessariamente irredutível) $F = X^n + a_1 \cdot X^{n-1} + \dots + a_n \in K[X]$ será chamado *separável* se F e sua derivada $F' = nX^{n-1} + (n-1)a_1 \cdot X^{n-2} + \dots + a_{n-1}$ forem primos entre si, isto é, se $\text{MDC}(F, F') = 1$.⁽²⁾ Prova-se que isto equivale a cada uma das seguintes condições:

- (i) Para toda extensão L de K , não existe nenhum $G \in L[X] \setminus L$ tal que G^2 divida F .
- (ii) Na fatoração de F em $\Omega[X]$, os fatores, necessariamente lineares, são distintos (ou seja, todas as raízes de F em Ω são simples).
- (iii) O discriminante de F definido por

$$\text{disc}(F) = \prod_{i=1}^n \prod_{j=i+1}^n (\alpha_j - \alpha_i)^2$$

é não-nulo.

Observemos que $\text{disc}(F)$ é da forma $D(a_1, \dots, a_n)$, para um certo polinômio $D \in \mathbb{Z}[X_1, \dots, X_n]$. Isto pode ser concluído do fato de $\text{disc}(F)$ ser uma função simétrica nas raízes de F , ou do fato de coincidir (a menos do sinal) com a resultante $\text{Res}(F, F')$ (veja van der Waerden [34], §26-28). Em particular, temos que

$$\text{disc}(X^2 + a \cdot X + b) = a^2 - 4b,$$

$$\text{disc}(X^3 + a \cdot X^2 + b \cdot X + c) = a^2 \cdot b^2 - 4b^3 - 4a^3 \cdot c - 27c^2 + 18a \cdot b \cdot c.$$

Um polinômio irredutível e mônico $F \in K[X]$ será separável se e somente se $F' \neq 0$. Isto ocorrerá quando K for um corpo *perfeito*, isto é, tiver característica zero, ou tiver característica $p \neq 0$ e todo $a \in K$ for uma potência p -ésima em K . Por exemplo, todo corpo finito é perfeito, bem como qualquer corpo algebricamente fechado.

Um elemento α algébrico sobre K será chamado *separável* sobre K se for raiz de um polinômio separável $F \in K[X]$; neste caso, o polinômio minimal $P_{\alpha|K}$ também é separável.

Uma extensão algébrica L de K será chamada *separável* se todo $\alpha \in L$ for separável sobre K ; para isto é suficiente que $L = K(\mathcal{A})$ para algum

⁽¹⁾ Usa-se "isomorfismo de L em M " em lugar das expressões mais exatas "homomorfismo (necessariamente injetivo) de L em M " ou "isomorfismo de L sobre um subcorpo de M ". O prefixo " K -" significa que a restrição a K é a aplicação idêntica de K .

⁽²⁾ Observe-se que, no caso de polinômios *reduzíveis*, alguns autores usam a palavra "separável" em outro sentido.

conjunto $\mathcal{A}$ de elementos separáveis sobre K . Uma extensão finita L de K será separável se e somente se existirem exatamente $[L:K]$ K -isomorfismos de L em Ω . Toda extensão finita e separável é simples, isto é, existe um "elemento primitivo" α tal que $L = K(\alpha)$. Note-se que toda extensão algébrica de um corpo perfeito é separável.

Seja L uma extensão finita de K , de grau n . Para cada $\alpha \in L$ consideramos o polinômio característico $F_{\alpha, L|K}$ de α em relação a $L|K$, definido por $\det(X \cdot \delta_{ij} - a_{ij})$, onde a matriz (a_{ij}) , de elementos $a_{ij} \in K$, é determinada por $\alpha \cdot \beta_i = \sum_{j=1}^n a_{ij} \cdot \beta_j$ ($i = 1, \dots, n$), sendo $\beta_1, \dots, \beta_n$ uma base da extensão L de K , e δ_{ij} o "símbolo de Kronecker", isto é, $\delta_{ii} = 1$ e $\delta_{ij} = 0$ quando $i \neq j$. Prova-se que $F_{\alpha, L|K} = P_{\alpha|K}^m$, onde $m = [L:K(\alpha)]$ e, portanto, independe da escolha da base $\beta_1, \dots, \beta_n$. Sendo $F_{\alpha, L|K} = X^n + f_1 \cdot X^{n-1} + \dots + f_n$, definimos o *traço* e a *norma* de α em relação a $L|K$ por

$$\mathcal{T}_{L|K} \alpha = -f_1 = \sum_{i=1}^n a_{ii}$$

$$\text{e} \quad \mathcal{N}_{L|K} \alpha = (-1)^n \cdot f_n = \det(a_{ij}).$$

Mencionamos que $\mathcal{N}_{L|K}(\alpha \cdot \beta) = \mathcal{N}_{L|K} \alpha \cdot \mathcal{N}_{L|K} \beta$, $\mathcal{N}_{L|K} a = a^n$ e $\mathcal{T}_{L|K}(a \cdot \alpha + b \cdot \beta) = a \cdot \mathcal{T}_{L|K} \alpha + b \cdot \mathcal{T}_{L|K} \beta$, $\mathcal{T}_{L|K} a = na$, quaisquer que sejam $\alpha, \beta \in L$ e $a, b \in K$.

Se L for uma extensão separável de K e $\sigma_1, \dots, \sigma_n$ os K -isomorfismos de L em Ω , então $F_{\alpha, L|K} = \prod_{i=1}^n (X - \sigma_i \alpha)$, $\mathcal{N}_{L|K} \alpha = \prod_{i=1}^n \sigma_i \alpha$ e $\mathcal{T}_{L|K} \alpha = \sum_{i=1}^n \sigma_i \alpha$. (Veja van der Waerden [34], §41, ou Borevich-Shafarevich [6], Algebraic Supplement, §2).

Uma extensão finita N de K será dita *normal* se satisfizer as seguintes condições equivalentes:

- (i) Para todo K -isomorfismo σ de N em Ω temos que $\sigma N \subseteq N$.
- (ii) Para qualquer $\alpha \in N$, $P_{\alpha|K}$ fatora-se em $N[X]$ em fatores lineares.
- (iii) Existe $F \in K[X]$ tal que $N = K(\alpha_1, \dots, \alpha_r)$, sendo $\alpha_1, \dots, \alpha_r$ todas as raízes de F em Ω .

Neste caso, vale a igualdade em (i), isto é, todos os K -isomorfismos de N em Ω são K -automorfismos de N . A condição (iii) significa que N é o *corpo das raízes* (ou "corpo de decomposição") do polinômio F sobre K .

Uma extensão finita N de K será chamada *galoisiana* se for normal e separável. Se K for perfeito (por exemplo, se for finito ou tiver característica zero), então toda extensão normal de K será galoisiana.

Seja N uma extensão galoisiana de K de grau n . Então existem exatamente n K -automorfismos de N e, em relação à composição, estes formam um grupo $\text{Aut}(N|K)$, chamado o *grupo de Galois* de $N|K$. Pelo Teorema Fundamental de Galois, os subgrupos Δ de $\Gamma = \text{Aut}(N|K)$ correspondem biunivocamente aos corpos L entre K e N através das aplicações

$$L \mapsto \Delta_L = \{\sigma \in \Gamma \mid \sigma\alpha = \alpha \text{ para todo } \alpha \in L\} = \text{Aut}(N|L) \text{ e}$$

$$\Delta \mapsto L_\Delta = \{\alpha \in N \mid \sigma\alpha = \alpha \text{ para todo } \sigma \in \Delta\} \text{ (= corpo fixo de } \Delta);$$

em particular, temos que $\Delta_K = \text{Aut}(N|K)$, $\Delta_N = \{1\}$ (1 = aplicação idêntica de N), $L_{(1)} = N$, $L_\Gamma = K$.

Além disto, L será uma extensão normal (logo galoisiana) se e somente se Δ_L for um subgrupo normal de Γ , e neste caso $\text{Aut}(L|K)$ é isomorfo a Γ/Δ_L , sendo o isomorfismo induzido pela aplicação $\sigma \mapsto \sigma_L$ ($\sigma \in \Gamma$), onde σ_L é a restrição de σ ao corpo L .

B) Anéis

Por um *anel* R entendemos sempre um anel comutativo com unidade. Consideraremos somente subanéis R' de R que contêm a unidade de R (a qual, portanto, coincide com a de R'), e homomorfismos entre anéis que levem a unidade na unidade. O anel R será chamado *não-trivial* se sua unidade for diferente do zero, ou seja, se $\#R > 1$. Se, além disto, R não possuir divisores de zero, isto é, se $a \cdot b = 0$ implicar $a = 0$ ou $b = 0$, então R será chamado um *domínio* (de integridade).

Os elementos *invertíveis* de um anel R , isto é, os $u \in R$ tais que $u \cdot v = 1$ para algum $v \in R$, formam um grupo multiplicativo $U(R)$. Por exemplo, o anel $\mathbb{Z}$ dos números inteiros (rationais) é um domínio com $U(\mathbb{Z}) = \{1, -1\}$, e os anéis de polinômios $K[X], \dots, K[X_1, \dots, X_n], \dots, K[X_i \mid i \in I]$, em uma ou várias indeterminadas sobre um corpo K , são domínios cujo grupo dos invertíveis coincide com K^* , o grupo multiplicativo do corpo K .

Seja (a_{ij}) uma matrix quadrada, com $a_{ij} \in R$ ($i, j = 1, \dots, n$), e seja $a = \det(a_{ij})$. Então temos que $a \in R$, e existem $a_{ij}^* \in R$ tais que $\sum_{j=1}^n a_{ij}^* \cdot a_{jk} = a \cdot \delta_{ik}$ ($i, k = 1, \dots, n$; veja Greub [11], Chap. IV, §4). Se $a \in U(R)$ então (a_{ij}) possuirá uma matriz inversa, a saber, $(a^{-1} \cdot a_{ij}^*)$.

Dados um anel S , um subanel R e um subconjunto $\mathcal{A}$ de S , denotamos por $R[\mathcal{A}]$ o anel obtido de R pela adjunção de $\mathcal{A}$, ou seja, o menor anel

entre R e S que contém $\mathcal{A}$. No caso $\mathcal{A} = \{\alpha_1, \dots, \alpha_s\}$ escreveremos $R[\alpha_1, \dots, \alpha_s]$ em lugar de $R[\mathcal{A}]$.

Todo subanel R de um corpo L é um domínio, e $Q(R) = \{a \cdot b^{-1} \mid a, b \in R, b \neq 0\}$ é o menor subcorpo de L que contém R , chamado o *corpo de quocientes* de R em L . Este corpo $Q(R)$ é canonicamente R -isomorfo a, e usualmente identificado com, o *corpo de frações* $\{a/b \mid a, b \in R, b \neq 0\}$ de R , que é construído a partir de R da mesma maneira como se constrói $\mathbb{Q}$ a partir de $\mathbb{Z}$. Mais geralmente, para qualquer subconjunto multiplicativo M de R (isto é, tal que $1 \in M$ e que $s, t \in M$ implique $s \cdot t \in M$) o *anel de frações de R em relação a M* é definido como o subanel $R_M = \{a/b \mid a \in R, b \in M\}$ do corpo $Q(R)$. Obviamente, $M \subseteq M'$ implica $R_M \subseteq R_{M'}$. Em particular, $R_{(1)} = R_{U(R)} = R$ e $R_{R \setminus \{0\}} = Q(R)$. Para todo ideal primo $\mathfrak{p}$ de R , o conjunto $M = R \setminus \mathfrak{p}$ é um subconjunto multiplicativo de R , e R_M é chamado a *localização de R em relação a $\mathfrak{p}$* ; em particular, temos que $R_M = Q(R)$ no caso em que $\mathfrak{p} = (0)$.

Seja L uma extensão algébrica de $K = Q(R)$ e seja S um subanel de L que contenha R ; então obviamente $S_{R \setminus \{0\}} = K[S] = Q(S)$.

Seja $\mathfrak{a}$ um ideal do anel R , isto é, um subgrupo do grupo aditivo de R tal que $r \cdot a \in \mathfrak{a}$ para quaisquer $r \in R$ e $a \in \mathfrak{a}$. Recordemos que o conjunto $R/\mathfrak{a} = \{r + \mathfrak{a} \mid r \in R\}$ forma um anel, chamado o *anel quociente* de R em relação ao ideal $\mathfrak{a}$, e que a aplicação definida por $r \mapsto r + \mathfrak{a}$ ($r \in R$) é um homomorfismo, chamado *canônico*, de R sobre $R/\mathfrak{a}$, com núcleo $\mathfrak{a}$. Por outro lado, qualquer homomorfismo de R sobre um anel R' , com núcleo $\mathfrak{a}$, induz um isomorfismo de $R/\mathfrak{a}$ sobre R' .

Entre os ideais de R distinguem-se os ideais *principais*, isto é, os ideais $(a) = a \cdot R = R \cdot a$ gerados por um só elemento $a \in R$. Em particular, $(0) = \{0\}$, $(1) = R$, e teremos que $(a) = R$ se e somente se $a \in U(R)$. Além disto, $(a) \subseteq (b)$ se e somente se $b \mid a$ (isto é, b divide a , ou seja, a é um múltiplo de b). Em particular, teremos que $(a) = (b)$ se (e, no caso de um domínio R , somente se) a, b forem associados, isto é, se existir $u \in U(R)$ tal que $a = u \cdot b$.

Recordemos também que $\mathfrak{a}$ será um ideal *primo* (respectivamente *maximal*⁽¹⁾), se e somente se $R/\mathfrak{a}$ for um domínio (respectivamente corpo). Em particular, R será um domínio se e somente se (0) for um ideal primo; R será um corpo se e somente se (0) for um ideal maximal e, portanto, o único ideal de R diferente de R . Todo ideal $\mathfrak{a}$ de R tal que $\mathfrak{a} \neq R$ está contido num ideal maximal de R (veja Atiyah-Macdonald [3], p. 4).

⁽¹⁾ Utilizaremos a palavra "maximal" no sentido de "não existe maior". Convém distingui-la da palavra "máximo", uma vez que esta tem outro significado, a saber, "o maior de todos". Analogamente distinguiremos entre "minimal" e "mínimo".

Seja R um domínio. Um elemento não-nulo e não-invertível $r \in R$ será chamado *irredutível* se não for produto de dois elementos de $R \setminus U(R)$, e será chamado *primo*, se o ideal principal (r) for um ideal primo. Todo elemento primo é irredutível. O domínio R será chamado *fatorial* se houver "fatoração única", no sentido que a aplicação $f : U(R) \times \mathbb{N}^{(\mathcal{P})} \rightarrow R \setminus \{0\}$, definida por $(u, (n_p)_{p \in \mathcal{P}}) \mapsto u \cdot \prod_{p \in \mathcal{P}} p^{n_p}$, é bijetiva, sendo $\mathcal{P}$ um sistema de repre-

sentantes dos elementos irredutíveis de R (isto é, todo elemento irredutível é associado a um e um só $p \in \mathcal{P}$), e $\mathbb{N}^{(\mathcal{P})}$ o conjunto das famílias $(n_p)_{p \in \mathcal{P}}$ com $n_p \in \mathbb{N}$, tais que $n_p = 0$ para quase todos os $p \in \mathcal{P}$. Para um domínio R ser fatorial é necessário e suficiente que a aplicação f seja sobrejetiva e que todo elemento irredutível seja primo. Num domínio fatorial, para quaisquer elementos $r = u \cdot \prod p^{n_p}$, $s = v \cdot \prod p^{m_p}$, existem o máximo divisor comum $\text{MDC}(r, s)$ e o mínimo múltiplo comum $\text{MMC}(r, s)$, univocamente determinados a menos de um fator invertível, por $\prod p^{\min(n_p, m_p)}$ e $\prod p^{\max(n_p, m_p)}$, respectivamente.

Notemos ainda que a aplicação f se estende a uma aplicação $f : U(R) \times \mathbb{Z}^{(\mathcal{P})} \rightarrow Q(R)^*$, a qual será sobrejetiva (respectivamente bijetiva) se e somente se f o for. Desta maneira, num domínio R fatorial, a fatoração única estende-se aos elementos não-nulos do seu corpo de frações $Q(R)$.

Um domínio R será chamado *principal* se todo ideal de R for principal. Todo elemento irredutível de um domínio principal gera um ideal maximal e, portanto, é primo. Além disto, a aplicação f acima indicada é sobrejetiva (o que, aliás, será demonstrado em (7.10) num contexto mais geral). Por isto, todo domínio principal é fatorial.

C) Módulos

A definição de R -módulo, para um anel R qualquer, obtém-se como generalização natural da noção de K -espaço. Entendemos por um R -módulo um grupo abeliano M , escrito aditivamente e munido de uma operação externa (usualmente escrita como multiplicação), satisfazendo os seguintes axiomas:

$$\begin{aligned} a \cdot (x + y) &= a \cdot x + a \cdot y, \quad (a + b) \cdot x = a \cdot x + b \cdot x, \\ (a \cdot b) \cdot x &= a \cdot (b \cdot x), \quad 1 \cdot x = x, \end{aligned}$$

para quaisquer $a, b \in R$ e $x, y \in M$.

Evidentemente, todo grupo abeliano (aditivo) A é um $\mathbb{Z}$ -módulo, sendo $(\pm n) \cdot x$ definido por $\pm(x + \dots + x)$ para quaisquer $n \in \mathbb{N}$ e $x \in A$.

O *produto cartesiano* de R -módulos é um R -módulo, sendo as operações definidas componente a componente. É óbvio o que se entende por um *submódulo* N do R -módulo M , por um *módulo quociente* M/N e por um homomorfismo entre R -módulos. Em particular, a aplicação definida por $x \mapsto x + N$ ($x \in M$) é um homomorfismo de M sobre M/N , com núcleo N . Por outro lado, todo homomorfismo de M sobre M' , com núcleo N , induz um isomorfismo de M/N sobre M' .

Um R -módulo M será chamado *finitamente gerado* se existirem $x_1, \dots, x_r \in M$ tais que $M = R \cdot x_1 + \dots + R \cdot x_r$; neste caso, dizemos que $x_1, \dots, x_r$ formam um *sistema de geradores* de M . Diremos que os elementos $y_1, \dots, y_s$ de M são *linearmente independentes* (sobre R) se, para

quaisquer $a_1, \dots, a_s \in R$, a igualdade $\sum_{j=1}^s a_j \cdot y_j = 0$ implicar que $a_1 = \dots =$

$= a_s = 0$. Se, além disto, $y_1, \dots, y_s$ formarem um sistema de geradores de M , então este será chamado uma *base* de M . É importante notar que nem todo módulo finitamente gerado possui uma base. Em particular, a caracterização das bases de um K -espaço, como sistemas minimais de geradores ou sistemas maximais de elementos linearmente independentes, não se generaliza a módulos. Um R -módulo que possua uma base é chamado *livre*.⁽¹⁾

Muitas vezes consideraremos módulos cuja operação externa é definida por uma multiplicação interna. Em particular, dado um anel R , todo anel S que contiver R será considerado como R -módulo, sendo o produto externo $r \cdot x$, para $r \in R$ e $x \in S$, definido como o produto $r \cdot x$ tomado em S ; estudam-se então os submódulos do R -módulo S . Em particular, o próprio R é considerado como R -módulo, e os submódulos de R são exatamente os ideais de R . Note-se que um ideal α de R será um R -módulo livre se e somente se α for um ideal principal, gerado por um elemento que não seja um divisor de zero de R ; tal elemento forma então uma base de α .

Sejam R um domínio e L uma extensão do corpo de quocientes $K = Q(R)$; então, os elementos $\alpha_1, \dots, \alpha_r \in L$ serão linearmente independentes sobre R se e somente se o forem sobre K . Suponhamos ainda que $[L:K] = n$ e que S seja um subanel de L que contenha R e que, como R -módulo, possua uma base $\beta_1, \dots, \beta_q$. É fácil ver que $q \leq n$ e que as seguintes condições são equivalentes:

⁽¹⁾ Notemos que as noções "sistema de geradores", "linearmente independente" e "base" se estendem a subconjuntos infinitos de M , e que "módulo livre" pode significar a existência de uma base não necessariamente finita.

- (i) $q = n$
- (ii) $\beta_1, \dots, \beta_q$ formam uma base de $L|K$
- (iii) $L = S_{R \setminus \{0\}}$.

Como $S_{R \setminus \{0\}} = Q(S)$, a condição (iii) é equivalente à igualdade $L = Q(S)$.

Note-se, entretanto, que uma base de $L|K$ que consiste de elementos de S não é necessariamente uma base do R -módulo S . Na verdade, nem sempre S é um R -módulo livre.

§1. O anel I_L dos inteiros algébricos

Por um *número algébrico* entendemos qualquer $\alpha \in \mathbb{C}$ que é algébrico sobre $\mathbb{Q}$. Um subcorpo L de $\mathbb{C}$ será chamado *corpo de números algébricos* se for uma extensão finita de $\mathbb{Q}$ ou, equivalentemente, se $L = \mathbb{Q}(\alpha)$ para algum número algébrico α ; neste caso, todo elemento de L é um número algébrico.

As vezes convém generalizar levemente esta noção, chamando de corpo de números algébricos a qualquer extensão finita L de $\mathbb{Q}$, não necessariamente contida em $\mathbb{C}$. Sabemos que existem $[L:\mathbb{Q}]$ isomorfismos de L em $\mathbb{C}$; portanto L é isomorfo a (pelo menos) um corpo de números algébricos no sentido original.

Pretendemos mostrar que todo corpo de números algébricos $L = \mathbb{Q}(\alpha)$ possui um subanel distinguido I_L , com corpo de frações igual a L . Este anel em geral não coincide com o anel $\mathbb{Z}[\alpha]$, o qual depende da escolha do elemento primitivo α da extensão L de $\mathbb{Q}$. Definiremos I_L como o conjunto dos elementos de L que são "inteiros" sobre $\mathbb{Z}$ no sentido da definição seguinte, que introduziremos num contexto mais geral.

Sejam S um anel e R um subanel de S . Diremos que um elemento $\alpha \in S$ é *inteiro* sobre R se existir um polinômio mônico $F \in R[X]$ tal que $F(\alpha) = 0$. Em particular, todo elemento de R é inteiro sobre R .

No caso $S = \mathbb{C}$, $R = \mathbb{Z}$, os números inteiros sobre $\mathbb{Z}$ são chamados *inteiros algébricos*. Por exemplo, os números $i = \sqrt{-1}$, $\sqrt[3]{12}$, $\cos \frac{2\pi}{n} + i \cdot \sin \frac{2\pi}{n}$, $\frac{1 + \sqrt{5}}{2}$ são inteiros algébricos pois são raízes dos polinômios $X^2 + 1$, $X^3 - 12$, $X^n - 1$, $X^2 - X - 1 \in \mathbb{Z}[X]$, respectivamente. Veremos mais tarde que basta considerar o polinômio minimal $P_{\alpha|\mathbb{Q}}$ para decidir se o número algébrico α é inteiro ou não.

É óbvio que no caso de corpos $S = L$ e $R = K$, um elemento $\alpha \in L$ será inteiro sobre K se e somente se for algébrico sobre K .

Pretendemos mostrar que o conjunto dos elementos de S que são inteiros sobre R forma um subanel $I_S(R)$ de S . Para provar que a diferença (respectivamente o produto) de dois elementos $\alpha, \beta \in S$ inteiros sobre R é também um inteiro, podemos tentar construir, a partir de polinômios mônicos $F, G \in R[X]$ tais que $F(\alpha) = G(\beta) = 0$, um polinômio mônico $H \in R[X]$ com raiz $\alpha - \beta$ (respectivamente $\alpha \cdot \beta$). Tal construção, entretanto, é viável somente em casos bem simples. Em geral, é mais prático usar as condições equivalentes do seguinte teorema, que relaciona a propriedade de um elemento ser inteiro sobre R com a propriedade de um certo R -módulo ser finitamente gerado. (Neste contexto, usamos a palavra " R -módulo" no sentido de "submódulo do R -módulo S ".)

(1.1) **TEOREMA.** *Para qualquer $\alpha \in S$ as seguintes condições são equivalentes:*

- (i) α é inteiro sobre R .
- (ii) $R[\alpha]$ é um R -módulo finitamente gerado.
- (iii) Existe um subanel S' de S que é um R -módulo finitamente gerado e tal que $\alpha \in S'$.
- (iv) Existe um R -módulo finitamente gerado M tal que $\alpha \cdot M \subseteq M$ e que $\gamma \cdot M \neq \{0\}$ para todo $\gamma \in R[\alpha] \setminus \{0\}$.

Observamos que a condição (iv) será usada apenas no Exercício 1.2. Aliás, a última parte de (iv) se reduz à condição $M \neq \{0\}$ no caso em que S é um domínio.

Demonstração: (i) $\Rightarrow$ (ii): α é raiz de um polinômio $F = X^n + a_1 \cdot X^{n-1} + \dots + a_n \in R[X]$. Seja $M = R + R \cdot \alpha + \dots + R \cdot \alpha^{n-1}$; obviamente $M \subseteq R[\alpha]$. Supondo que $1, \alpha, \dots, \alpha^{n-1+k} \in M$, o que é trivial para $k = 0$, concluímos que $\alpha^{n+k} = -a_1 \cdot \alpha^{n-1+k} - \dots - a_n \cdot \alpha^k \in M$; logo $M = R[\alpha]$.

(ii) $\Rightarrow$ (iii): $S' = R[\alpha]$ tem a propriedade desejada.

(iii) $\Rightarrow$ (iv): $M = S'$ tem as propriedades desejadas uma vez que $\alpha \cdot S' \subseteq S'$ e $\gamma = \gamma \cdot 1 \in \gamma \cdot S'$.

(iv) $\Rightarrow$ (i): Seja $\beta_1, \dots, \beta_r$ um sistema de geradores de M . Como $\alpha \cdot M \subseteq M$, existem $a_{jk} \in R$ tais que $\alpha \cdot \beta_j = \sum_{k=1}^r a_{jk} \cdot \beta_k$ ($j = 1, \dots, r$), logo $\beta_1, \dots, \beta_r$ é uma solução do sistema homogêneo de equações lineares $\sum_{k=1}^r e_{jk} \cdot X_k = 0$

($j = 1, \dots, r$), onde $\varepsilon_{jk} = \alpha \cdot \delta_{jk} - a_{jk} \in R[\alpha]$. Temos $\varepsilon = \det(\varepsilon_{jk}) \in R[\alpha]$ e existem $\varepsilon_{ij}^* \in R[\alpha]$ tais que $\sum_{j=1}^r \varepsilon_{ij}^* \cdot \varepsilon_{jk} = \varepsilon \cdot \delta_{ik}$ ($i, k = 1, \dots, r$). Resulta que

$$0 = \sum_{j,k=1}^r \varepsilon_{ij}^* \cdot \varepsilon_{jk} \cdot \beta_k = \sum_{k=1}^r \varepsilon \cdot \delta_{ik} \cdot \beta_k = \varepsilon \cdot \beta_i \quad (i = 1, \dots, r),$$

logo $\varepsilon \cdot M = \{0\}$, e assim $\varepsilon = 0$. Concluimos que α é raiz do polinômio mônico $\det(X \cdot \delta_{jk} - a_{jk}) \in R[X]$; logo α é inteiro sobre R . $\square$

(1.2) COROLÁRIO. Se $\alpha_1, \dots, \alpha_m \in S$ forem inteiros sobre R então $R[\alpha_1, \dots, \alpha_m]$ será um R -módulo finitamente gerado.

Demonstração: Supomos que $R_k = R[\alpha_1, \dots, \alpha_k]$, considerado como R -módulo, possua um sistema finito $\beta_1, \dots, \beta_s$ de geradores, o que é trivial para $k=0$. Como α_{k+1} é inteiro sobre R_k , o anel $R_{k+1} = R_k[\alpha_{k+1}]$, considerado como R_k -módulo, possui um sistema finito de geradores $\gamma_1, \dots, \gamma_t$; logo, considerado como R -módulo, é gerado pelos produtos $\beta_i \cdot \gamma_j$ ($i = 1, \dots, s; j = 1, \dots, t$). Por indução, concluímos que R_m é um R -módulo finitamente gerado. $\square$

Denotando por $I_S(R)$ o conjunto dos elementos de S que são inteiros sobre R , demonstramos:

(1.3) COROLÁRIO. a) $I_S(R)$ é um subanel de S que contém R .
b) Todo subanel S' de S que é um R -módulo finitamente gerado, está contido em $I_S(R)$.

Demonstração: a) Obviamente $R \subseteq I_S(R) \subseteq S$. Sejam $\alpha, \beta \in I_S(R)$; então $\alpha - \beta, \alpha \cdot \beta \in R[\alpha, \beta]$, e $R[\alpha, \beta]$ é um R -módulo finitamente gerado, por (1.2); logo $\alpha - \beta, \alpha \cdot \beta \in I_S(R)$, por (1.1). Portanto, $I_S(R)$ é um subanel de S .

b) é uma consequência imediata de (1.1). $\square$

O anel $I_S(R)$ é chamado o *fecho inteiro* de R em S . Quando $I_S(R) = R$ diremos que R é *integralmente fechado* em S . Quando $I_S(R) = S$ diremos que S é *inteiro* sobre R . No caso de corpos $S = L$ e $R = K$, $I_L(K)$ é um subcorpo de L , a saber, o fecho algébrico de K em L . Em particular, teremos que $I_L(K) = K$ se e somente se K for algebricamente fechado em L , e $I_L(K) = L$ se e somente se a extensão $L|K$ for algébrica.

No caso em que $S = L$ é um corpo de números algébricos, o anel $I_L(\mathbb{Z})$ é chamado o *anel dos inteiros algébricos* de L e será denotado por I_L .

A propriedade de ser inteiro é transitiva no seguinte sentido.

(1.4) COROLÁRIO. *Sejam S um subanel de T e R um subanel de S . As seguintes condições são equivalentes:*

- (i) T é inteiro sobre S e S é inteiro sobre R .
- (ii) T é inteiro sobre R .

Demonstração. (i) $\Rightarrow$ (ii): Cada $\gamma \in T$ é raiz de um polinômio $X^m + \alpha_1 \cdot X^{m-1} + \dots + \alpha_m \in S[X]$. Como γ é inteiro sobre $S' = R[\alpha_1, \dots, \alpha_m]$, $S'[\gamma]$ é um S' -módulo finitamente gerado. Por (1.2), S' é um R -módulo finitamente gerado. Resulta que $S'[\gamma]$ é um R -módulo finitamente gerado; logo por (1.1), γ é inteiro sobre R . — A implicação (ii) $\Rightarrow$ (i) é imediata. $\square$

O nome “fecho inteiro” se justifica pelo fato de $I_S(\quad)$ ser uma *operação de fecho* no seguinte sentido.

(1.5) COROLÁRIO. *Seja $\mathcal{R}$ o conjunto dos subanéis de S . Por*

$$R \mapsto I_S(R) \quad (R \in \mathcal{R})$$

é definida uma aplicação de $\mathcal{R}$ em $\mathcal{R}$ tal que

$$R \subseteq I_S(R) = I_S(I_S(R)) \text{ e } [R \subseteq R' \Rightarrow I_S(R) \subseteq I_S(R')] \quad (R, R' \in \mathcal{R}).$$

Demonstração. A única afirmação não trivial é a inclusão $I_S(I_S(R)) \subseteq I_S(R)$, a qual resulta imediatamente de (1.4). $\square$

No caso $S = \mathbb{Q}$, o anel $I_S(\mathbb{Z}) = I_{\mathbb{Q}}$ coincide com o anel $\mathbb{Z}$ dos números inteiros racionais. Isto é uma consequência imediata do seguinte

(1.6) TEOREMA. *Todo domínio fatorial R é integralmente fechado no seu corpo de frações.*

Demonstração: Todo $x \in K = Q(R)$, $x \neq 0$, escreve-se como quociente $a \cdot b^{-1}$, onde $a, b \in R$, $\text{MDC}(a, b) = 1$. Se $x \in I_K(R)$, então existem $c_1, \dots, c_m \in R$ tais que $x^m + c_1 \cdot x^{m-1} + \dots + c_m = 0$. Multiplicando esta igualdade por b^m , obtemos $a^m + c_1 \cdot b \cdot a^{m-1} + \dots + c_m \cdot b^m = 0$; logo b é um divisor de a^m . De $\text{MDC}(a, b) = 1$ resulta que $b \in U(R)$; logo $x \in R$. $\square$

Supondo que $S = L$ é um corpo e R um subanel de S , estudaremos o corpo de frações do anel $I_L(R)$.

(1.7) TEOREMA. *Seja R um subanel do corpo L . Então*

$$Q(I_L(R)) = (I_L(R))_{R \setminus \{0\}} = I_L(Q(R)).$$

Em particular, $Q(I_L(R)) = L$ se e somente se L for algébrico sobre $Q(R)$.

Demonstração: Seja $\gamma \in Q(I_L(R))$, digamos $\gamma = \alpha \cdot \beta^{-1}$ onde $\alpha, \beta \in I_L(R)$, $\beta \neq 0$. Como $I_L(Q(R))$ é um subcorpo de L contendo $I_L(R)$, temos que $\gamma \in I_L(Q(R))$. — Para qualquer $\gamma \in I_L(Q(R))$ existem $a_1, \dots, a_m, d \in R$, $d \neq 0$, tais que $\gamma^m + a_1 \cdot d^{-1} \cdot \gamma^{m-1} + \dots + a_m \cdot d^{-1} = 0$. Multiplicando esta igualdade por d^m , obtemos que $\gamma \cdot d \in I_L(R)$, logo $\gamma \in (I_L(R))_{R \setminus \{0\}}$. — A inclusão $(I_L(R))_{R \setminus \{0\}} \subseteq Q(I_L(R))$ é óbvia. — A última afirmação resulta do fato que $I_L(Q(R)) = L$ se e somente se L for algébrico sobre $Q(R)$. $\square$

Aplicando (1.7) ao caso em que L é um corpo de números algébricos, obtemos o seguinte

(1.8) COROLÁRIO. *Seja L um corpo de números algébricos. Então*

$$Q(I_L) = (I_L)_{\mathbb{Z} \setminus \{0\}} = L.$$

Dados um corpo L qualquer e um subanel R de L , consideramos, para todo elemento $\gamma \in I_L(R)$, o seu polinômio minimal $P_{\gamma|K}$ sobre $K = Q(R)$. Apesar de γ ser raiz de algum polinômio mônico $F \in R[X]$, não podemos afirmar, em geral, que $P_{\gamma|K} \in R[X]$. A este respeito, podemos mostrar apenas o seguinte

(1.9) TEOREMA. *Seja R um subanel de L e seja $K = Q(R)$.*

- a) *Se F, G forem polinômios mônicos em $K[X]$ e $F \cdot G \in R[X]$, então $F, G \in I_K(R)[X]$.*
b) *Para qualquer $\gamma \in I_L(R)$ temos que $P_{\gamma|K} \in I_K(R)[X]$.*

Demonstração: a) Existem $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in \Omega$ (fecho algébrico de L) tais que $F = \prod_{i=1}^m (X - \alpha_i)$ e $G = \prod_{j=1}^n (X - \beta_j)$. De $F \cdot G \in R[X]$

resulta que $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in I_\Omega(R)$; portanto os coeficientes de F e G estão em $I_\Omega(R) \cap K = I_K(R)$.

b) γ é raiz de um polinômio mônico $H \in R[X]$; logo existe um polinômio mônico $G \in K[X]$ tal que $H = P_{\gamma|K} \cdot G$. De a) resulta que $P_{\gamma|K} \in I_K(R)[X]$. $\square$

Diremos que um domínio R é *integralmente fechado* se for integralmente fechado no seu corpo de frações $K = Q(R)$, isto é, se $I_K(R) = R$. Neste caso, podemos simplificar o teorema (1.9) substituindo $I_K(R)[X]$ por $R[X]$, e obtemos o seguinte corolário, o qual, por conveniência, formulamos não somente para $I_L(R)$ mas também para subanel S de $I_L(R)$.

(1.10) COROLÁRIO. *Sejam R um domínio integralmente fechado, L uma extensão finita de $K = Q(R)$ e S um subanel de $I_L(R)$ que contém R . Para qualquer $\gamma \in S$ temos que:*

- a) $P_{\gamma|K} \in R[X]$, $F_{\gamma,L|K} \in R[X]$, $\mathcal{N}_{L|K} \gamma \in R$, $\mathcal{F}_{L|K} \gamma \in R$.
- b) $\mathcal{N}_{L|K} \gamma$ é um múltiplo de γ no anel S .
- c) $\gamma \in U(S)$ se e somente se $\mathcal{N}_{L|K} \gamma \in U(R)$.
- d) Se $\mathcal{N}_{L|K} \gamma$ for irredutível em R então γ será irredutível em S .

Demonstração. Sem perda de generalidade podemos supor que $\gamma \neq 0$.

- a) Resulta de (1.9b) e da igualdade $F_{\gamma,L|K} = P_{\gamma|K}^m$, onde $m = [L : K(\gamma)]$.
- b) Como $F_{\gamma,L|K} = X^n + f_1 \cdot X^{n-1} + \dots + f_n \in R[X]$ e $\mathcal{N}_{L|K} \gamma = (-1)^n \cdot f_n$, temos que $\gamma^{-1} \cdot \mathcal{N}_{L|K} \gamma = (-1)^{n-1} \cdot (\gamma^{n-1} + f_1 \cdot \gamma^{n-2} + \dots + f_{n-1}) \in S$.
- c) Se $\gamma \cdot \delta = 1$ com $\delta \in S$, então $\mathcal{N}_{L|K} \gamma \cdot \mathcal{N}_{L|K} \delta = 1$, onde $\mathcal{N}_{L|K} \delta \in R$. — Por b) existe $\beta \in S$ tal que $\mathcal{N}_{L|K} \gamma = \gamma \cdot \beta$. Se $\mathcal{N}_{L|K} \gamma \in U(R)$ então $\beta \cdot (\mathcal{N}_{L|K} \gamma)^{-1}$ é o inverso de γ em S .
- d) resulta de c) e da multiplicatividade da norma. $\square$

Reformulamos (1.10) no caso especial em que $R = \mathbb{Z}$, observando que $\mathbb{Z}$ é integralmente fechado e está contido em qualquer subanel de I_L , e que $U(\mathbb{Z}) = \{1, -1\}$.

(1.11) COROLÁRIO. *Sejam L um corpo de números algébricos e S um subanel de I_L . Para qualquer $\gamma \in S$ temos que:*

- a) $P_{\gamma|\mathbb{Q}} \in \mathbb{Z}[X]$, $F_{\gamma,L|\mathbb{Q}} \in \mathbb{Z}[X]$, $\mathcal{N}_{L|\mathbb{Q}} \gamma \in \mathbb{Z}$, $\mathcal{F}_{L|\mathbb{Q}} \gamma \in \mathbb{Z}$.
- b) $\mathcal{N}_{L|\mathbb{Q}} \gamma$ é um múltiplo de γ no anel S .
- c) $\gamma \in U(S)$ se e somente se $|\mathcal{N}_{L|\mathbb{Q}} \gamma| = 1$.
- d) Se $|\mathcal{N}_{L|\mathbb{Q}} \gamma|$ for um número primo então γ será irredutível em S .

Este corolário mostra, em particular, que, para decidir se um número algébrico é inteiro ou não, basta considerar o seu polinômio minimal sobre $\mathbb{Q}$. Por exemplo, seja $\gamma = r \cdot \sqrt[p]{p}$, sendo $r \in \mathbb{Q} \setminus \{0\}$ e p, q números primos; então $P_{\gamma|\mathbb{Q}} = X^q - r^q \cdot p$; portanto, γ será um inteiro algébrico se e somente se $r \in \mathbb{Z}$, e certamente γ não é invertível em $I_{\mathbb{Q}(\gamma)}$.

É natural perguntar se é possível decidir se um elemento $\alpha \in L$ é um inteiro algébrico ou não, através de uma base apropriada de $L | \mathbb{Q}$. Mais precisamente, perguntamos se existe uma base $\beta_1, \dots, \beta_n$ de $L | \mathbb{Q}$ tal que $\alpha = \sum_{i=1}^n a_i \cdot \beta_i \in I_L$ se e somente se $a_1, \dots, a_n \in \mathbb{Z}$. Mostraremos no §5 que a resposta é afirmativa pois, para qualquer extensão L de $\mathbb{Q}$, de grau n , o anel I_L é um $\mathbb{Z}$ -módulo livre de posto n ; qualquer uma das suas bases é chamada uma *base integral* de L .

Em particular, indicaremos no §2 uma base integral para cada corpo quadrático L (isto é, tal que $[L : \mathbb{Q}] = 2$). Mostraremos, por exemplo, que $1, \sqrt{2}$ é uma base integral de $\mathbb{Q}(\sqrt{2})$, e que $1, \frac{1+\sqrt{5}}{2}$ é uma base integral de $\mathbb{Q}(\sqrt{5})$. Note-se que $1, \sqrt{5}$ não é uma base integral de $\mathbb{Q}(\sqrt{5})$, uma vez que $\frac{1}{2} + \frac{1}{2} \cdot \sqrt{5}$ é um inteiro algébrico.

A seguir, consideraremos domínios quaisquer R e S , R contido em S , e estudaremos as relações entre estes domínios no caso em que S é inteiro sobre R , isto é, $I_S(R) = S$.

(1.12) TEOREMA. *Seja o domínio S inteiro sobre R . Então:*

- a) *Para qualquer ideal $\mathfrak{A}$ não-nulo de S , $\mathfrak{A} \cap R$ é um ideal não-nulo de R .*
- b) $U(S) \cap R = U(R)$.
- c) *S será um corpo se e somente se R for um corpo.*
- d) *Um ideal primo $\mathfrak{P}$ de S será um ideal maximal de S se e somente se $\mathfrak{P} \cap R$ for um ideal maximal de R .*

Demonstração: a) Seja $\alpha \in \mathfrak{A} \neq 0$, e seja $X^n + a_1 \cdot X^{n-1} + \dots + a_n$ um polinômio em $R[X]$ de menor grau que tenha α como raiz. Então $a_n = -\alpha \cdot (\alpha^{n-1} + a_1 \cdot \alpha^{n-2} + \dots + a_{n-1}) \neq 0$ e $a_n \in \alpha \cdot S \cap R \subseteq \mathfrak{A} \cap R$.

b) Obviamente $U(S) \cap R \supseteq U(R)$. Seja $u \in U(S) \cap R$; então $u^{-1} \in S$; logo existem $c_1, \dots, c_m \in R$ tais que $u^{-m} + c_1 \cdot u^{-m+1} + \dots + c_m = 0$. Multiplicando esta igualdade por u^{m-1} , obtemos que

$$u^{-1} = -(c_1 + \dots + c_m \cdot u^{m-1}) \in R[u] \subseteq R; \text{ logo } u \in U(R).$$

c) Seja S um corpo. Então $U(S) = S \setminus \{0\}$, logo $U(R) = U(S) \cap R = R \setminus \{0\}$; portanto R é um corpo. — Se S não for um corpo, então possuirá um ideal não-nulo $\mathfrak{A}$ com $1 \notin \mathfrak{A}$. Por a), o ideal $\mathfrak{A} \cap R$ de R é não-nulo; logo R não é um corpo.

d) Seja κ o homomorfismo canônico de S sobre $S/\mathfrak{P}$. Obviamente $\kappa S = S/\mathfrak{P}$ é inteiro sobre o subanel κR , o qual é isomorfo a $R/(\mathfrak{P} \cap R)$. O ideal $\mathfrak{P}$ de S será maximal se e somente se $S/\mathfrak{P}$ for um corpo, o que, por c), ocorrerá se e somente se $R/(\mathfrak{P} \cap R)$ for um corpo, se e somente se $\mathfrak{P} \cap R$ for um ideal maximal de R . $\square$

Observemos que (1.12d) não é a única relação entre os ideais primos de S e os de R . De fato, a este respeito será provado mais tarde o teorema (1.1.10), do qual resulta em particular que, para todo ideal primo $\mathfrak{p}$ de R , existe um ideal primo $\mathfrak{P}$ de S tal que $\mathfrak{P} \cap R = \mathfrak{p}$. Outros fatos, que se referem à comparabilidade (relativa à inclusão) entre ideais primos de S , serão irrelevantes quando se considerar apenas o domínio I_L , uma vez que todos os seus ideais primos, exceto o ideal (0) , são maximais, como será mostrado a seguir.

(1.13) COROLÁRIO. *Seja o domínio S inteiro sobre R . Se todo ideal primo não-nulo de R for maximal então todo ideal primo não-nulo de S será maximal.*

Demonstração. Seja $\mathfrak{P}$ um ideal primo não-nulo de S . Então, por (1.12 a), $\mathfrak{P} \cap R$ é um ideal primo não-nulo de R , logo maximal, por hipótese. Por (1.12 d), $\mathfrak{P}$ é um ideal maximal de S . $\square$

É bem conhecido que $\mathbb{Z}$, e mais geralmente qualquer domínio principal, tem a propriedade indicada em (1.13). Portanto, todo domínio que for inteiro sobre $\mathbb{Z}$ terá a mesma propriedade. Disto resulta, em particular:

(1.14) COROLÁRIO. *Seja L um corpo de números algébricos. Então todo ideal primo não-nulo de I_L é um ideal maximal de I_L .*

Terminaremos este parágrafo mostrando duas importantes propriedades de finitude para corpos de números algébricos.

(1.15) TEOREMA. *Seja $[L:\mathbb{Q}] = n$ e sejam $\sigma_1, \dots, \sigma_n$ os isomorfismos de L em $\mathbb{C}$. Para qualquer $k \geq 1$ o conjunto*

$$\{\alpha \in I_L \mid |\sigma_1 \alpha| \leq k, \dots, |\sigma_n \alpha| \leq k\}$$

é finito.

Demonstração. Seja $\mathcal{M}$ o conjunto dos polinômios mônicos $F \in \mathbb{Z}[X]$ de grau n , cujos coeficientes tenham valor absoluto menor ou

igual a $\max\{\binom{n}{1} \cdot k, \dots, \binom{n}{n} \cdot k^n\}$. Como $\mathcal{M}$ é finito, basta mostrar que todo $\alpha \in I_L$ tal que $|\sigma_1 \alpha| \leq k, \dots, |\sigma_n \alpha| \leq k$ é raiz de um $F \in \mathcal{M}$. De fato, α é raiz do polinômio

$$F_{\alpha, L|Q} = \prod_{i=1}^n (X - \sigma_i \alpha) = X^n + \sum_{j=1}^n (-1)^j \cdot S_j(\sigma_1 \alpha, \dots, \sigma_n \alpha) \cdot X^{n-j} \in \mathbb{Z}[X],$$

onde S_j é o j -ésimo polinômio simétrico elementar em n indeterminadas.

Para todo $j = 1, \dots, n$ temos que $|S_j(\sigma_1 \alpha, \dots, \sigma_n \alpha)| =$

$$= \left| \sum_{1 \leq i_1 < \dots < i_j \leq n} \sigma_{i_1} \alpha \cdot \dots \cdot \sigma_{i_j} \alpha \right| \leq \sum_{1 \leq i_1 < \dots < i_j \leq n} |\sigma_{i_1} \alpha| \cdot \dots \cdot |\sigma_{i_j} \alpha| \leq \binom{n}{j} \cdot k^j; \text{ logo } F_{\alpha, L|Q} \in \mathcal{M}. \quad \square$$

Deste teorema resultará que o subgrupo de torção $W(L)$ do grupo multiplicativo $L^\times$ de L é finito, e que os seus elementos, as "raízes da unidade" em L , podem ser caracterizados por meio do valor absoluto dos seus conjugados. De fato;

(1.16) COROLÁRIO. Com as notações de (1.15) temos que

$$W(L) = \{\alpha \in I_L \mid |\sigma_1 \alpha| = \dots = |\sigma_n \alpha| = 1\},$$

e que $W(L)$ é finito.

Demonstração. $\subseteq$: Para qualquer $\eta \in W(L)$ existe $m \geq 1$ tal que $\eta^m = 1$. Portanto temos que $\eta \in I_L$ e $|\sigma_j \eta|^m = |\sigma_j \eta^m| = 1$; logo $|\sigma_j \eta| = 1$ para todo $j \in \{1, \dots, n\}$.

$\supseteq$: Seja $V = \{\alpha \in I_L \mid |\sigma_1 \alpha| = \dots = |\sigma_n \alpha| = 1\}$; é óbvio que se $\beta \in V$, então $\beta^m \in V$ para qualquer $m \in \mathbb{N}$. Como V é finito, por (1.15), existem $j, k \in \mathbb{N}$, $j < k$, tais que $\beta^j = \beta^k$, logo $\beta^{k-j} = 1$, logo $\beta \in W(L)$. $\square$

Observemos que a caracterização das raízes da unidade através do valor absoluto dos conjugados não se restringe a corpos de números algébricos (veja Exercício 1.8).

A segunda propriedade de finitude, a qual será usada somente no §18, se refere ao número de classes de elementos associados que têm como norma absoluta um dado número $k \in \mathbb{N}$.

(1.17) TEOREMA. Sejam $[L:\mathbb{Q}] = n$, S um subanel de L que, como $\mathbb{Z}$ -módulo, seja finitamente gerado, e $k \in \mathbb{N}$. Então, existem apenas um número finito de classes de elementos associados $U(S) \cdot \alpha_1, \dots, U(S) \cdot \alpha_m$ em S tais que $|\mathcal{N}_{L|Q} \alpha_i| = k$ ($i = 1, \dots, m$).

Demonstração. Seja $S = \mathbb{Z} \cdot \omega_1 + \dots + \mathbb{Z} \cdot \omega_r$; então todo $\alpha \in S$ é congruo mod $k \cdot S$ a (pelo menos) um dos elementos $d_1 \cdot \omega_1 + \dots + d_r \cdot \omega_r$ ($0 \leq d_i < k$, $i = 1, \dots, r$), isto é, existem no máximo k^r classes de S mod $k \cdot S$. Basta então provar que, se $\alpha, \beta \in S$ tais que $\alpha - \beta \in k \cdot S$ e $|\mathcal{N}_{L|\mathbb{Q}}\alpha| = |\mathcal{N}_{L|\mathbb{Q}}\beta| = k$, então α, β serão associados em S . De fato, por (1.3 b), S está contido em I_L e, por (1.11b), k é um múltiplo de α e de β em S , digamos $k = \alpha \cdot \alpha' = \beta \cdot \beta'$, com $\alpha', \beta' \in S$; portanto, de $\alpha - \beta = k \cdot \gamma$ resultam $\alpha = \beta \cdot (1 + \beta' \cdot \gamma)$ e $\beta = \alpha \cdot (1 - \alpha' \cdot \gamma)$; logo α, β são associados em S . $\square$

EXERCÍCIOS

- 1.1. Seja F um polinômio mônico em $\mathbb{Z}[X]$ e seja $\alpha \in \mathbb{C}$. Prove que se $F(\alpha)$ for um inteiro algébrico então α será um inteiro algébrico.
- 1.2. Sejam S um anel, R um subanel de S e β um elemento invertível em S . Prove que $R[\beta] \cap R[\beta^{-1}] \subseteq I_S(R)$. (Sugestão: Para cada $\alpha \in R[\beta] \cap R[\beta^{-1}]$ existe $n \in \mathbb{N}$ tal que $\alpha \cdot (R + R \cdot \beta + \dots + R \cdot \beta^n) \subseteq R + R \cdot \beta + \dots + R \cdot \beta^n$).
- 1.3. Sejam R um domínio, L uma extensão separável finita de $K = Q(R)$ e S um subanel de L que contenha R . Prove que existe $\alpha \in S$ tal que $Q(S) = K(\alpha)$.
- 1.4. Seja L um corpo de números algébricos. Prove:
 - a) Todo ideal não-nulo de I_L contém um número natural $n > 0$.
 - b) Todo subanel de L que é integralmente fechado em L contém I_L .
 - c) No caso em que $[L:\mathbb{Q}]$ é um número primo, $\mathbb{Z}$ é o único anel estritamente contido em I_L que é integralmente fechado (no seu corpo de frações).
- 1.5. Seja α um inteiro algébrico não-nulo. Prove que α^{-1} será um inteiro algébrico se e somente se $P_{\alpha|\mathbb{Q}}(0) \in \{1, -1\}$.
- 1.6. Sejam R um domínio, L uma extensão algébrica de $K = Q(R)$, $\alpha \in L$ e n o grau de $P = P_{\alpha|K}$. Supondo que $P \in R[X]$, prove:
 - a) $1, \alpha, \dots, \alpha^{n-1}$ formam uma base do R -módulo $R[\alpha]$.
 - b) O homomorfismo κ_α de $R[X]$ sobre $R[\alpha]$, definido por $F \mapsto F(\alpha)$ ($F \in R[X]$), tem como núcleo o ideal principal gerado por P .
 - c) Para todo ideal $\mathfrak{a}$ de R , κ_α induz um homomorfismo de $(R/\mathfrak{a})[X]$ sobre $R[\alpha]/\mathfrak{a} \cdot R[\alpha]$, cujo núcleo é o ideal principal gerado por $\bar{P}$ (= imagem de P pelo homomorfismo canônico de $R[X]$ sobre $(R/\mathfrak{a})[X]$).

1.7. Seja L um corpo de números algébricos. Prove:

- Todo elemento primo π de I_L divide um e um só número primo p .
- Se $\alpha \in I_L$ dividir o número primo p , então $\mathcal{N}_{L|\mathbb{Q}}\alpha \in \{p^k, -p^k\}$ para algum $k \in \{0, \dots, [L:\mathbb{Q}]\}$; em particular, α será associado a p se e somente se $k = [L:\mathbb{Q}]$.

1.8. Para qualquer $\zeta \in \mathbb{C}$ as seguintes condições são equivalentes:

- Existe $n \geq 1$ tal que $\zeta^n = 1$ (ou seja, ζ é uma raiz da unidade).
- ζ é raiz de um polinômio mônico em $\mathbb{Z}[X]$ cujas raízes têm valor absoluto igual a 1.
- ζ é um inteiro algébrico tal que todos os seus conjugados (sobre $\mathbb{Q}$) tenham valor absoluto igual a 1.

§2. Corpos quadráticos

Consideraremos neste parágrafo *corpos quadráticos*, isto é, subcorpos L de $\mathbb{C}$ tais que $[L:\mathbb{Q}] = 2$.

Observamos que qualquer $\alpha \in L \setminus \mathbb{Q}$ é um elemento primitivo da extensão $L|\mathbb{Q}$ (uma vez que de $1 < [\mathbb{Q}(\alpha):\mathbb{Q}] \leq [L:\mathbb{Q}] = 2$ decorre que $\mathbb{Q}(\alpha) = L$), os elementos $1, \alpha$ formam uma base desta extensão, e $P_{\alpha|\mathbb{Q}} = F_{\alpha,L|\mathbb{Q}}$ é um polinômio em $\mathbb{Q}[X]$ de grau 2. Para cada $r \in \mathbb{Q} \setminus \{0\}$ denotamos por $\sqrt{r}$ uma das raízes do polinômio $X^2 - r$; a outra raiz é $-\sqrt{r}$.

Mostraremos que todo corpo quadrático possui um elemento primitivo distinguido da forma $\sqrt{d}$, univocamente determinado a menos do sinal, onde d é um número inteiro “livre de quadrados”. Mais precisamente, denotando por $\mathcal{D}$ o conjunto dos números $d \in \mathbb{Z} \setminus \{0, 1\}$ que não são divisíveis por nenhum quadrado $c^2 \neq 1$ (onde $c \in \mathbb{Z}$), mostraremos o seguinte:

(2.1) A aplicação definida por $d \mapsto \mathbb{Q}(\sqrt{d})$ ($d \in \mathcal{D}$) é uma bijeção de $\mathcal{D}$ sobre o conjunto de todos os corpos quadráticos.

Demonstração. Para qualquer $d \in \mathcal{D}$ temos que $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}] \leq 2$, pois $P_{\sqrt{d}|\mathbb{Q}}$ divide $X^2 - d$. Vale a igualdade, pois caso contrário teríamos que $\sqrt{d} \in \mathbb{Q}$, logo $\sqrt{d} \in \mathbb{Z}$ e, portanto, $d = (\sqrt{d})^2 \notin \mathcal{D}$, o que é absurdo. — Para provar que a aplicação é injetiva, supomos que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$, onde $d, d' \in \mathcal{D}$. Existem $r, s \in \mathbb{Q}$ tais que $\sqrt{d'} = r + s \cdot \sqrt{d}$; logo $d' = r^2 + s^2 \cdot d + 2r \cdot s \cdot \sqrt{d}$; concluímos que $r \cdot s = 0$, logo $r = 0$ ou $s = 0$. A igualdade $s = 0$ implicaria que $\sqrt{d'} = r \in I_L \cap \mathbb{Q} = \mathbb{Z}$, logo $d' \notin \mathcal{D}$, o que é impossível; portanto

temos que $r=0$, $d'=s^2 \cdot d$. Nas fatorações de d' e de d , todo número primo p ocorre com um expoente 0 ou 1; na fatoração de s^2 , porém, com um expoente par; donde resulta que $s^2=1$, $d'=d$. — Mostremos que a aplicação é sobrejetiva. Seja $L=\mathbb{Q}(\alpha)$ um corpo quadrático com $P_{\alpha|\mathbb{Q}}=X^2+a \cdot X+b \in \mathbb{Q}[X]$.

Pondo $\beta=\alpha+\frac{a}{2}$, temos que $L=\mathbb{Q}(\beta)$ e $P_{\beta|\mathbb{Q}}=X^2-\left(\frac{a^2}{4}-b\right)$. Vê-se fa-

cilmente que existem $d \in \mathcal{D}$ e $r \in \mathbb{Q} \setminus \{0\}$ tais que $\frac{a^2}{4}-b=r^2 \cdot d$; obviamente $L=\mathbb{Q}(\sqrt{d})$. $\square$

Usando 1, $\sqrt{d}$ como base da extensão $L=\mathbb{Q}(\sqrt{d})$ de $\mathbb{Q}$, o polinômio característico de qualquer elemento $\alpha=r+s \cdot \sqrt{d} \in L$ é obtido como

$$F_{\alpha,L|\mathbb{Q}} = \det \begin{pmatrix} X-r & -s \\ -s \cdot d & X-r \end{pmatrix} = X^2 - 2r \cdot X + r^2 - s^2 \cdot d,$$

uma vez que $\alpha=r+s \cdot \sqrt{d}$ e $\alpha \cdot \sqrt{d}=s \cdot d+r \cdot \sqrt{d}$. Seus coeficientes, além do coeficiente dominante 1, são o negativo do traço $\mathcal{T}_{L|\mathbb{Q}}\alpha=2r$ e a norma $\mathcal{N}_{L|\mathbb{Q}}\alpha=r^2-s^2 \cdot d$. É importante observar que a norma será sempre não-negativa quando $d < 0$.

Ainda usando esta base, determinamos o anel I_L dos inteiros algébricos de L da seguinte maneira.

(2.2) Seja $L=\mathbb{Q}(\sqrt{d})$ onde $d \in \mathcal{D}$. Então

$$I_L = \left\{ \frac{m}{2} + \frac{n}{2} \cdot \sqrt{d} \mid m, n \in \mathbb{Z}; m^2 \equiv n^2 \cdot d \pmod{4} \right\}.$$

Demonstração. $\supseteq$: Se $\alpha = \frac{m}{2} + \frac{n}{2} \cdot \sqrt{d}$ tal que $m, n \in \mathbb{Z}$ e $m^2 \equiv n^2 \cdot d \pmod{4}$,

então $\mathcal{T}_{L|\mathbb{Q}}\alpha = m$ e $\mathcal{N}_{L|\mathbb{Q}}\alpha = \frac{m^2}{4} - \frac{n^2}{4} \cdot d \in \mathbb{Z}$; logo $F_{\alpha,L|\mathbb{Q}} \in \mathbb{Z}[X]$ e assim $\alpha \in I_L$.

$\subseteq$: Sejam $r, s \in \mathbb{Q}$ tais que $\alpha = r + s \cdot \sqrt{d} \in I_L$; então $2r = \mathcal{T}_{L|\mathbb{Q}}\alpha \in \mathbb{Z}$ e $r^2 - s^2 \cdot d = \mathcal{N}_{L|\mathbb{Q}}\alpha \in \mathbb{Z}$; logo $(2s)^2 \cdot d = (2r)^2 - 4 \cdot (r^2 - s^2 \cdot d) \in \mathbb{Z}$. Sendo $k_p \in \mathbb{Z}$ (respectivamente $e_p \in \{0, 1\}$), o expoente do número primo p na fatoração de $2s$ (respectivamente de d), concluímos de $(2s)^2 \cdot d \in \mathbb{Z}$ que $2k_p + e_p \geq 0$; logo $k_p \geq 0$; portanto $2s \in \mathbb{Z}$. Resulta que $\alpha = \frac{m}{2} + \frac{n}{2} \cdot \sqrt{d}$ onde $m = 2r \in \mathbb{Z}$ e $n = 2s \in \mathbb{Z}$, e que $m^2 - n^2 \cdot d = 4 \cdot (r^2 - s^2 \cdot d)$ é um múltiplo de 4. $\square$

A representação, indicada em (2.2), dos inteiros algébricos de L como elementos do $\mathbb{Z}$ -módulo $\mathbb{Z} \cdot \frac{1}{2} + \mathbb{Z} \cdot \frac{\sqrt{d}}{2}$, cujos coeficientes satisfazem uma certa congruência, ainda não é satisfatória. Mostraremos a seguir que I_L é um $\mathbb{Z}$ -módulo livre, mas a base $1, \sqrt{d}$ é uma base integral de L somente nos casos em que $d \equiv 2$ ou $3 \pmod{4}$, devendo ser substituída por $1, \frac{1+\sqrt{d}}{2}$ no caso em que $d \equiv 1 \pmod{4}$.

(2.3) TEOREMA. Seja $L = \mathbb{Q}(\sqrt{d})$ onde $d \in \mathcal{D}$, e seja $\delta = \sqrt{d}$ (respectivamente $= \frac{1+\sqrt{d}}{2}$) no caso em que $d \equiv 2$ ou $3 \pmod{4}$ (respectivamente $\equiv 1 \pmod{4}$). Então, $1, \delta$ formam uma base do $\mathbb{Z}$ -módulo I_L .

Demonstração. Os elementos $1, \delta$ são linearmente independentes sobre $\mathbb{Z}$, pois o são sobre $\mathbb{Q}$; por isto basta provar que $\mathbb{Z} + \mathbb{Z} \cdot \delta = I_L$. Por (2.2) temos que $\delta \in I_L$, logo $\mathbb{Z} + \mathbb{Z} \cdot \delta \subseteq I_L$. Para provar a inclusão inversa, observamos que qualquer $\alpha \in I_L$ é da forma $\frac{m}{2} + \frac{n}{2} \cdot \sqrt{d}$, com $m, n \in \mathbb{Z}$ e $m^2 \equiv n^2 \cdot d \pmod{4}$, por (2.2). No caso em que $d \equiv 1 \pmod{4}$, temos que $m^2 \equiv n^2 \pmod{4}$, logo m, n têm a mesma paridade, digamos $m = 2k + n$ com $k \in \mathbb{Z}$; logo $\alpha = k + n \cdot \frac{1+\sqrt{d}}{2} = k + n \cdot \delta$. No caso em que $d \equiv 2$ ou $3 \pmod{4}$, basta mostrar que m e n são pares. Se n fosse ímpar teríamos que $n^2 \equiv 1 \pmod{4}$, logo $m^2 \equiv n^2 \cdot d \equiv d \pmod{4}$ e, portanto, $d \equiv 0$ ou $\equiv 1 \pmod{4}$, o que é absurdo. Concluimos que n é par, e de $m^2 \equiv n^2 \cdot d \equiv 0 \pmod{4}$ decorre que m também é par. $\square$

É fácil ver que, para qualquer $d \in \mathcal{D}$, apenas uma das seguintes inclusões

$$\mathbb{Z}[\sqrt{d}] \subseteq I_L \subseteq \mathbb{Z} \left[\frac{1+\sqrt{d}}{2} \right]$$

é a igualdade, a saber, a primeira (respectivamente a segunda) no caso em que $d \equiv 2$ ou $3 \pmod{4}$ (respectivamente $\equiv 1 \pmod{4}$). Note que estes domínios têm L como corpo de frações, e que no caso $d \equiv 1 \pmod{4}$ o domínio $\mathbb{Z}[\sqrt{d}]$ não é integralmente fechado (veja Exercício 1.4.b) e portanto não é fatorial, devido a (1.6).

Mais interessante, entretanto, é a questão se o próprio anel I_L , o qual obviamente é integralmente fechado, é um domínio fatorial ou não. O contra-exemplo mais conhecido é o seguinte:

(2.4) Seja $L = \mathbb{Q}(\sqrt{-5})$. O domínio $I_L = \mathbb{Z}[\sqrt{-5}]$ não é fatorial.

Demonstração. Como $(1 + 2 \cdot \sqrt{-5}) \cdot (1 - 2 \cdot \sqrt{-5}) = 3 \cdot 7$ e $\frac{1}{3} \cdot (1 \pm 2 \cdot \sqrt{-5}) \notin I_L$, basta mostrar que os fatores $1 + 2 \cdot \sqrt{-5}$, $1 - 2 \cdot \sqrt{-5}$, 3 e 7 são irredutíveis em I_L . Como eles têm norma 21, 21, 9, 49, respectivamente, eles não são invertíveis em I_L por (1.11). Se $1 + 2 \cdot \sqrt{-5}$ fosse redutível, isto é, se existissem $\alpha, \beta \in I_L \setminus U(I_L)$ tais que $1 + 2 \cdot \sqrt{-5} = \alpha \cdot \beta$, então teríamos que $21 = \mathcal{N}_{L/\mathbb{Q}} \alpha \cdot \mathcal{N}_{L/\mathbb{Q}} \beta$, logo $\mathcal{N}_{L/\mathbb{Q}} \alpha \in \{3, -3, 7, -7\}$. Mas isto é impossível pois $\mathcal{N}_{L/\mathbb{Q}}(m + n \cdot \sqrt{-5}) = m^2 + n^2 \cdot 5 \notin \{3, -3, 7, -7\}$, quaisquer que sejam $m, n \in \mathbb{Z}$. A irredutibilidade de $1 - 2 \cdot \sqrt{-5}$, 3 e 7 é provada analogamente. $\square$

Exemplos de corpos quadráticos L tais que I_L seja fatorial podem ser obtidos usando-se a noção de domínio euclidiano. Diremos que um domínio R é *euclidiano* se existir uma aplicação $\partial : R \setminus \{0\} \rightarrow \mathbb{N}$ com as seguintes propriedades: Para quaisquer $a, b \in R \setminus \{0\}$,

- (i) de $a|b$ decorre $\partial a \leq \partial b$
- (ii) existem $q, r \in R$ tais que $a = q \cdot b + r$ e $[r = 0 \text{ ou } \partial r < \partial b]$.

É fácil mostrar:

(2.5) Todo domínio euclidiano é principal e, portanto, fatorial.

Demonstração. Dado um ideal não-nulo $\mathfrak{a}$ de R , existe $b \in \mathfrak{a} \setminus \{0\}$ tal que ∂b seja minimal em $\{\partial a \mid a \in \mathfrak{a} \setminus \{0\}\}$. Para qualquer $a \in \mathfrak{a}$ sejam $q, r \in R$ tais que $a = q \cdot b + r$ e $[r = 0 \text{ ou } \partial r < \partial b]$. Como $r = a - q \cdot b \in \mathfrak{a}$, a desigualdade $\partial r < \partial b$ é impossível devido à minimalidade de ∂b ; portanto $r = 0$, $a = q \cdot b \in (b)$. Concluimos que $\mathfrak{a} = (b)$. Resulta que R é um domínio principal, logo fatorial. $\square$

Os exemplos mais conhecidos de domínios euclidianos são $\mathbb{Z}$ e o anel de polinômio $K[X]$, sobre um corpo K qualquer, sendo a aplicação ∂ igual ao valor absoluto e ao grau de polinômio, respectivamente.

No caso do anel I_L dos inteiros algébricos de um corpo quadrático $L = \mathbb{Q}(\sqrt{d})$, um candidato natural para a aplicação ∂ é a norma absoluta

(restrita a $I_L \setminus \{0\}$), isto é, a aplicação definida por $\alpha \mapsto |\mathcal{N}_{L|\mathbb{Q}} \alpha|$, a qual obviamente satisfaz a condição (i) da definição acima e que, como veremos a seguir, em certos casos satisfaz também a condição (ii). Note-se que, no caso $d < 0$, a norma absoluta coincide com a própria norma uma vez que, neste caso, $\mathcal{N}_{L|\mathbb{Q}} \alpha \geq 0$ para qualquer $\alpha \in L$. O exemplo mais importante é o do anel dos inteiros de Gauss $\mathbb{Z}[i]$, igual ao anel I_L dos inteiros algébricos do corpo dos números de Gauss $L = \mathbb{Q}(i)$ (sendo $i = \sqrt{-1}$):

(2.6) $\mathbb{Z}[i]$ é euclidiano em relação à norma $\mathcal{N}_{\mathbb{Q}(i)|\mathbb{Q}}$.

Demonstração: Dados elementos não-nulos $\alpha, \beta \in \mathbb{Z}[i]$, existem $u, v \in \mathbb{Q}$ tais que $\alpha \cdot \beta^{-1} = u + v \cdot i$. Existem $m, n \in \mathbb{Z}$ tais que $|u - m| \leq \frac{1}{2}$ e $|v - n| \leq \frac{1}{2}$. Temos que $\alpha = (m + n \cdot i) \cdot \beta + \rho$, onde $\rho = [(u - m) + (v - n) \cdot i] \cdot \beta = \alpha - (m + n \cdot i) \cdot \beta \in \mathbb{Z}[i]$, e $0 \leq \mathcal{N}_{\mathbb{Q}(i)|\mathbb{Q}} \rho = [(u - m)^2 + (v - n)^2] \cdot \mathcal{N}_{\mathbb{Q}(i)|\mathbb{Q}} \beta < \mathcal{N}_{\mathbb{Q}(i)|\mathbb{Q}} \beta$; portanto $m + ni$ e ρ (em lugar de q e r) têm a propriedade indicada em (ii). $\square$

De maneira análoga mostra-se que $I_{\mathbb{Q}(\sqrt{d})}$ é euclidiano, em relação à norma, para $d \in \{-2, -3, -7, -11\}$, e estes números, além de -1 , são os únicos $d \in \mathscr{D}$ negativos com esta propriedade (veja Exercício 2.6). Além disto, $\{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$ é o conjunto dos $d \in \mathscr{D}$ positivos para os quais $I_{\mathbb{Q}(\sqrt{d})}$ é euclidiano em relação à norma absoluta (veja Barnes, Swinnerton-Dyer [5]). Não se sabe se existem outros $d \in \mathscr{D}$ tais que o domínio indicado seja euclidiano em relação a uma função ∂ diferente da norma absoluta (veja Stewart-Tall [33], p. 92).

Para I_L ser um domínio fatorial é suficiente, mas não é necessário, que ele seja euclidiano. De fato, $\{-19, -43, -67, -163\}$ é o conjunto dos $d \in \mathscr{D}$ negativos tais que $I_{\mathbb{Q}(\sqrt{d})}$ seja fatorial mas não euclidiano em relação à norma absoluta (veja Baker [4], Theorem 5.1). Existem também muitos $d \in \mathscr{D}$ positivos com esta propriedade, mas ainda é um problema em aberto se existe uma infinidade de números positivos $d \in \mathscr{D}$ tais que $I_{\mathbb{Q}(\sqrt{d})}$ seja fatorial (conjetura de Gauss).

Mencionamos neste contexto que, para qualquer corpo de números algébricos L , o anel I_L será fatorial se e somente se for um domínio principal, se e somente se o seu "número de classes" h_L for igual a 1 (veja §8).

Diremos que um corpo quadrático L é real quando $L \subseteq \mathbb{R}$; caso contrário, ele é chamado imaginário. Sendo $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathscr{D}$, é óbvio

que L será real (respectivamente imaginário) se e somente se $d > 0$ (respectivamente < 0). A distinção entre os corpos quadráticos reais e os imaginários será importante quando se estudar o grupo $U(I_L)$ dos elementos invertíveis de I_L .

Mostraremos a seguir que, para qualquer corpo quadrático imaginário L , o grupo $U(I_L)$ é igual a $\{1, -1\}$ exceto nos casos $d = -1$ e $d = -3$, nos quais é cíclico de ordem 4 e 6, respectivamente.

(2.7) TEOREMA. Seja $L = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathcal{D}$, $d < 0$.

- a) No caso $d = -1$, $U(I_L)$ consiste dos elementos $1, i, i^2 = -1, i^3 = -i$.
- b) No caso $d = -3$, $U(I_L)$ consiste dos elementos $1, \zeta, \zeta^2, \zeta^3 = -1, \zeta^4, \zeta^5$, onde $\zeta = \frac{1 + \sqrt{-3}}{2}$.
- c) Nos casos $d \notin \{-1, -3\}$ temos que $U(I_L) = \{1, -1\}$.

Demonstração. Notamos que $\mathcal{N}_{L/\mathbb{Q}}(u + v \cdot \sqrt{d}) = u^2 - v^2 \cdot d = u^2 + v^2 \cdot |d| \geq 0$ para quaisquer $u, v \in \mathbb{Q}$. Consideremos primeiro o caso em que $d \equiv 2$ ou $3 \pmod{4}$. Por (2.3), todo $\alpha \in I_L$ é da forma $m + n \cdot \sqrt{d}$, com $m, n \in \mathbb{Z}$, e por (1.11), teremos que $\alpha \in U(I_L)$ se e somente se $m^2 + n^2 \cdot |d| = 1$. Quando $d = -1$, isto ocorrerá se e somente se $(m, n) \in \{(1, 0), (0, 1), (-1, 0), (0, -1)\}$, se e somente se $\alpha \in \{1, i, -1, -i\}$. Quando $d \neq -1$, isto ocorrerá se e somente se $(m, n) \in \{(1, 0), (-1, 0)\}$, se e somente se $\alpha \in \{1, -1\}$.

No caso em que $d \equiv 1 \pmod{4}$, os elementos $\alpha \in I_L$ são da forma $\frac{m}{2} + \frac{n}{2} \cdot \sqrt{d}$, com $m, n \in \mathbb{Z}$, $m^2 \equiv n^2 \pmod{4}$ ou seja, $m \equiv n \pmod{2}$ (veja (2.2)).

Por (1.11), teremos que $\alpha \in U(I_L)$ se e somente se $\frac{m^2}{4} + \frac{n^2}{4} \cdot |d| = 1$, ou seja, $m^2 + n^2 \cdot |d| = 4$. Quando $d \neq -3$, isto ocorrerá se e somente se $(m, n) \in \{(2, 0), (-2, 0)\}$, se e somente se $\alpha \in \{1, -1\}$. Quando $d = -3$, isto ocorrerá se e somente se $(m, n) \in \{(2, 0), (1, 1), (-1, 1), (-2, 0), (-1, -1), (1, -1)\}$, se e somente se

$$\alpha \in \left\{ 1, \frac{1 + \sqrt{-3}}{2}, \frac{-1 + \sqrt{-3}}{2}, -1, \frac{-1 - \sqrt{-3}}{2}, \frac{1 - \sqrt{-3}}{2} \right\}.$$

Note que estes elementos são as potências $\zeta^0, \zeta^1, \zeta^2, \zeta^3, \zeta^4, \zeta^5$ de $\zeta = \frac{1 + \sqrt{-3}}{2}$. $\square$

Por outro lado, para qualquer corpo quadrático *real* L , o grupo $U(I_L)$ é produto direto de $\{1, -1\}$ e de um subgrupo cíclico infinito, que é gerado por um elemento $\varepsilon > 1$, chamado o *invertível fundamental* de I_L . Isto será demonstrado no §19, como caso particular do teorema de invertíveis de Dirichlet. Por exemplo, no caso $L = \mathbb{Q}(\sqrt{2})$ vê-se facilmente que $1 + \sqrt{2}$ é um elemento de $U(I_L)$ de ordem infinita; veremos no §19 que $1 + \sqrt{2}$ é o invertível fundamental de I_L .

Terminaremos este parágrafo com um estudo mais detalhado do anel $\mathbb{Z}[i]$ dos inteiros de Gauss. Daremos uma resposta completa à questão de como os números primos $p \in \mathbb{Z}$ se fatoram em $\mathbb{Z}[i]$. Antes, porém, mostraremos que esta questão está ligada ao problema de determinar os números primos que são somas de dois quadrados $m^2 + n^2$, com $m, n \in \mathbb{Z}$.

(2.8) *Seja p um número primo e sejam $m, n \in \mathbb{Z}$. As seguintes condições são equivalentes:*

- (i) $p = m^2 + n^2$
- (ii) $m + n \cdot i$ é um divisor próprio de p , não-invertível em $\mathbb{Z}[i]$.

Neste caso temos que $m \neq 0 \neq n$; os elementos $m + n \cdot i$, $m - n \cdot i$ são primos em $\mathbb{Z}[i]$ e $p = (m + n \cdot i) \cdot (m - n \cdot i)$.

Demonstração. Obviamente, $\mathcal{N}(m + n \cdot i) = \mathcal{N}(m - n \cdot i) = (m + n \cdot i) \cdot (m - n \cdot i) = m^2 + n^2 \geq 0$ (sendo $\mathcal{N} = \mathcal{N}_{\mathbb{Q}(i)|\mathbb{Q}}$).

(i) $\Rightarrow$ (ii): De $p = m^2 + n^2$ resulta que $m \neq 0 \neq n$; logo $m + n \cdot i$ e $m - n \cdot i$ não são invertíveis em $\mathbb{Z}[i]$, por (2.7), e portanto são divisores próprios de p . Além disto, são irredutíveis em $\mathbb{Z}[i]$, por (1.11 d), e mesmo primos, devido a (2.6) e (2.5).

(ii) $\Rightarrow$ (i): Existe $\alpha \in \mathbb{Z}[i] \setminus U(\mathbb{Z}[i])$ tal que $p = (m + n \cdot i) \cdot \alpha$, e de (1.11 c) resulta que $\mathcal{N}\alpha \neq 1 \neq \mathcal{N}(m + n \cdot i)$. Como $p^2 = \mathcal{N}p = \mathcal{N}(m + n \cdot i) \cdot \mathcal{N}\alpha$, concluímos que $\mathcal{N}(m + n \cdot i) = p$. $\square$

Os números primos p que satisfazem as condições equivalentes de (2.8), para certos $m, n \in \mathbb{Z}$, são aqueles que se tornam redutíveis em $\mathbb{Z}[i]$. O seguinte teorema mostra que estes são exatamente os números primos $p \equiv 1 \pmod{4}$ e $p = 2$.

(2.9) TEOREMA. a) *Se $p \equiv 3 \pmod{4}$, então p é irredutível em $\mathbb{Z}[i]$.*

b) *Se $p \equiv 1 \pmod{4}$, então existem números $m, n \in \mathbb{Z}$, m positivo e par, n ímpar, tais que $p = (m + n \cdot i) \cdot (m - n \cdot i)$. Os elementos $m + n \cdot i$,*

$m - n \cdot i$ são irredutíveis não-associados em $\mathbb{Z}[i]$.

c) $2 = i \cdot (1 - i)^2$, e $1 - i$ é irredutível em $\mathbb{Z}[i]$.

Demonstração. a) Se p for redutível em $\mathbb{Z}[i]$, então existirão $m, n \in \mathbb{Z}$ tais que $p = m^2 + n^2$, por (2.8). Obviamente, m^2 e n^2 são congruos a 0 ou 1 mod 4, logo $p = m^2 + n^2 \equiv 0$ ou 1 ou 2 mod 4; portanto $p \not\equiv 3 \pmod{4}$.

b) Seja μ um gerador do grupo multiplicativo $\mathbb{F}_p^*$ do corpo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, o qual é cíclico de ordem $p - 1$ (veja (3.1)). Seu único subgrupo de ordem 2 é gerado pelo elemento $-1 = \mu^{\frac{p-1}{2}}$, o qual é um quadrado em $\mathbb{F}_p^*$, pois

$4 \mid p - 1$. Seja $h \in \mathbb{Z}$ um representante de $\mu^{\frac{p-1}{4}}$; então $h^2 \equiv -1 \pmod{p}$, ou seja, p divide $h^2 + 1 = (h + i) \cdot (h - i)$. Como $\mathbb{Z}[i]$ é fatorial, existe um elemento primo π de $\mathbb{Z}[i]$ tal que $\pi \mid p$; portanto π divide $h + i$ ou $h - i$. Por outro lado, p obviamente não divide $h + i$ nem $h - i$; logo π é um divisor próprio de p . De (2.8) resulta que existem $m, n \in \mathbb{Z} \setminus \{0\}$ tais que $p = m^2 + n^2 = (m + n \cdot i) \cdot (m - n \cdot i)$, e ambos os fatores são irredutíveis em $\mathbb{Z}[i]$. Como $p \equiv 1 \pmod{4}$, m e n têm paridades diferentes. Substituindo, se necessário, $m + n \cdot i$ por um dos elementos associados $-m - n \cdot i$, $n - m \cdot i$, $-n + m \cdot i$, podemos assumir que m é positivo e par e n é ímpar. Obviamente, os elementos $m + n \cdot i$ e $m - n \cdot i$ não são associados em $\mathbb{Z}[i]$.

c) Temos que $2 = (1 + i) \cdot (1 - i) = i \cdot (1 - i)^2$ e, por (2.8), $1 - i$ é irredutível em $\mathbb{Z}[i]$. $\square$

Como consequência de (2.8) e (2.9) obtemos imediatamente o seguinte resultado devido a Fermat:

(2.10) COROLÁRIO. Para qualquer número primo p , as seguintes condições são equivalentes:

- (i) Existem $m, n \in \mathbb{Z}$ tais que $p = m^2 + n^2$.
- (ii) p é redutível em $\mathbb{Z}[i]$.
- (iii) $p = 2$ ou $p \equiv 1 \pmod{4}$.

O Teorema (2.9) será generalizado mais tarde, no §15, a qualquer corpo quadrático L . Em particular, será mostrado que cada número primo p é de um dos seguintes tipos:

- (a) p é inerte em L , isto é, continua irredutível em L ;
- (b) p é decomposto em L , isto é, é um produto de dois elementos irredutíveis, não-associados em L ;

- (c) p é ramificado em I_L , isto é, é associado ao quadrado de um elemento irredutível em I_L .

sendo que o último caso ocorre apenas para um número finito de primos p . Na verdade, as definições de “inerte”, “decomposto” e “ramificado” acima indicadas se aplicam apenas ao caso em que I_L é fatorial. No caso geral, elas devem ser substituídas por definições análogas, que se referem aos ideais maximais de I_L .

EXERCÍCIOS

- 2.1. Mostre que $\frac{5+3\sqrt{2}}{1+\sqrt{2}}$ é um inteiro algébrico e determine seu polinômio minimal sobre $\mathbb{Q}$.
- 2.2. Seja $L = \mathbb{Q}(\sqrt{d})$ onde $d \in \mathcal{D}$. Indique todos os $r, s \in \mathbb{Q}$ tais que $1, r+s\sqrt{d}$ formem uma base integral de L .
(Distinga os casos $d \equiv 1 \pmod{4}$ e $d \equiv 2$ ou $3 \pmod{4}$.)
- 2.3. Para cada um dos pares $(a, b) \in \{(2+3i, 1+i), (3-2i, 1+2i), (4+5i, 2-i)\}$ determine $q, r \in \mathbb{Z}[i]$ tais que $a = q \cdot b + r$ e $\mathcal{N}_{\mathbb{Q}(i)|\mathbb{Q}} r < \mathcal{N}_{\mathbb{Q}(i)|\mathbb{Q}} b$.
- 2.4. Prove que os domínios $\mathbb{Z}[\sqrt{-3}]$ e $\mathbb{Z}[\sqrt{65}]$ não são fatoriais.
- 2.5. a) Seja $L = \mathbb{Q}(\sqrt{-26})$. Mostre que $3, 1+\sqrt{-26}$ e $1-\sqrt{-26}$ são irredutíveis em I_L e conclua que I_L não é fatorial.
b) Seja $L = \mathbb{Q}(\sqrt{10})$. Mostre que $2, 3, 4+\sqrt{10}$ e $4-\sqrt{10}$ são irredutíveis em I_L e conclua que I_L não é fatorial.
c) Seja $L = \mathbb{Q}(\sqrt{-19})$. Porque a igualdade

$$(4 + \sqrt{-19}) \cdot (4 - \sqrt{-19}) = 5 \cdot 7$$
 não contradiz o fato de I_L ser fatorial?
- 2.6. Seja $L = \mathbb{Q}(\sqrt{d})$ onde $d \in \mathcal{D}$.
- a) Prove que as seguintes condições são equivalentes:
- (i) I_L é euclidiano em relação à norma absoluta.
 - (ii) Para qualquer $\lambda \in L$ existe $\alpha \in I_L$ tal que $|\mathcal{N}_{L|\mathbb{Q}}(\lambda - \alpha)| < 1$.
 - (iii) Para quaisquer $r, s \in \mathbb{Q}$ existem $m, n \in \mathbb{Z}$ tais que:

$$\begin{cases} |(r-m)^2 - d \cdot (s-n)^2| < 1 \text{ no caso } d \equiv 2 \text{ ou } 3 \pmod{4}, \\ \left| \left(r - m + \frac{s-n}{2} \right)^2 - d \cdot \left(\frac{s-n}{2} \right)^2 \right| < 1 \text{ no caso } d \equiv 1 \pmod{4}. \end{cases}$$

- b) Mostre que todo $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 13\}$ satisfaz a condição (iii), o que não acontece com nenhum outro $d \in \mathcal{D}$ negativo. (Veja Weiss [37], Proposition 6-4-1).
- 2.7. Seja $\prod p^{k_p}$ a fatoração (em $\mathbb{Z}$) do número natural $g \neq 0$. Prove que existirão $m, n \in \mathbb{Z}$ tais que $g = m^2 + n^2$ se e somente se, para cada $p \equiv 3 \pmod{4}$, o expoente k_p for par.
- 2.8. Seja $L = \mathbb{Q}(\sqrt{d})$ onde $d \in \mathcal{D}$.
- a) Supondo $d < 0$ e
- $$F(X, Y) = \begin{cases} X^2 + |d| \cdot Y^2 & \text{no caso } d \equiv 2 \text{ ou } 3 \pmod{4}, \\ X^2 + X \cdot Y + \frac{1-d}{4} \cdot Y^2 & \text{no caso } d \equiv 1 \pmod{4}, \end{cases}$$
- prove que, para qualquer número primo p , as seguintes condições são equivalentes:
- (i) A equação $F(X, Y) = p$ tem uma solução $(m, n) \in \mathbb{Z} \times \mathbb{Z}$.
 - (ii) Existe $\alpha \in I_L$ tal que $\mathcal{N}_{L/\mathbb{Q}} \alpha = p$.
 - (iii) p é redutível em I_L .
- b) Tente formular e provar uma afirmação semelhante no caso em que $d > 0$.
(Note que é desnecessário supor que I_L seja fatorial.)
- 2.9. Sejam p, m e n como em (2.8). Indique todos os elementos de $\mathbb{Z}[i]$ que dividem p . Quais deles são associados entre si?
- 2.10. Seja n um número natural tal que $n = 4^g \cdot (7 + 8h)$, onde $g, h \in \mathbb{N}$. Prove que n não é soma de três quadrados, isto é, $n \neq k^2 + \ell^2 + m^2$ quaisquer que sejam $k, \ell, m \in \mathbb{Z}$.
(Observação: Pode se provar que todos os outros números naturais n são somas de três quadrados. Veja Hardy-Wright [12], §20.10).
- 2.11. Prove que existe uma infinidade de elementos $\alpha \in \mathbb{Q}(i)$ tais que $|\alpha| = 1$.

§3. Corpos ciclotômicos

Consideraremos neste parágrafo *corpos ciclotômicos*, isto é, subcorpos $\mathbb{Q}(\zeta)$ de $\mathbb{C}$ gerados por uma raiz da unidade, ζ .

Convém estudar preliminarmente as raízes da unidade contidas num corpo K qualquer. Para qualquer elemento não-nulo α de K denotamos

por $o(\alpha)$ a ordem (finita ou infinita) de α no grupo multiplicativo K^* . Ela independe de K no sentido que coincide com a ordem de α em L^* , qualquer que seja o corpo $L \supseteq K$.

Diremos que $\zeta \in K$ é uma raiz n -ésima da unidade em K quando $\zeta^n = 1$, isto é, quando n for um múltiplo de $o(\zeta)$. O conjunto $W_n(K)$ das raízes n -ésimas da unidade em K é um subgrupo de K^* cuja ordem é no máximo igual a n , uma vez que $W_n(K)$ consiste das raízes em K do polinômio $X^n - 1$.

(3.1) *Todo subgrupo finito V de K^* é cíclico e igual a $W_m(K)$, sendo m a ordem de V .*

Demonstração. Por um resultado conhecido da teoria dos grupos abelianos finitos (veja Exercício 5.2 d), V possui um elemento γ de ordem $r = \text{MMC}\{o(\alpha) \mid \alpha \in V\}$. Temos que $V \subseteq W_r(K) \subseteq W_m(K)$, pois r é múltiplo de $o(\alpha)$ para todo $\alpha \in V$ e m é múltiplo de r . Nestas inclusões valem as igualdades, uma vez que $W_m(K)$ tem no máximo m elementos; logo $r = m$, e γ é um gerador de V . $\square$

Para determinar a ordem de $W_n(K)$, convém considerar o conjunto $\mathcal{P}_n(K)$ das raízes primitivas n -ésimas da unidade de K , isto é, dos $\zeta \in K^*$ tais que $o(\zeta) = n$. Denotamos por p (zero ou um número primo) a característica de K . Observemos que o polinômio $X^n - 1 \in K[X]$ será separável se e somente se p não dividir n (pois $(X^n - 1)' = n \cdot X^{n-1}$); isto ocorrerá, em particular, quando $p = 0$.

(3.2) *Para qualquer $n \geq 1$ as seguintes condições são equivalentes:*

- (i) $W_n(K)$ tem ordem n .
- (ii) $\mathcal{P}_n(K) \neq \emptyset$.
- (iii) $p \nmid n$ e $X^n - 1$ fatora-se em $K[X]$ em fatores lineares.

Neste caso, $\mathcal{P}_d(K) \neq \emptyset$ para todo $d \mid n$, e

$$W_n(K) = \bigcup_{d \mid n} \mathcal{P}_d(K) \quad (\text{reunião disjunta}).$$

Demonstração. (i) $\Rightarrow$ (ii) resulta de (3.1).

(ii) $\Rightarrow$ (iii): Seja $\zeta \in \mathcal{P}_n(K)$. Então $p \nmid n$, pois, caso contrário, teríamos $p \neq 0$ e $(\zeta^p)^{\frac{n}{p}} = \zeta^n = 1$, logo $\zeta^{\frac{n}{p}} = 1$, o que é absurdo. O polinômio $X^n - 1$ tem

as n raízes $1, \zeta, \dots, \zeta^{n-1} \in K$, logo fatora-se em $K[X]$ em fatores lineares.

(iii) $\Rightarrow$ (i): Existem $\eta_1, \dots, \eta_n \in K$ tais que $X^n - 1 = (X - \eta_1) \cdot \dots \cdot (X - \eta_n)$. Como $X^n - 1$ é separável, os elementos $\eta_1, \dots, \eta_n$ são distintos e formam $W_n(K)$.

Para todo $d \mid n$ temos que $\zeta^{\frac{n}{d}} \in \mathcal{P}_d(K)$. A última igualdade é trivial. $\square$

Obviamente, qualquer corpo algebricamente fechado cuja característica não divida n e, em particular, o corpo $\mathbb{C}$, satisfaz as condições equivalentes de (3.2). Por outro lado, para qualquer subcorpo K de $\mathbb{R}$ teremos que $W_n(K) = \{1\}$ (respectivamente $= \{1, -1\}$) se n for ímpar (respectivamente par), e $\mathcal{P}_n(K) = \phi$ para qualquer $n > 2$.

Se K tiver característica $p \neq 0$, então $W_n(K) = W_{n, p^r}(K)$ e $\mathcal{P}_{n, p^r}(K) = \phi$ para $r \geq 1$. Notemos ainda que $W_{q-1}(\mathbb{F}_q) = \mathbb{F}_q^*$, sendo $\mathbb{F}_q$ o corpo de $q = p^n$ elementos.

Estes exemplos mostram que o grupo

$$W(K) = \bigcup_{n \geq 1} W_n(K)$$

de todas as raízes da unidade em K , o qual obviamente coincide com o grupo de torção de K^* , pode ser finito ou infinito. Se for finito, digamos de ordem n , então $W(K) = W_n(K)$, e teremos que $\mathcal{P}_d(K) \neq \phi$ se e somente se $d \mid n$; em particular, exceto no caso de característica $p = 2$, a ordem n é par, pois $-1 \in \mathcal{P}_2(K)$.

Mencionamos ainda que, para qualquer subanel R de L , a interseção $W(L) \cap R$ é um subgrupo de $U(R)$ e $W(L)$ é um subgrupo de $U(I_L(R))$. Em particular, $W(L)$ será um subgrupo de $U(R)$ quando R for integralmente fechado em L .

Para qualquer corpo de números algébricos L , $W(L)$ é um subgrupo de $U(I_L)$ e é finito, como foi demonstrado em (1.16); uma outra demonstração é sugerida no Exercício 3.2. Se L for um corpo quadrático, digamos $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$, então $W(L)$ tem ordem 2, exceto nos casos $d = -1$ e $d = -3$, nos quais tem ordem 4 respectivamente 6, sendo gerado por uma raiz primitiva quarta respectivamente sexta da unidade (veja (2.7)).

Seja K um corpo que possui uma raiz primitiva n -ésima da unidade ζ , isto é, que satisfaz as condições equivalentes de (3.2). Para determinar as outras raízes primitivas n -ésimas da unidade, usaremos o fato de $W_n(K)$ ser cíclico de ordem n e, portanto, isomorfo ao grupo aditivo

$(\mathbb{Z}/n\mathbb{Z})^+$ do anel $\mathbb{Z}/n\mathbb{Z}$. Mais precisamente, observamos que a aplicação definida por $k \mapsto \zeta^k$ ($k \in \mathbb{Z}$) induz um isomorfismo de $(\mathbb{Z}/n\mathbb{Z})^+$ sobre $W_n(K)$ e que, sob este isomorfismo, os geradores de $(\mathbb{Z}/n\mathbb{Z})^+$ correspondem biunivocamente aos geradores de $W_n(K)$, ou seja, aos elementos de $\mathcal{P}_n(K)$. Sabe-se que os geradores de $(\mathbb{Z}/n\mathbb{Z})^+$ são exatamente as *classes primas* mod n , isto é, as classes $k + n\mathbb{Z}$ tais que $\text{MDC}(k, n) = 1$, e que estas formam o grupo multiplicativo $U(\mathbb{Z}/n\mathbb{Z})$ dos elementos invertíveis do anel $\mathbb{Z}/n\mathbb{Z}$. A ordem do grupo $U(\mathbb{Z}/n\mathbb{Z})$ é denotada por $\varphi(n)$, sendo φ chamada a *função de Euler*. Resumindo:

(3.3) *Seja $\zeta \in \mathcal{P}_n(K)$. O isomorfismo $\zeta : (\mathbb{Z}/n\mathbb{Z})^+ \rightarrow W_n(K)$, bem-definido por $k + n\mathbb{Z} \mapsto \zeta^k$ ($k \in \mathbb{Z}$), induz uma bijeção de $U(\mathbb{Z}/n\mathbb{Z})$ sobre $\mathcal{P}_n(K)$. Portanto, $\# \mathcal{P}_n(K) = \varphi(n)$.*

A função de Euler satisfaz a seguinte igualdade:

$$\varphi(p_1^{k_1} \cdot \dots \cdot p_r^{k_r}) = p_1^{k_1-1} \cdot \dots \cdot p_r^{k_r-1} \cdot (p_1 - 1) \cdot \dots \cdot (p_r - 1),$$

para quaisquer números primos distintos $p_1, \dots, p_r$ e quaisquer $k_1, \dots, k_r \geq 1$. Esta igualdade é uma consequência imediata dos seguintes fatos:

- a) O grupo $U(\mathbb{Z}/p^r\mathbb{Z})$ tem ordem $p^{r-1} \cdot (p - 1)$ (sendo p primo e $r \geq 1$).
- b) Se $\text{MDC}(m, n) = 1$ então $U(\mathbb{Z}/mn\mathbb{Z})$ será isomorfo ao produto cartesiano de $U(\mathbb{Z}/m\mathbb{Z})$ por $U(\mathbb{Z}/n\mathbb{Z})$. (Veja Exercício 6.4.)

Obviamente, $U(\mathbb{Z}/n\mathbb{Z})$ é abeliano mas nem sempre cíclico. Prova-se que será cíclico se e somente se n for igual a 4, ou igual a p^r ou $p^r \cdot 2$, para algum primo p ímpar e $r \geq 0$ (veja Ribenboim [28], Chapter 3).

Mostraremos ainda que os elementos de $U(\mathbb{Z}/n\mathbb{Z})$ agem como automorfismos do grupo $W_n(K)$. De fato, denotando por $k_{(n)}$ o endomorfismo de $W_n(K)$ definido por $\eta \mapsto \eta^k$ ($\eta \in W_n(K)$), afirmamos:

(3.4) *A aplicação definida por $k \mapsto k_{(n)}$ ($k \in \mathbb{Z}$) induz um isomorfismo de $U(\mathbb{Z}/n\mathbb{Z})$ sobre o grupo dos automorfismos de $W_n(K)$.*

Demonstração. Sendo $W_n(K)$ cíclico de ordem n , todo endomorfismo de $W_n(K)$ é da forma $k_{(n)}$ para algum $k \in \mathbb{Z}$; e teremos que $k_{(n)} = k'_{(n)}$ se e somente se $k \equiv k' \pmod{n}$. Além disto, $k_{(n)}$ será um automorfismo de $W_n(K)$ se e somente se $\text{MDC}(k, n) = 1$, se e somente se $k + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$. Por isto, a aplicação acima indicada induz uma bijeção de $U(\mathbb{Z}/n\mathbb{Z})$ sobre o conjunto dos automorfismos de $W_n(K)$, a qual é obviamente um isomorfismo. $\square$

A seguir, partindo de um corpo K qualquer, estudaremos a extensão L de K obtida pela adjunção de uma raiz primitiva n -ésima da unidade, ζ , pertencente a um corpo algebricamente fechado $\Omega \supseteq K$. Recordamos que tal ζ existirá, isto é, $\mathcal{P}_n(\Omega) \neq 0$, se e somente se n não for divisível pela característica p de K (o que é trivial quando $p = 0$).

(3.5) TEOREMA. *Seja $L = K(\zeta)$, sendo $\zeta \in \Omega$ uma raiz primitiva n -ésima da unidade. Então L é uma extensão galoisiana de K cujo grupo de Galois $\text{Aut}(L|K)$ é canonicamente isomorfo a um subgrupo de $U(\mathbb{Z}/n\mathbb{Z})$.*

Em particular, $\text{Aut}(L|K)$ é um grupo abeliano e sua ordem divide $\varphi(n)$

Demonstração. L é o corpo das raízes do polinômio separável $X^n - 1$ logo é uma extensão galoisiana de K . Associando a todo $\sigma \in \text{Aut}(L|K)$ a sua restrição ao grupo $W_n(L)$, obtemos um homomorfismo injetivo de $\text{Aut}(L|K)$ no grupo dos automorfismos de $W_n(L)$ que por sua vez, é canonicamente isomorfo ao grupo $U(\mathbb{Z}/n\mathbb{Z})$, por (3.4). O resto é óbvio. $\square$

Observemos que o grau $[L:K]$, igual à ordem de $\text{Aut}(L|K)$, pode ser um divisor próprio de $\varphi(n)$, e isto acontece até no caso em que K é um corpo primo $\mathbb{F}_p$ (por exemplo, quando $p > 3$ e $n = p - 1$). Por outro lado, no caso $K = \mathbb{Q}$ vale o seguinte

(3.6) TEOREMA. *Seja $\zeta \in \mathbb{C}$ uma raiz primitiva n -ésima da unidade. Então $L = \mathbb{Q}(\zeta)$ é uma extensão galoisiana de $\mathbb{Q}$, cujo grupo de Galois é canonicamente isomorfo a $U(\mathbb{Z}/n\mathbb{Z})$ e, portanto, é abeliano de ordem $\varphi(n)$.*

Além disto, o polinômio minimal $P_{\zeta|\mathbb{Q}}$ é igual ao polinômio

$$\Phi_n = \prod_{\eta \in \mathcal{P}_n(\mathbb{C})} (X - \eta).$$

Demonstração. Provaremos primeiro que, para todo número primo p que não dividir n , os polinômios minimais $P = P_{\zeta|\mathbb{Q}}$ e $P_1 = P_{\zeta^p|\mathbb{Q}}$ coincidem. Suponhamos que $P \neq P_1$; então existe $G \in \mathbb{Q}[X]$ tal que $X^n - 1 = P \cdot P_1 \cdot G$. Como ζ é raiz de $P_1(X^p)$, existe $H \in \mathbb{Q}[X]$ tal que $P_1(X^p) = P \cdot H$. Como P e P_1 são polinômios mônicos em $\mathbb{Z}[X]$ devido a (1.11a), concluímos de (1.9a) que o mesmo vale para os polinômios G e H . Aplicando o homomorfismo canônico $\kappa: \mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$, obtemos que $\kappa P \cdot \kappa H = \kappa(P_1(X^p)) = (\kappa P_1)^p$; logo κP e κP_1 possuem um divisor comum

$\bar{D} \in \mathbb{F}_p[X] \setminus \mathbb{F}_p$. Resulta que $\bar{D}^2$ divide $\kappa(X^n - 1)$, o que é absurdo devido à separabilidade de $X^n - \kappa 1 \in \mathbb{F}_p[X]$; portanto temos que $P = P_1$.

Aplicando este raciocínio sucessivamente às potências $\zeta^p, \zeta^{p \cdot p'}, \zeta^{p \cdot p' \cdot p''}, \dots$ onde $p, p', p'', \dots$ são números primos que não dividem n , concluímos que todas essas potências, e portanto todos os elementos $\eta \in \mathcal{P}_n(\mathbb{C})$, têm o mesmo polinômio minimal $P_{\eta|\mathbb{Q}} = P$; portanto Φ_n divide P . Vale mesmo $\Phi_n = P$, pois $\partial \Phi_n = \varphi(n) \geq [L:K] = \partial P$ devido a (3.5); portanto $\varphi(n) = [L:K]$. De (3.5) resulta então que $\text{Aut}(L|K)$ é canonicamente isomorfo ao próprio grupo $U(\mathbb{Z}/n\mathbb{Z})$. $\square$

O corpo $\mathbb{Q}(\zeta)$ chama-se o n -ésimo *corpo ciclotômico*. O n -ésimo *polinômio ciclotômico*, Φ_n , que, devido a (3.6), é um polinômio mônico em $\mathbb{Z}[X]$, de grau $\varphi(n)$, e irredutível em $\mathbb{Q}[X]$, pode ser facilmente calculado a partir da seguinte igualdade:

$$(3.7) \quad X^n - 1 = \prod_{d|n} \Phi_d,$$

a qual resulta imediatamente da igualdade indicada em (3.2). Por exemplo, para qualquer número primo p temos que $X^p - 1 = \Phi_1 \cdot \Phi_p$; logo $\Phi_p = (X - 1)^{-1} \cdot (X^p - 1) = X^{p-1} + X^{p-2} + \dots + X + 1$. Mais geralmente, para as potências p^r de um número primo p temos que

$$X^{p^r} - 1 = \Phi_1 \cdot \Phi_p \cdot \dots \cdot \Phi_{p^{r-1}} \cdot \Phi_{p^r} = (X^{p^{r-1}} - 1) \cdot \Phi_{p^r},$$

logo $\Phi_{p^r} = X^{p^{r-1} \cdot (p-1)} + X^{p^{r-1} \cdot (p-2)} + \dots + X^{p^{r-1}} + 1$. O polinômio Φ_6 obtém-se da igualdade

$$X^6 - 1 = \Phi_1 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_6 = (X^3 - 1) \cdot (X + 1) \cdot \Phi_6;$$

logo $\Phi_6 = X^2 - X + 1$. Pode-se provar que para $n < 105$, todos os coeficientes de Φ_n estão em $\{0, 1, -1\}$, mas que ocorrem coeficientes arbitrariamente grandes para números $n \geq 105$, como foi provado por Schur (veja Lehmer [23]).

Recordamos que, para qualquer corpo de números algébricos L , o grupo $W(L)$ é finito. Determinemo-lo explicitamente no caso do n -ésimo corpo ciclotômico.

(3.8) **COROLÁRIO.** *Sejam $\zeta \in L = \mathbb{Q}(\zeta)$ como no teorema (3.6). Então $W(L)$ tem ordem n (respectivamente $2n$) no caso em que n é par (respectivamente ímpar).*

Demonstração. Sejam n' a ordem e η um gerador de $W(L)$. Como $\zeta \in W(L)$, temos que $n \mid n'$. Seja $n = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$ a fatoração de n ; então existem $k'_1 \geq k_1, \dots, k'_r \geq k_r$ e $m \in \mathbb{N}$ tais que $n' = p_1^{k'_1} \cdot \dots \cdot p_r^{k'_r} \cdot m$ e $\text{MDC}(m, p_j) = 1$ ($j = 1, \dots, r$). Por outro lado, o grau

$$[\mathbb{Q}(\eta) : \mathbb{Q}] = \varphi(n') = p_1^{k'_1-1} \cdot \dots \cdot p_r^{k'_r-1} \cdot (p_1 - 1) \cdot \dots \cdot (p_r - 1) \cdot \varphi(m)$$

é um divisor do grau

$$[L : \mathbb{Q}] = \varphi(n) = p_1^{k_1-1} \cdot \dots \cdot p_r^{k_r-1} \cdot (p_1 - 1) \cdot \dots \cdot (p_r - 1);$$

logo $k'_1 = k_1, \dots, k'_r = k_r$ e $\varphi(m) = 1$. Resulta que $n' = n \cdot m$ e que $m \in \{1, 2\}$. Sendo n' par e $\text{MDC}(m, n) = 1$, teremos que $m = 2$ se e somente se n for ímpar. $\square$

A seguir estudaremos o anel I_L dos inteiros do corpo ciclotômico L , restringindo-nos entretanto ao caso em que n é um número primo p ímpar.

Seja $L = \mathbb{Q}(\zeta)$, sendo ζ uma raiz primitiva p -ésima da unidade. Então $[L : \mathbb{Q}] = p - 1$; $1, \zeta, \dots, \zeta^{p-2}$ formam uma base de L sobre $\mathbb{Q}$ e $\zeta, \zeta^2, \dots, \zeta^{p-1}$ são as raízes do polinômio ciclotômico $\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1$. O grupo de Galois $\text{Aut}(L | \mathbb{Q})$ consiste dos $p - 1$ automorfismos $\sigma_1, \dots, \sigma_{p-1}$, sendo σ_j univocamente determinado por $\sigma_j \zeta = \zeta^j$ ($j = 1, \dots, p - 1$); em particular, σ_1 é a identidade de L .

No anel I_L , os elementos $\zeta - 1, \zeta^2 - 1, \dots, \zeta^{p-1} - 1$ representam um papel importante. Calculemos o seu polinômio minimal sobre $\mathbb{Q}$:

(3.9) $\zeta - 1, \dots, \zeta^{p-1} - 1$ são raízes do polinômio

$$\psi_p = X^{p-1} + \binom{p}{p-1} \cdot X^{p-2} + \dots + \binom{p}{j} \cdot X^{j-1} + \dots + \binom{p}{1} \in \mathbb{Z}[X],$$

que é irredutível em $\mathbb{Q}[X]$.

Demonstração. Para todo $j \in \{1, \dots, p - 1\}$, o elemento $\zeta^j - 1$ é obviamente raiz do polinômio

$$\Phi_p(X + 1) = \frac{(X + 1)^p - 1}{(X + 1) - 1} = \frac{1}{X} \cdot \sum_{k=1}^p \binom{p}{k} \cdot X^k = \psi_p,$$

o qual é irredutível pelo critério de Eisenstein. $\square$

É óbvio que a irredutibilidade de ψ_p segue também da irredutibilidade de Φ_p , demonstrada em (3.6). Por outro lado, a irredutibilidade de

Φ_p pode ser concluída da de ψ_p , o que fornece uma alternativa para a demonstração dada em (3.6), no caso em que $n = p$.

Como cada um dos elementos ζ^j e $\zeta^j - 1$ é um elemento primitivo da extensão L de $\mathbb{Q}$, o seu polinômio minimal sobre $\mathbb{Q}$ coincide com o polinômio característico em relação a $L | \mathbb{Q}$. Portanto, escrevendo $\mathcal{F}$ e $\mathcal{N}$ em lugar de $\mathcal{F}_{L|\mathbb{Q}}$ e $\mathcal{N}_{L|\mathbb{Q}}$, temos, para $j = 1, \dots, p-1$, que:

$$(3.10) \quad \begin{aligned} \mathcal{F}\zeta^j &= -1, & \mathcal{F}(\zeta^j - 1) &= -p, & \mathcal{F}(1 - \zeta^j) &= p; \\ \mathcal{N}\zeta^j &= 1, & \mathcal{N}(\zeta^j - 1) &= p, & \mathcal{N}(1 - \zeta^j) &= p. \end{aligned}$$

É óbvio que as potências de ζ são invertíveis em I_L . Por outro lado mostraremos que:

$$(3.11) \quad \begin{aligned} \text{a)} & \quad 1 - \zeta, \dots, 1 - \zeta^{p-1} \text{ são irredutíveis em } I_L, \text{ associados dois a dois.} \\ \text{b)} & \quad (1 - \zeta) \cdot I_L \cap \mathbb{Z} = p \cdot \mathbb{Z}. \\ \text{c)} & \quad p \text{ é associado a } (1 - \zeta)^{p-1} \text{ em } I_L. \end{aligned}$$

Demonstração. a) Para $j = 1, \dots, p-1$ temos que $1 - \zeta^j \in I_L$ e $\mathcal{N}(1 - \zeta^j) = p$; logo $1 - \zeta^j$ é irredutível em I_L , por (1.11d). Além disto, $1 - \zeta^j$ é associado a $1 - \zeta$, uma vez que

$$1 - \zeta^j = (1 - \zeta) \cdot (\zeta^{j-1} + \zeta^{j-2} + \dots + \zeta + 1).$$

b) De (1.11b) concluímos que $p = \mathcal{N}(1 - \zeta) \in (1 - \zeta) \cdot I_L \cap \mathbb{Z}$. Como $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$ e $1 \notin (1 - \zeta) \cdot I_L$, por a), resulta que $p\mathbb{Z} = (1 - \zeta) \cdot I_L \cap \mathbb{Z}$.

c) $p = \mathcal{N}(1 - \zeta) = \prod_{j=1}^{p-1} \sigma_j(1 - \zeta) = \prod_{j=1}^{p-1} (1 - \zeta^j)$ é associado a $(1 - \zeta)^{p-1}$, por a). $\square$

Podemos agora demonstrar que o $\mathbb{Z}$ -módulo I_L é livre. Mais precisamente:

$$(3.12) \quad \text{TEOREMA. } 1, \zeta, \dots, \zeta^{p-2} \text{ formam uma base do } \mathbb{Z}\text{-módulo } I_L.$$

Demonstração: $1, \zeta, \dots, \zeta^{p-2}$ são linearmente independentes sobre $\mathbb{Z}$, pois o são sobre $\mathbb{Q}$. Obviamente $\mathbb{Z} + \mathbb{Z} \cdot \zeta + \dots + \mathbb{Z} \cdot \zeta^{p-2} \subseteq I_L$; portanto basta provar a inclusão inversa. Seja $\alpha \in I_L$, digamos $\alpha = a_0 + a_1 \cdot \zeta + \dots + a_{p-2} \cdot \zeta^{p-2}$, sendo $a_0, \dots, a_{p-2} \in \mathbb{Q}$. Mostraremos primei-

ro que $a_0 \in \mathbb{Z}$. Aplicando o traço ao produto $\alpha \cdot (1 - \zeta) = \sum_{j=0}^{p-2} a_j \cdot (\zeta^j - \zeta^{j+1})$ e observando que $\mathcal{T}(\zeta^j - \zeta^{j+1}) = \mathcal{T}\zeta^j - \mathcal{T}\zeta^{j+1} = 0$ para $j = 1, \dots, p-2$, obtemos que $\mathcal{T}(\alpha \cdot (1 - \zeta)) = a_0 \cdot \mathcal{T}(1 - \zeta) = a_0 \cdot p$. Por outro lado, temos que $\mathcal{T}(\alpha \cdot (1 - \zeta)) = \sum_{j=1}^{p-1} \sigma_j(\alpha \cdot (1 - \zeta)) = \sum_{j=1}^{p-1} \sigma_j \alpha \cdot (1 - \zeta^j) \in (1 - \zeta) \cdot I_L \cap \mathbb{Z} = p\mathbb{Z}$ por (1.11a) e (3.11); portanto $a_0 \in \mathbb{Z}$.

Supondo, por indução, que $a_0, \dots, a_{j-1} \in \mathbb{Z}$ para algum $j \in \{1, \dots, p-2\}$, mostraremos que $a_j \in \mathbb{Z}$. De fato, multiplicando α por ζ^{p-j} , obtemos que $\alpha \cdot \zeta^{p-j} = a_j + a_{j+1} \cdot \zeta + \dots + a_{p-2} \cdot \zeta^{p-j-2} + a_0 \cdot \zeta^{p-j} + \dots + a_{j-1} \cdot \zeta^{p-1}$. Substituindo ζ^{p-1} por $-1 - \zeta - \dots - \zeta^{p-2}$ concluímos que $\alpha \cdot \zeta^{p-j} = (a_j - a_{j-1}) + b_1 \cdot \zeta + \dots + b_{p-2} \cdot \zeta^{p-2}$, com $b_1, \dots, b_{p-2} \in \mathbb{Q}$ apropriados. Como $\alpha \cdot \zeta^{p-j} \in I_L$, resulta da primeira parte da demonstração que $a_j - a_{j-1} \in \mathbb{Z}$; portanto $a_j = (a_j - a_{j-1}) + a_{j-1} \in \mathbb{Z}$. Concluímos que $a_0, \dots, a_{p-2} \in \mathbb{Z}$, logo $\alpha \in \mathbb{Z} + \mathbb{Z} \cdot \zeta + \dots + \mathbb{Z} \cdot \zeta^{p-2}$. $\square$

Mencionamos, sem demonstração, que este teorema se generaliza ao n -ésimo corpo ciclotômico, para qualquer $n > 1$; de fato, este tem $1, \zeta, \dots, \zeta^{\varphi(n)-1}$ como base integral, sendo ζ uma raiz primitiva n -ésima da unidade (veja Ribenboim [28], Chapter 13 (4), ou Weiss [37], 7-5-4).

Terminaremos este parágrafo mostrando, para o p -ésimo corpo ciclotômico $L = \mathbb{Q}(\zeta)$, um resultado de Kummer sobre o grupo $U(I_L)$, que teve um papel importante na tentativa de provar o Último Teorema de Fermat (veja Borevich-Shafarevich [6], Chapter III, §1). Ele afirma que todo elemento invertível de I_L é produto de uma raiz p -ésima da unidade por um elemento invertível *real*; em outras palavras:

(3.13) TEOREMA. $U(I_L)$ é produto direto dos subgrupos $W_p(L)$ e $U(I_L) \cap \mathbb{R}$.

Demonstração. Para qualquer $\omega \in \mathbb{C}$ denotamos por ω^* o complexo-conjugado de ω . Lembramos que $\omega \cdot \omega^* = |\omega|^2 = |\omega^*|^2$, e que $\omega = \omega^*$ se e somente se $\omega \in \mathbb{R}$. Notamos que a restrição, ao subcorpo L do automorfismo $*$ de $\mathbb{C}$ coincide com σ_{p-1} , pois $\zeta \cdot \zeta^* = |\zeta|^2 = 1 = \zeta \cdot \sigma_{p-1}\zeta$. Seja $\alpha \in U(I_L)$; então $\alpha^* = \sigma_{p-1}\alpha \in U(I_L)$ e, para todo $j = 1, \dots, p-1$, temos que $\sigma_j \alpha^* = \sigma_j(\sigma_{p-1}\alpha) = \sigma_{p-1}(\sigma_j \alpha) = (\sigma_j \alpha)^*$, pois $\text{Aut}(L | \mathbb{Q})$ é abeliano; portanto $\sigma_j \left(\frac{\alpha}{\alpha^*} \right) = ((\sigma_j \alpha)^*)^{-1} \cdot \sigma_j \alpha$ tem valor absoluto igual a 1. De (1.16

concluimos que $\frac{\alpha}{\alpha^*} \in W(L)$, e de (3.8) resulta que $\frac{\alpha}{\alpha^*} = (-1)^e \cdot \zeta^k$, com $e \in \{0, 1\}$ e $k \in \mathbb{N}$.

Para mostrar que $e = 0$, consideramos o homomorfismo canônico θ do anel I_L sobre o anel quociente $\tilde{I} = I_L/(1 - \zeta) \cdot I_L$. Obviamente $\theta\zeta = \theta 1 = \tilde{1}$ (unidade de $\tilde{I}$), logo $\theta\zeta^* = \theta\zeta^{p-1} = \tilde{1}$ e assim $\theta\beta = \sum_{i=0}^{p-2} \theta b_i = \theta\beta^*$ para qualquer $\beta = \sum_{i=0}^{p-2} b_i \cdot \zeta^i$ (com $b_0, \dots, b_{p-2} \in \mathbb{Z}$); em particular, $\theta\alpha = \theta\alpha^*$. Suponhamos que $e = 1$; então $\alpha = -\zeta^k \cdot \alpha^*$, logo $\theta\alpha = -\theta\alpha^*$, logo $\theta(2\alpha) = 2 \cdot \theta\alpha = 0$, ou seja, $2\alpha \in (1 - \zeta) \cdot I_L$. Como $\alpha \in U(I_L)$, temos que $2 \in (1 - \zeta) \cdot I_L \cap \mathbb{Z} = p\mathbb{Z}$ por (3.11b), o que é absurdo; portanto $\alpha = \zeta^k \cdot \alpha^*$. Existe $m \in \mathbb{N}$ tal que $k \equiv 2m \pmod{p}$, logo $\frac{\alpha}{\zeta^m} = \zeta^m \cdot \alpha^* = \left(\frac{\alpha}{\zeta^m}\right)^* \in \mathbb{R}$. Concluímos que $\alpha = \zeta^m \cdot \frac{\alpha}{\zeta^m} \in W_p(L) \cdot (U(I_L) \cap \mathbb{R})$. Como $W_p(L) \cap \mathbb{R} = \{1\}$, este produto é direto. $\square$

Observemos que de (3.13) resulta também a igualdade

$$U(I_L) = W_{2p} \odot (U(I_L) \cap \mathbb{R}_{>0}),$$

onde $\mathbb{R}_{>0}$ é o grupo multiplicativo dos números reais positivos. Veremos no §18 que $U(I_L) \cap \mathbb{R}_{>0}$ é um grupo abeliano livre de posto $\frac{p-3}{2}$.

EXERCÍCIOS

- 3.1. Prove que não existe nenhum corpo infinito cujo grupo multiplicativo seja cíclico.
- 3.2. Seja $m \in \mathbb{N} \setminus \{0\}$ e sejam $p_1, \dots, p_s$ os números primos menores que $m+2$. Prove:
 - a) Se $k \in \mathbb{N} \setminus \{0\}$ tal que $\varphi(k) \nmid m$, então $k \nmid m \cdot p_1 \cdot \dots \cdot p_s$.
 - b) Para qualquer extensão L de $\mathbb{Q}$ de grau m , $W(L)$ é um grupo finito e sua ordem divide $m \cdot p_1 \cdot \dots \cdot p_s$.
- 3.3. Sejam $\zeta, \eta \in \mathbb{C}$ raízes primitivas n - respectivamente m -ésimas da unidade.
 - a) Prove que se $\text{MDC}(m, n) = 1$ então $\zeta \cdot \eta$ é uma raiz primitiva nm -ésima da unidade.

- b) Conclua que se n for ímpar, então $-\zeta$ será uma raiz primitiva $2n$ -ésima da unidade e $\Phi_{2n} = \Phi_n(-X)$.

3.4. Prove que:

- a) Qualquer polinômio mônico $F \in \mathbb{Z}[X]$, tal que todas as raízes de F em $\mathbb{C}$ tenham valor absoluto igual a 1, é um produto de polinômios ciclotômicos.
- b) Para cada $m \geq 1$ existe, no máximo, um polinômio de grau m deste tipo que é irredutível em $\mathbb{Q}[X]$. Determine os números m para os quais tal polinômio realmente existe.

3.5. Seja L o 12-ésimo corpo ciclotômico.

- a) Determine $\text{Aut}(L|\mathbb{Q})$ indicando explicitamente seus elementos.
- b) Determine todos os subgrupos de $\text{Aut}(L|\mathbb{Q})$ e todos os subcorpos de L .
- c) Calcule o polinômio ciclotômico Φ_{12} .

3.6. Seja Ω um corpo algebricamente fechado e seja $n > 1$ não divisível pela característica p (zero ou prima) de Ω . Sendo $\Phi_{n,\Omega} = \prod_{\eta \in \mathcal{P}_n(\Omega)} (X - \eta)$, prove que:

- a) $\Phi_{n,\Omega}$ é a imagem de Φ_n pelo homomorfismo canônico $\mathbb{Z}[X] \rightarrow \Omega[X]$ e, portanto, seus coeficientes estão no corpo primo de Ω . Dê uma demonstração que não utilize a irredutibilidade de Φ_n .
- b) No caso $p \neq 0$, $\Phi_{n,\Omega}$ é um produto de $\frac{\varphi(n)}{f}$ polinômios irredutíveis em $\mathbb{F}_p[X]$, de grau f , sendo f a ordem da classe $p + n\mathbb{Z}$ no grupo $U(\mathbb{Z}/n\mathbb{Z})$.

3.7. Seja $L = \mathbb{Q}(\zeta)$, sendo ζ uma raiz primitiva m -ésima da unidade, onde $m > 2$, e seja $K = \mathbb{Q}(\zeta + \zeta^{-1})$. Prove que:

- a) $P_{\zeta|K} = X^2 - (\zeta + \zeta^{-1}) \cdot X + 1$.
- b) Seja σ o automorfismo de L determinado por $\sigma\zeta = \zeta^{-1}$; então K é o corpo fixo do subgrupo de $\text{Aut}(L|\mathbb{Q})$ gerado por σ .
- c) K é o maior subcorpo de L que está contido em $\mathbb{R}$.
- d) $[L:K] = 2$ e $[K:\mathbb{Q}] = \frac{\varphi(m)}{2}$.
- e) Determine os m tais que K seja o único subcorpo de L com $[L:K] = 2$.

3.8. Seja $L = \mathbb{Q}(\zeta)$, sendo $\zeta \in \mathbb{C}$ uma raiz p -ésima da unidade, onde p é um número primo $\neq 2$.

a) Visualize no plano complexo a posição dos elementos invertíveis de I_L , usando o Teorema (3.13).

b) Prove que $1 + \zeta \in U(I_L)$ e indique um $k \in \mathbb{N}$ tal que $(1 + \zeta) \cdot \zeta^{-k} \in \mathbb{R}$.

c) Prove que, para qualquer $\alpha \in U(I_L)$, temos que $|\alpha| \in U(I_L)$ e

$$\frac{\alpha}{|\alpha|} \in W(L).$$

d) Prove que os elementos invertíveis $\left| \frac{1 - \zeta^j}{1 - \zeta} \right| = \sqrt{\frac{1 - \zeta^j}{1 - \zeta} \cdot \frac{1 - \zeta^{-j}}{1 - \zeta^{-1}}}$ ($j = 1, \dots, \frac{p-1}{2}$) são distintos dois a dois.

§4. Discriminante

Mais importante que o discriminante $\text{disc}(F)$ de um polinômio $F \in K[X]$, definido no §0, é o discriminante $\text{disc}_{L|K}(\alpha_1, \dots, \alpha_n)$ de uma n -upla de elementos $\alpha_1, \dots, \alpha_n$ pertencentes a uma extensão L de K , de grau n , que introduziremos a seguir. Usá-lo-emos para provar, no caso de um corpo de número algébricos L , que I_L está contido num $\mathbb{Z}$ -módulo livre, o que permitirá demonstrar, no §5, que o próprio I_L é um $\mathbb{Z}$ -módulo livre, ou seja, que L possui uma base integral. Além disso, o discriminante de uma base integral de L , que será chamado o discriminante do corpo L e denotado por d_L , representará um papel importante no §13, onde será mostrado que seus fatores irredutíveis são exatamente os números primos que se ramificam em L .

Seja L uma extensão finita de K de grau n . Para quaisquer $\alpha_1, \dots, \alpha_n \in L$ definimos o discriminante da n -upla $\alpha_1, \dots, \alpha_n$ como

$$\text{disc}_{L|K}(\alpha_1, \dots, \alpha_n) = \det(\mathcal{T}_{L|K}(\alpha_i \cdot \alpha_j)) \in K.$$

Sem perda de generalidade podemos supor que a extensão L de K seja separável, pois, caso contrário, o discriminante sempre seria igual a zero, uma vez que $\mathcal{T}_{L|K}\alpha = 0$ para todo $\alpha \in L$.

Discriminantes de diferentes n -uplas estão relacionados da seguinte maneira.

(4.1) Para $i = 1, \dots, n$ seja $\gamma_i = \sum_{j=1}^n c_{ij} \cdot \alpha_j$, onde $c_{ij} \in K$. Então

$$\text{disc}_{L|K}(\gamma_1, \dots, \gamma_n) = (\det(c_{ij}))^2 \cdot \text{disc}_{L|K}(\alpha_1, \dots, \alpha_n).$$

Demonstração. Basta aplicar $\mathcal{T}_{L|K}$ à igualdade $\gamma_k \cdot \gamma_m = \sum_{i,j=1}^n c_{ki} \cdot c_{mj} \cdot \alpha_i \cdot \alpha_j$ e considerar os determinantes das matrizes assim obtidas. $\square$

Sejam $\sigma_1, \dots, \sigma_n$ os n K -isomorfismos de L em Ω (corpo algebricamente fechado que contém L); então, para quaisquer $\alpha_1, \dots, \alpha_n \in L$ temos que

$$(4.2) \quad \text{disc}_{L|K}(\alpha_1, \dots, \alpha_n) = (\det(\sigma_i \alpha_j))^2.$$

Demonstração. Resulta de $\mathcal{T}_{L|K}(\alpha_i \cdot \alpha_j) = \sum_{k=1}^n \sigma_k \alpha_i \cdot \sigma_k \alpha_j$ ($i, j = 1, \dots, n$). $\square$

Mostraremos que o discriminante da n -upla $1, \alpha, \dots, \alpha^{n-1}$ coincide com o discriminante do polinômio característico de α ; de fato:

(4.3) Para qualquer $\alpha \in L$ temos que

$$\begin{aligned} \text{disc}_{L|K}(1, \alpha, \dots, \alpha^{n-1}) &= \prod_{i=1}^n \prod_{j=i+1}^n (\sigma_j \alpha - \sigma_i \alpha)^2 = \text{disc}(F) = \\ &= (-1)^{\binom{n}{2}} \mathcal{N}_{L|K}(F'(\alpha)), \text{ sendo } F = F_{\alpha, L|K}. \end{aligned}$$

Demonstração. Substituindo X_i por $\sigma_i \alpha$ no determinante de Vandermonde

$$\det(X_i^{j-1}) = \prod_{i=1}^n \prod_{j=i+1}^n (X_j - X_i) \text{ (veja Zariski-Samuel [38],$$

p. 94) e usando (4.2), obtemos a primeira igualdade. Resulta que

$\text{disc}_{L|K}(1, \alpha, \dots, \alpha^{n-1}) = \text{disc}(F)$, uma vez que $F = \prod_{j=1}^n (X - \sigma_j \alpha)$. Como

$$F' = \sum_{i=1}^n (X - \sigma_1 \alpha) \cdot \dots \cdot (X - \sigma_{i-1} \alpha) \cdot (X - \sigma_{i+1} \alpha) \cdot \dots \cdot (X - \sigma_n \alpha),$$

temos que

$$F'(\sigma_i \alpha) = (\sigma_i \alpha - \sigma_1 \alpha) \cdot \dots \cdot (\sigma_i \alpha - \sigma_{i-1} \alpha) \cdot (\sigma_i \alpha - \sigma_{i+1} \alpha) \cdot \dots \cdot (\sigma_i \alpha - \sigma_n \alpha),$$

logo

$$\begin{aligned} \mathcal{N}_{L|K} F'(\alpha) &= \prod_{i=1}^n F'(\sigma_i \alpha) = \prod_{i=1}^n \prod_{j=1}^{i-1} (\sigma_i \alpha - \sigma_j \alpha) \cdot \prod_{i=1}^n \prod_{j=i+1}^n (\sigma_i \alpha - \sigma_j \alpha) = \\ &= (-1)^{\binom{n}{2}} \prod_{i=1}^n \prod_{j=i+1}^n (\sigma_i \alpha - \sigma_j \alpha)^2. \quad \square \end{aligned}$$

Usamos (4.3) para caracterizar as bases da extensão L de K por meio do discriminante:

(4.4) *Sejam $\beta_1, \dots, \beta_n \in L$. Teremos que $\text{disc}_{L|K}(\beta_1, \dots, \beta_n) \neq 0$ se e somente se $\beta_1, \dots, \beta_n$ formarem uma base da extensão L de K .*

Demonstração. Seja α um elemento primitivo da extensão L de K . Então $\sigma_1 \alpha, \dots, \sigma_n \alpha$ são elementos distintos, logo $\text{disc}_{L|K}(1, \alpha, \dots, \alpha^{n-1}) \neq 0$, por (4.3). Como $1, \alpha, \dots, \alpha^{n-1}$ formam uma base, existem $b_{ij} \in \mathbb{Q}$ tais que $\beta_i = \sum_{j=1}^n b_{ij} \cdot \alpha^{j-1}$ ($i=1, \dots, n$). Obviamente $\beta_1, \dots, \beta_n$ formarão uma base se e somente se $\det(b_{ij}) \neq 0$, o que ocorrerá se e somente se $\text{disc}_{L|K}(\beta_1, \dots, \beta_n) \neq 0$, devido a (4.1). $\square$

Usando (4.4), mostraremos que toda base da extensão L de K possui uma base dual. Isto será uma consequência da seguinte afirmação:

(4.5) *Suponhamos que $\beta_1, \dots, \beta_n$ formem uma base da extensão L de K . Para quaisquer $c_1, \dots, c_n \in K$ existe um e um só $\alpha \in L$ tal que $\mathcal{T}_{L|K}(\beta_i \cdot \alpha) = c_i$ ($i=1, \dots, n$).*

Demonstração. O sistema de equações lineares $\sum_{j=1}^n \mathcal{T}_{L|K}(\beta_i \cdot \beta_j) \cdot X_j = c_i$ ($i=1, \dots, n$) possui uma e uma só solução $a_1, \dots, a_n \in K$, uma vez que $\det(\mathcal{T}_{L|K}(\beta_i \cdot \beta_j)) = \text{disc}_{L|K}(\beta_1, \dots, \beta_n) \neq 0$, por (4.4). Obviamente, $\alpha = a_1 \cdot \beta_1 + \dots + a_n \cdot \beta_n$ é o único elemento de L que tem a propriedade desejada. $\square$

(4.6) *Para qualquer base $\beta_1, \dots, \beta_n$ da extensão L de K existe uma e uma só base $\beta'_1, \dots, \beta'_n$ desta extensão tal que*

$$\mathcal{T}_{L|K}(\beta_i \cdot \beta'_j) = \delta_{ij} \quad (i, j = 1, \dots, n).$$

Para todo $\alpha \in L$ temos que $\alpha = \sum_{j=1}^n \mathcal{T}_{L|K}(\beta_j \cdot \alpha) \cdot \beta'_j$.

Demonstração. De (4.5) resultam a existência e unicidade de elementos $\beta'_1, \dots, \beta'_n \in L$ que satisfazem as igualdades indicadas. Para quaisquer $a_1, \dots, a_n \in K$ temos que

$$\mathcal{T}_{L|K}\left(\beta_i \cdot \left(\sum_{j=1}^n a_j \cdot \beta'_j\right)\right) = \sum_{j=1}^n a_j \cdot \mathcal{T}_{L|K}(\beta_i \cdot \beta'_j) = a_i \quad (i = 1, \dots, n);$$

portanto $\alpha = \sum_{j=1}^n a_j \cdot \beta'_j$ implica que $a_j = \mathcal{T}_{L|K}(\beta_j \cdot \alpha)$ ($j = 1, \dots, n$). Em particular, se $\alpha = 0$ então $a_1 = \dots = a_n = 0$; portanto $\beta'_1, \dots, \beta'_n$ são linearmente independentes, logo formam uma base da extensão L de K . $\square$

A base $\beta'_1, \dots, \beta'_n$ indicada em (4.6) é chamada a *base dual* da base $\beta_1, \dots, \beta_n$. É óbvio que, por outro lado, $\beta_1, \dots, \beta_n$ formam a base dual da base $\beta'_1, \dots, \beta'_n$ e que todo $\alpha \in L$ se escreve como $\alpha = \sum_{i=1}^n \mathcal{T}_{L|K}(\alpha \cdot \beta'_i) \cdot \beta_i$.

No que se segue, sejam R um domínio integralmente fechado e L uma extensão separável, de grau n , do corpo de frações $K = Q(R)$. Mostraremos que $I_L(R)$ está entre dois R -módulos livres, M e M' , sendo o primeiro gerado por uma base $\beta_1, \dots, \beta_n$ da extensão L de K tal que $\beta_j \in I_L(R)$ ($j = 1, \dots, n$) e o segundo pela base dual. Observamos que uma base $\beta_1, \dots, \beta_n$ deste tipo pode ser obtida multiplicando uma base arbitrária por um certo elemento $d \in R \setminus \{0\}$, uma vez que $L = (I_L(R))_{R \setminus \{0\}}$, por (1.7).

(4.7) **TEOREMA.** *Suponhamos que $\beta_1, \dots, \beta_n \in I_L(R)$ formem uma base da extensão L de K e $\beta'_1, \dots, \beta'_n$ a sua base dual. Então temos que $M \subseteq I_L(R) \subseteq M'$, onde $M = R \cdot \beta_1 + \dots + R \cdot \beta_n$ e $M' = R \cdot \beta'_1 + \dots + R \cdot \beta'_n$ são R -módulos livres, com bases $\beta_1, \dots, \beta_n$ e $\beta'_1, \dots, \beta'_n$, respectivamente.*

Demonstração. Obviamente, $\beta_1, \dots, \beta_n$ e $\beta'_1, \dots, \beta'_n$ são linearmente independentes sobre R ; portanto formam bases de M e M' respectivamente. A inclusão $M \subseteq I_L(R)$ é óbvia. Todo $\alpha \in I_L(R)$ escreve-se como $\alpha = \sum_{j=1}^n \mathcal{T}_{L|K}(\beta_j \cdot \alpha) \cdot \beta'_j$, por (4.6), e temos que $\mathcal{T}_{L|K}(\beta_j \cdot \alpha) \in R$ ($j = 1, \dots, n$), devido a (1.10). Portanto, temos que $I_L(R) \subseteq M'$. $\square$

Consideremos agora, para qualquer subanel S de $I_L(R)$ que contém R , o discriminante formado por n -uplas de elementos de S . De (1.10 a) resulta:

(4.8) Seja $R \subseteq S \subseteq I_L(R)$. Para quaisquer $\alpha_1, \dots, \alpha_n \in S$ temos que

$$\text{disc}_{L|K}(\alpha_1, \dots, \alpha_n) \in R.$$

O ideal $\mathfrak{d}_{S|R}$ de R , gerado pelo conjunto dos discriminantes $\text{disc}_{L|K}(\alpha_1, \dots, \alpha_n)$, onde $\alpha_1, \dots, \alpha_n$ percorrem todos os elementos de S , é chamado o *ideal discriminante* de $S|R$.

(4.9) Seja $R \subseteq S \subseteq I_L(R)$ e suponhamos que S , considerado como R -módulo, possua uma base $\beta_1, \dots, \beta_n$; então,

a) $\mathfrak{d}_{S|R}$ é um ideal principal, gerado por $\text{disc}_{L|K}(\beta_1, \dots, \beta_n)$. Além disto, para quaisquer $\alpha_1, \dots, \alpha_n \in S$, temos que:

b) $\text{disc}_{L|K}(\alpha_1, \dots, \alpha_n) = a^2 \cdot \text{disc}_{L|K}(\beta_1, \dots, \beta_n)$ para algum $a \in R$;

c) $\alpha_1, \dots, \alpha_n$ formarão uma base do R -módulo S se e somente se $a \in U(R)$.

Demonstração. b) Seja $\alpha_i = \sum_{j=1}^n a_{ij} \cdot \beta_j$ ($i = 1, \dots, n$), com $a_{ij} \in R$; então, a

igualdade indicada vale com $a = \det(a_{ij}) \in R$, por (4.1).

a) é uma consequência imediata de b).

c) $\alpha_1, \dots, \alpha_n$ formarão uma base do R -módulo S se e somente se a matriz (a_{ij}) possuir uma inversa com elementos em R , o que ocorrerá se e somente se $a \in U(R)$. $\square$

Concluimos de (4.9) que os discriminantes $\text{disc}_{L|K}(\beta_1, \dots, \beta_n)$ e $\text{disc}_{L|K}(\alpha_1, \dots, \alpha_n)$, formados por diferentes bases $\beta_1, \dots, \beta_n$ e $\alpha_1, \dots, \alpha_n$ do R -módulo S , se distinguem apenas por um fator que é o quadrado de um elemento invertível de R .

Exemplos de anéis S que satisfazem as hipóteses de (4.9) são fornecidos pelos anéis $R[\alpha]$, onde $\alpha \in I_L(R)$ é um elemento primitivo de $L|K$. De fato:

(4.10) Para qualquer $\alpha \in I_L(R)$, as seguintes condições são equivalentes:

(i) $L = K(\alpha)$.

(ii) $1, \alpha, \dots, \alpha^{n-1}$ formam uma base do R -módulo $R[\alpha]$.

Neste caso, $\mathfrak{d}_{R[\alpha]|R}$ é gerado por $\text{disc}_{L|K}(1, \alpha, \dots, \alpha^{n-1})$.

Demonstração. (i) $\Rightarrow$ (ii): Os elementos $1, \alpha, \dots, \alpha^{n-1}$ são linearmente independentes sobre K , logo também sobre R . Eles formam um sistema de geradores do R -módulo $R[\alpha]$, uma vez que α é raiz do polinômio mônico $P_{\alpha|K} \in R[X]$, de grau n .

(ii) $\Rightarrow$ (i): Como $1, \alpha, \dots, \alpha^{n-1}$ são linearmente independentes sobre K , temos que $[K(\alpha) : K] \geq n = [L : K]$; logo $K(\alpha) = L$.

A última afirmação resulta de (4.9). $\square$

A seguir, restringimo-nos ao caso em que L é um corpo de números algébricos, $n = [L : \mathbb{Q}]$ e $R = \mathbb{Z}$. Neste caso, obtemos de (4.9) a seguinte afirmação mais forte:

(4.11) *Seja $S \subseteq I_L$. Para todas as bases $\beta_1, \dots, \beta_n$ do $\mathbb{Z}$ -módulo S (caso tais bases existam), os discriminantes $\text{disc}_{L|\mathbb{Q}}(\beta_1, \dots, \beta_n)$ coincidem.*

Em particular, os discriminantes de todas as bases integrais de L coincidem.

Demonstração. Por (4.9), o quociente dos discriminantes de duas bases quaisquer do $\mathbb{Z}$ -módulo S é invertível e é um quadrado em $\mathbb{Z}$; logo é igual a 1. $\square$

Será provado no §5 que todo corpo de números algébricos L possui uma base integral $\beta_1, \dots, \beta_n$; o discriminante $\text{disc}_{L|\mathbb{Q}}(\beta_1, \dots, \beta_n)$ (que independe da escolha desta base, por (4.11)) é chamado o *discriminante do corpo L* e será denotado por d_L . Será mostrado também que nem sempre existe uma base integral da forma $1, \alpha, \dots, \alpha^{n-1}$. Condições necessárias e suficientes para a existência de uma base integral deste tipo são dadas na seguinte proposição, que é uma consequência imediata de (4.10) e (4.11).

(4.12) *Seja $[L : \mathbb{Q}] = n$. Para qualquer $\alpha \in I_L$, as seguintes condições são equivalentes:*

- (i) $I_L = \mathbb{Z}[\alpha]$.
- (ii) $1, \alpha, \dots, \alpha^{n-1}$ formam uma base integral de L .
- (iii) $d_L = \text{disc}_{L|\mathbb{Q}}(1, \alpha, \dots, \alpha^{n-1})$.

A seguir, calcularemos o discriminante d_L no caso de corpos quadráticos e ciclotômicos L . Veremos, em particular, que nestes casos existe um $\alpha \in I_L$ que satisfaz as condições equivalentes de (4.12). Quanto a um método para calcular o discriminante d_L no caso geral, veja Ribenboim [28], Chapter 13 (1).

A) Corpos quadráticos

Seja $L = \mathbb{Q}(\sqrt{d})$, sendo $d \in \mathcal{O}$. Para qualquer $\alpha = r + s \cdot \sqrt{d}$, com $r, s \in \mathbb{Q}$, temos que $\alpha^2 = (r^2 + s^2 \cdot d) + 2r \cdot s \cdot \sqrt{d}$; logo

$$\text{disc}_{L|\mathbb{Q}}(1, \alpha) = \det \begin{pmatrix} \mathcal{T}1 & \mathcal{T}\alpha \\ \mathcal{T}\alpha & \mathcal{T}\alpha^2 \end{pmatrix} = \det \begin{pmatrix} 2 & 2r \\ 2r & 2(r^2 + s^2 \cdot d) \end{pmatrix} = 4s^2 \cdot d.$$

Em particular, temos que $\text{disc}_{L|\mathbb{Q}}(1, \sqrt{d}) = 4d$ e $\text{disc}_{L|\mathbb{Q}}\left(1, \frac{1+\sqrt{d}}{2}\right) = d$.

Como $1, \sqrt{d}$ (respectivamente $1, \frac{1+\sqrt{d}}{2}$) formam uma base integral de L no caso em que $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) mod 4 (veja (2.3)), concluímos que:

$$(4.13) \quad d_L = \begin{cases} 4d & \text{quando } d \equiv 2 \text{ ou } 3 \pmod{4} \\ d & \text{quando } d \equiv 1 \pmod{4} \end{cases}$$

B) Corpos ciclotômicos

Seja $L = \mathbb{Q}(\zeta)$, sendo ζ uma raiz primitiva p -ésima da unidade, onde p é um número primo ímpar. Recordamos que $P_{\zeta|\mathbb{Q}} = F_{\zeta, L|\mathbb{Q}} = \Phi_p$, que $\Phi_p(\zeta^j) = 0$ para $j = 1, \dots, p-1$, e que $1, \zeta, \dots, \zeta^{p-2}$ formam uma base integral de L . Afirmamos que

$$(4.14) \quad d_L = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}.$$

Demonstração. Temos que $d_L = \text{disc}_{L|\mathbb{Q}}(1, \zeta, \dots, \zeta^{p-2}) = (-1)^{\binom{p-1}{2}} \mathcal{N}_{L|\mathbb{Q}}(\Phi_p'(\zeta))$ por (4.3). Como $\binom{p-1}{2} = \frac{p-1}{2} \cdot (p-2)$ e $\frac{p-1}{2}$ têm a mes-

ma paridade, basta provar que $\mathcal{N}_{L|\mathbb{Q}}(\Phi_p'(\zeta)) = p^{p-2}$. De $X^p - 1 = (X-1) \cdot \Phi_p$ obtemos que $p \cdot X^{p-1} = (X-1) \cdot \Phi_p' + \Phi_p$, logo $p \cdot \zeta^{p-1} = (\zeta - 1) \cdot \Phi_p'(\zeta)$. Aplicando a norma, resulta que $p^{p-1} = p \cdot \mathcal{N}_{L|\mathbb{Q}}(\Phi_p'(\zeta))$ por (3.10); logo $\mathcal{N}_{L|\mathbb{Q}}(\Phi_p'(\zeta)) = p^{p-2}$. $\square$

Mencionamos, sem demonstração, que a igualdade (4.14) se generaliza ao n -ésimo corpo ciclotômico, para qualquer $n > 1$ (podendo-se supor, sem perda de generalidade, que n seja ímpar ou divisível por 4) da seguinte maneira:

$$d_L = (-1)^{\frac{\varphi(n)}{2} \cdot s} \cdot \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}},$$

sendo s o número de fatores primos distintos, de n (veja Ribenboim [28], Chapter 13 (4)).

EXERCÍCIOS

- 4.1. Seja $[L:\mathbb{Q}] = n$ e seja s o número de isomorfismos de L em $\mathbb{R}$.
- Prove que $n - s$ é par.
 - Prove que $n - s$ será divisível por 4 se e somente se existir $\alpha \in L$ tal que $\text{disc}_{L|\mathbb{Q}}(1, \alpha, \dots, \alpha^{n-1}) > 0$. Neste caso, temos que $\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n) \geq 0$ para quaisquer $\alpha_1, \dots, \alpha_n \in L$.
- 4.2. Seja L um corpo quadrático.
- Dado $\alpha \in L \setminus \mathbb{Q}$, calcule a base dual da base $1, \alpha$.
 - Prove que $1, \frac{1}{2}(d_L + \sqrt{d_L})$ formam uma base integral de L .
- 4.3. Seja $[L:\mathbb{Q}] = n$ e suponhamos que $\beta_1, \dots, \beta_n \in I_L$ formem uma base da extensão L de $\mathbb{Q}$. Usando o fato (a ser demonstrado em (5.6)) que L possui uma base integral, prove que:
- $\beta_1, \dots, \beta_n$ formarão uma base integral de L se e somente se $|\text{disc}_{L|\mathbb{Q}}(\beta_1, \dots, \beta_n)| = \min(\{|\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n)| \mid \alpha_1, \dots, \alpha_n \in I_L \setminus \{0\}\})$.
 - $\beta_1, \dots, \beta_n$ formarão uma base integral de L se $\text{disc}_{L|\mathbb{Q}}(\beta_1, \dots, \beta_n)$ não for divisível por nenhum quadrado $c^2 \neq 1$ (onde $c \in \mathbb{Z}$).
 - Mostre, através de um exemplo, que não vale a afirmação inversa de b).
- 4.4. Seja $L = \mathbb{Q}(\alpha)$, sendo α uma raiz do polinômio $X^3 - 3X + 9$.
- Prove que $X^3 - 3X + 9$ é irredutível em $\mathbb{Q}[X]$.
 - Prove que $\text{disc}_{L|\mathbb{Q}}(1, \alpha, \alpha^2) = -27 \cdot 7 \cdot 11$.
 - Sendo $\beta = 3 \cdot \alpha^{-1}$, prove que $\beta \in I_L$, que $\mathbb{Z} + \mathbb{Z} \cdot \alpha + \mathbb{Z} \cdot \beta$ é um subanel de I_L e que $\mathbb{Z}[\alpha] \subset \mathbb{Z} + \mathbb{Z} \cdot \alpha + \mathbb{Z} \cdot \beta$.
 (Sugestão: Verifique que $\beta = 1 - \frac{1}{3}\alpha^2$).
 - Conclua que existe $m > 1$ tal que $\text{disc}_{L|\mathbb{Q}}(1, \alpha, \alpha^2) = m^2 \cdot \text{disc}_{L|\mathbb{Q}}(1, \alpha, \beta)$.
 - Usando o item b) do Exercício 4.3, conclua que $1, \alpha, \beta$ formam uma base integral de L .
- 4.5. Seja $L = \mathbb{Q}(\alpha)$, sendo α uma raiz do polinômio $X^3 - X - 1$ (respectivamente $X^3 + 10X + 1$). Prove que:
- Este polinômio é irredutível em $\mathbb{Q}[X]$.
 - $1, \alpha, \alpha^2$ formam uma base integral de L .
- 4.6. Determine uma base integral e o discriminante dos seguintes corpos de números algébricos: $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{6})$, $\mathbb{Q}(\sqrt[4]{2})$.

§5. Bases integrais

O nosso objetivo é mostrar que todo corpo de números algébricos L possui uma base integral, ou seja, que I_L é um $\mathbb{Z}$ -módulo livre. Como um primeiro passo, mostramos no §4 que I_L está contido num $\mathbb{Z}$ -módulo livre. De fato, de maneira mais geral, foi provado em (4.7) que, para qualquer domínio integralmente fechado R , o R -módulo $I_L(R)$ está contido no R -módulo livre $R \cdot \gamma_1 + \dots + R \cdot \gamma_n$, sendo $\gamma_1, \dots, \gamma_n$ uma base apropriada da extensão finita e separável L do corpo de frações $K = Q(R)$.

Assim podemos-nos restringir à questão de saber se todo submódulo de um R -módulo livre é livre. Para estudar esta questão, convém imergir o R -módulo livre M num K -espaço V , o que pode ser feito da seguinte maneira: Fixando uma base $\beta_1, \dots, \beta_n$ de M , consideramos o conjunto V de todas as combinações lineares "formais" $\sum_{j=1}^n a_j \cdot \beta_j$, onde $a_1, \dots, a_n$ percorrem K . Obviamente V é um K -espaço com base $\beta_1, \dots, \beta_n$ e, considerado como R -módulo, contém M como submódulo. Além disso, a construção de V independe da escolha da base, no sentido que os K -espaços construídos a partir de diferentes bases de M podem ser identificados.

Qualquer submódulo N de M gera um subespaço N_K do K -espaço V , consistindo de todas as somas finitas $a_1 \cdot v_1 + \dots + a_r \cdot v_r$, onde $v_1, \dots, v_r \in N$ e $a_1, \dots, a_r \in K$; em particular temos que $M_K = V$ e $(0)_K = (0)$. Pelo posto do R -módulo N entendemos a dimensão do K -espaço N_K , a qual no máximo é igual a n . Como a independência linear sobre R de elementos de N equivale à sua independência sobre K , concluímos que o posto de N é igual ao número de elementos de um sistema maximal de elementos de N linearmente independentes sobre R . Notamos que tal sistema nem sempre é uma base do R -módulo N , mas toda base do R -módulo N é um sistema deste tipo. Mencionamos ainda que o próprio M tem posto n , que (0) é o único submódulo de M que tem posto zero, e que $N \subset N' \subseteq M$ implica que o posto de N é no máximo igual a, mas nem sempre estritamente menor que, o posto de N' .

Vale a pena observar que a imersão de um R -módulo livre M num K -espaço V pode ser feita de uma maneira mais sofisticada, que dispensa a escolha de uma base de M , pelo processo de "extensão de escalares". Tal processo aplica-se a situações bem mais gerais, a saber, ao caso em que $R \subseteq S$ são anéis arbitrários e M é um R -módulo qualquer. Neste caso, o produto tensorial $S \otimes_R M$ é um S -módulo, e existe um homomorfismo (nem sempre injetivo) de M sobre um submódulo M_S de $S \otimes_R M$,

sendo este considerado como R -módulo. (Veja Exercício 5.6 e Atiyah-Macdonald [3], p. 27.)

Para que todo submódulo de um R -módulo livre seja livre, é necessário que o domínio R seja principal, como mostra o Exercício 5.4. O seguinte teorema mostra que esta condição também é suficiente. Utilizaremos na demonstração deste teorema o fato que, para domínios principais, todo conjunto não vazio de ideais possui um elemento maximal, o que será provado, num contexto mais amplo, em (7.3).

(5.1) TEOREMA. *Sejam R um domínio principal, M um R -módulo livre de posto n e M' um submódulo de M de posto q (sendo $q \leq n$). Então:*

- a) M' é um R -módulo livre.
- b) *Existem uma base $e_1, \dots, e_n$ de M e elementos $a_1, \dots, a_q \in R$ tais que $a_1 | a_2 | \dots | a_q$ e $a_1 \cdot e_1, \dots, a_q \cdot e_q$ formem uma base de M' .*

Demonstração. a) Podemos supor que $M' \neq (0)$. Consideremos o conjunto $\mathcal{L}(M, R)$ das "formas R -lineares" de M , isto é, dos homomorfismos do R -módulo M no R -módulo R . Obviamente $\mathcal{L}(M, R)$ é um R -módulo, sendo a adição e a multiplicação externa definidas respectivamente por

$$v + w: \gamma \mapsto v(\gamma) + w(\gamma) \quad \text{e} \quad a \cdot v: \gamma \mapsto a \cdot v(\gamma) \quad (\gamma \in M),$$

onde $v, w \in \mathcal{L}(M, R)$ e $a \in R$.

Para qualquer $v \in \mathcal{L}(M, R)$, $v(M')$ é um ideal de R . No conjunto $\{v(M') \mid v \in \mathcal{L}(M, R)\}$ escolhemos um elemento maximal, digamos $u(M') = a_u \cdot R$, sendo $u \in \mathcal{L}(M, R)$ e $a_u \in R$. Mostraremos primeiro que

(1) $a_u = 0$.

De fato, suponhamos que $\beta_1, \dots, \beta_n$ formam uma base de M e, para $j = 1, \dots, n$, seja $pr_j \in \mathcal{L}(M, R)$ definido por $\sum_{i=1}^n a_i \cdot \beta_i \mapsto a_j$ ($a_1, \dots, a_n \in R$).

Como M' possui um elemento não-nulo, digamos $\gamma = \sum_{i=1}^n c_i \cdot \beta_i$, existe

$k \in \{1, \dots, n\}$ tal que $pr_k(\gamma) = c_k \neq 0$; logo $pr_k(M') \neq (0)$. Concluimos que $a_u \neq 0$, devido à maximalidade de $u(M')$.

Escolhendo $\epsilon' \in M'$ tal que $u(\epsilon') = a_u$, afirmamos que

(2) a_u divide $v(e')$ para qualquer $v \in \mathcal{L}(M, R)$.

De fato, sendo R um domínio principal, os elementos $a_u, v(e')$ possuem um máximo divisor comum da forma $d = b \cdot a_u + c \cdot v(e')$, com $b, c \in R$, ou seja, $d = w(e')$, onde $w = b \cdot u + c \cdot v \in \mathcal{L}(M, R)$. De $d \mid a_u$ decorre que $a_u \cdot R \subseteq d \cdot R = w(e') \cdot R \subseteq w(M')$, e valem mesmo as igualdades, devido à maximalidade de $a_u \cdot R$. Concluímos que a_u é associado a d e, portanto, é um divisor de $v(e')$.

(3) Existe $\varepsilon \in M$ tal que $\varepsilon' = a_u \cdot \varepsilon$ e $u(\varepsilon) = 1$.

De fato, de (2) resulta que, para cada $j \in \{1, \dots, n\}$, existe $e_j \in R$ tal que $\text{pr}_j(e') = a_u \cdot e_j$. Seja $\varepsilon = \sum_{j=1}^n e_j \cdot \beta_j$; então $a_u \cdot \varepsilon = \sum_{j=1}^n a_u \cdot e_j \cdot \beta_j = \sum_{j=1}^n \text{pr}_j(e') \cdot \beta_j = \varepsilon'$. De $a_u = u(e') = u(a_u \cdot \varepsilon) = a_u \cdot u(\varepsilon)$ decorre que $u(\varepsilon) = 1$.

(4) M é soma direta dos submódulos $\text{Ker } u$ e $R \cdot \varepsilon$.

De fato, qualquer $\alpha \in M$ escreve-se como $\alpha = (\alpha - u(\alpha) \cdot \varepsilon) + u(\alpha) \cdot \varepsilon$, e temos que $\alpha - u(\alpha) \cdot \varepsilon \in \text{Ker } u$ devido a (3). Se $r \in R$ tal que $r \cdot \varepsilon \in \text{Ker } u$, então $0 = u(r \cdot \varepsilon) = r \cdot u(\varepsilon) = r$, logo $r \cdot \varepsilon = 0$; portanto $\text{Ker } u \cap R \cdot \varepsilon = (0)$, e assim a soma $\text{Ker } u + R \cdot \varepsilon$ é direta.

(5) M' é soma direta dos submódulos $M' \cap \text{Ker } u$ e $R \cdot \varepsilon'$.

De fato, escrevendo-se $\alpha \in M'$ como acima e observando-se que $u(\alpha) \in u(M') = a_u \cdot R$, concluímos que existe $b \in R$ tal que

$$\alpha = (\alpha - b \cdot a_u \cdot \varepsilon) + b \cdot a_u \cdot \varepsilon = (\alpha - b \cdot \varepsilon') + b \cdot \varepsilon' \in (\text{Ker } u \cap M') + R \cdot \varepsilon'.$$

De (4) resulta que a soma $(M' \cap \text{Ker } u) + R \cdot \varepsilon'$ é direta.

Completamos a demonstração de a) por indução sobre q . Sendo trivial para $q = 0$, supomos a) válido para quaisquer submódulos de M de posto $q - 1$, onde $q > 0$. De (5) resulta que o K -espaço M'_K é soma direta dos subespaços $(M' \cap \text{Ker } u)_K$ e $(R \cdot \varepsilon')_K = K \cdot \varepsilon'$; logo o posto de $M' \cap \text{Ker } u$ é igual a $q - 1$. Pela hipótese de indução, $M' \cap \text{Ker } u$ é um R -módulo livre. Usando novamente (5), concluímos que M' é um R -módulo livre.

b) A demonstração será feita por indução sobre n . Sendo trivial para $n = 0$, supomos b) válido para qualquer R -módulo livre de posto $n - 1$, onde $n > 0$. Consideramos o R -módulo $\text{Ker } u$ e o submódulo $M' \cap \text{Ker } u$. Pela parte a) do teorema, $\text{Ker } u$ é livre, e de (4) e (5) resulta que $\text{Ker } u$ e $M' \cap \text{Ker } u$ têm posto $n - 1$ e $q - 1$, respectivamente. Por hipótese, existem uma base $\varepsilon_2, \dots, \varepsilon_n$ de $\text{Ker } u$ e elementos $a_2, \dots, a_q \in R$

tais que $a_2 | a_3 | \dots | a_q$ e que $a_2 \cdot \varepsilon_2, \dots, a_n \cdot \varepsilon_q$ formem uma base de $M' \cap \text{Ker } \alpha$. Concluímos de (4) e (5) que $\varepsilon, \varepsilon_2, \dots, \varepsilon_n$ formam uma base de M e que $a_u \cdot \varepsilon, a_2 \cdot \varepsilon_2, \dots, a_q \cdot \varepsilon_q$ formam uma base de M' . Resta provar que a_u divide a_2 . De fato, seja $w \in \mathcal{L}(M, R)$ definido por

$$c_1 \cdot \varepsilon + c_2 \cdot \varepsilon_2 + \dots + c_n \cdot \varepsilon_n \mapsto c_1 + c_2 \quad (c_1, \dots, c_n \in R);$$

então $a_u = w(a_u \cdot \varepsilon) \in w(M')$, logo $a_u R = w(M')$ devido à maximalidade de $a_u \cdot R$. Por outro lado, $a_2 = w(a_2 \cdot \varepsilon_2) \in w(M') = a_u \cdot R$, logo $a_u | a_2$. $\square$

Mencionamos sem demonstração que os ideais $a_1 \cdot R, \dots, a_q \cdot R$ são univocamente determinados por M e M' e são chamados as *invariantes* de M' em M (veja S. Lang [20], p. 394-395).

(5.2) COROLÁRIO. Com as notações usadas em (5.1), o isomorfismo do R -módulo $\underbrace{R \times \dots \times R}_n$ sobre M definido por

$$(r_1, \dots, r_n) \mapsto \sum_{j=1}^n r_j \cdot \varepsilon_j \quad (r_1, \dots, r_n \in R)$$

induz um isomorfismo do R -módulo $R/(a_1 \cdot R) \times \dots \times R/(a_q \cdot R) \times \underbrace{R \times \dots \times R}_{n-q}$ sobre M/M' .

Demonstração. Seja $\gamma = \sum_{j=1}^n r_j \cdot \varepsilon_j$. Por (5.1b) teremos que $\gamma \in M'$ se e somente se $r_1 \in a_1 \cdot R, \dots, r_q \in a_q \cdot R, r_{q+1} = \dots = r_n = 0$. $\square$

De (5.2) obtemos um importante corolário sobre R -módulos finitamente gerados:

(5.3) COROLÁRIO. Sejam R um domínio principal e N um R -módulo gerado por n elementos. Então existem $s, t \in \mathbb{N}'$ com $s+t \leq n$ e elementos não-nulos $a_1, \dots, a_s \in R \setminus U(R)$ tais que $a_1 | a_2 | \dots | a_s$ e N seja isomorfo ao R -módulo $R/(a_1 \cdot R) \times \dots \times R/(a_s \cdot R) \times \underbrace{R \times \dots \times R}_t$.

Demonstração. Sendo $N = R \cdot \gamma_1 + \dots + R \cdot \gamma_n$, a aplicação definida por

$$(r_1, \dots, r_n) \mapsto \sum_{j=1}^n r_j \cdot \gamma_j \text{ é um homomorfismo do } R\text{-módulo}$$

livre $M = \underbrace{R \times \dots \times R}_n$ sobre N ; logo N é isomorfo a M/M' , sen-

do M' o núcleo deste homomorfismo. De (5.2) resulta que N é isomorfo a $R/(a_1 \cdot R) \times \dots \times R/(a_q \cdot R) \times \underbrace{R \times \dots \times R}_{n-q}$, e neste produto podem ser

suprimidos os fatores triviais, correspondentes àqueles elementos a_j que são invertíveis em R . $\square$

Aplicado a $\mathbb{Z}$ -módulos, ou seja, a grupos abelianos, este corolário fornece uma demonstração do teorema fundamental de grupos abelianos finitamente gerados (veja Exercício 5.2).

Finalmente, utilizaremos o teorema (5.1) para mostrar que todo corpo de números algébricos L possui uma base integral. Mais precisamente, trataremos da seguinte situação mais geral: Em lugar da extensão $L|\mathbb{Q}$ consideramos uma extensão separável finita $L|\mathbb{Q}(R)$, onde R é qualquer domínio principal e, além disto, consideraremos não somente o anel $I_L(R)$ mas também seus subanéis.

(5.4) TEOREMA. *Sejam R um domínio integralmente fechado e L uma extensão separável de $K = \mathbb{Q}(R)$, de grau n . Então,*

- a) *o R -módulo $I_L(R)$ tem posto n .*
- b) *Se R for um domínio principal então, para todo anel S entre R e L , as seguintes condições são equivalentes:*

- (i) $S \subseteq I_L(R)$;
- (ii) S é um R -módulo livre de posto $q \leq n$;
- (iii) S é um R -módulo finitamente gerado.

Neste caso, $q = n$ se e somente se $L = \mathbb{Q}(S)$.

Demonstração. a) Por (4.7), $I_L(R)$ está entre dois R -módulos livres de posto n ; portanto tem posto n .

b) (i) $\Rightarrow$ (ii): Por (4.7), S é um submódulo de um R -módulo livre de posto n ; portanto, a afirmação resulta de (5.1). (ii) $\Rightarrow$ (iii) é trivial. (iii) $\Rightarrow$ (i) resulta de (1.3b). Quanto à equivalência das igualdades $q = n$ e $L = \mathbb{Q}(S)$, veja o final do §0. $\square$

Restringindo-nos ao caso de um corpo de números algébricos L e $R = \mathbb{Z}$, concluímos que os subaneis S de L que são $\mathbb{Z}$ -módulos finitamente gerados, coincidem com os subanéis de I_L e são mesmo $\mathbb{Z}$ -módulos livres de posto $\leq n$. Além disto, obtemos o seguinte

(5.5) COROLÁRIO. Seja $[L:\mathbb{Q}] = n$. Para qualquer subanel S de L , as seguintes condições são equivalentes:

- (i) $S \subseteq I_L$ e $L = Q(S)$.
- (ii) S é um $\mathbb{Z}$ -módulo livre de posto n .

Em particular, I_L é um $\mathbb{Z}$ -módulo livre de posto n .

Os subanéis S de L que satisfazem as condições equivalentes de (5.5) são chamados (numa terminologia antiga) as “ordens” de L , e o anel I_L , sendo a maior destas “ordens”, é chamado a “ordem máxima” de L .

A última afirmação de (5.5) pode ser reformulada da seguinte maneira:

(5.6) COROLÁRIO. Todo corpo de números algébricos possui uma base integral.

Entre as “ordens” de L distinguem-se os anéis $\mathbb{Z}[\alpha]$, onde $\alpha \in I_L$ é um elemento primitivo de $L|\mathbb{Q}$ (veja Exercício 5.7). Por (4.9), temos que $\text{disc}_{L|\mathbb{Q}}(1, \alpha, \dots, \alpha^{n-1}) = k_\alpha^2 \cdot d_L$ para um certo número $k_\alpha \in \mathbb{N}$, o qual é chamado o índice de α . Este nome se justifica pela propriedade indicada no seguinte teorema.

(5.7) TEOREMA. Seja $\alpha \in I_L$ um elemento primitivo de $L|\mathbb{Q}$. Então, k_α é igual ao índice de $\mathbb{Z}[\alpha]$ em I_L , sendo ambos considerados como grupos aditivos.

Demonstração. Como $\mathbb{Z}[\alpha]$ é um submódulo do $\mathbb{Z}$ -módulo livre I_L e ambos têm posto n , concluímos de (5.1) e (5.2) que existem uma base $e_1, \dots, e_n$ de I_L e elementos $k_1, \dots, k_n \in \mathbb{Z}$ tais que $k_1 \cdot e_1, \dots, k_n \cdot e_n$ formam uma base de $\mathbb{Z}[\alpha]$. O grupo $I_L/\mathbb{Z}[\alpha]$ é isomorfo a $\mathbb{Z}/(k_1 \cdot \mathbb{Z}) \times \dots \times \mathbb{Z}/(k_n \cdot \mathbb{Z})$ e, portanto, tem ordem $|k_1 \cdot \dots \cdot k_n|$. Por outro lado, concluímos de (4.1) e (4.11) que

$$\begin{aligned} \text{disc}_{L|\mathbb{Q}}(1, \alpha, \dots, \alpha^{n-1}) &= \text{disc}_{L|\mathbb{Q}}(k_1 \cdot e_1, \dots, k_n \cdot e_n) = \\ &= (k_1 \cdot \dots \cdot k_n)^2 \cdot \text{disc}_{L|\mathbb{Q}}(e_1, \dots, e_n) = |k_1 \cdot \dots \cdot k_n|^2 \cdot d_L. \quad \square \end{aligned}$$

De (5.7) resulta em particular que $k_\alpha = 1$ se e somente se $I_L = \mathbb{Z}[\alpha]$, como já foi mostrado em (4.12).

Apesar de $\mathbb{Z}[\alpha]$ ser, em geral, um subanel próprio de I_L , mostraremos que os dois anéis “coincidem mod $\mathfrak{p}$ ”, para todo o ideal maximal $\mathfrak{p}$

de I_L que não contiver k_α , no sentido que a restrição a $\mathbb{Z}[\alpha]$ do homomorfismo canônico $I_L \rightarrow I_L/\mathfrak{p}$ é sobrejetiva. Em outras palavras:

(5.8) COROLÁRIO. *Seja $\alpha \in I_L$ um elemento primitivo de $L|\mathbb{Q}$ e seja $\mathfrak{p}$ um ideal maximal de I_L tal que $k_\alpha \notin \mathfrak{p}$. Então, para todo $\gamma \in I_L$, existe $\gamma' \in \mathbb{Z}[\alpha]$ tal que $\gamma - \gamma' \in \mathfrak{p}$.*

Demonstração. De $\mathfrak{p} + k_\alpha \cdot I_L = I_L$ resulta a existência de um $\beta \in I_L$ tal que $1 - k_\alpha \cdot \beta \in \mathfrak{p}$; logo $\gamma - k_\alpha \cdot \beta \cdot \gamma \in \mathfrak{p}$ para todo $\gamma \in I_L$. De (5.7) concluímos que $k_\alpha \cdot \beta \cdot \gamma \in \mathbb{Z}[\alpha]$. $\square$

Como já foi mencionado anteriormente, nem todo corpo de números algébricos L possui uma base integral da forma $1, \alpha, \dots, \alpha^{n-1}$, ou seja, nem sempre I_L é da forma $\mathbb{Z}[\alpha]$. De fato, o seguinte exemplo, devido a Dedekind, mostra que existe um corpo cúbico L tal que $k_\alpha \neq 1$ para todo elemento primitivo $\alpha \in I_L$, e mesmo o máximo divisor comum $k = \text{MDC}\{k_\alpha \mid \alpha \in I_L\}$ (chamado o *divisor não essencial* de discriminante) seja diferente de 1.

EXEMPLO (veja Ribenboim [28], Chapter 13(2), ou Samuel [30], Exercise 9B): Seja $L = \mathbb{Q}(\beta)$, onde $P_{\beta|\mathbb{Q}} = X^3 + X^2 - 2 \cdot X + 8$. Como $1, \beta, 4 \cdot \beta^{-1}$ formam uma base integral de L , temos que $d_L = \text{disc}_{L|\mathbb{Q}}(1, \beta, 4 \cdot \beta^{-1}) = -503$. Por outro lado, $\text{disc}_{L|\mathbb{Q}}(1, \beta, \beta^2) = 4 \cdot d_L$ e, para qualquer $\gamma \in I_L$, $\text{disc}_{L|\mathbb{Q}}(1, \gamma, \gamma^2)$ é um múltiplo de $4 \cdot d_L$; portanto $k = 2$.

EXERCÍCIOS

- 5.1. Seja A um grupo abeliano (escrito aditivamente) e seja $T(A) = \{a \in A \mid na = 0 \text{ para algum } n > 0\}$ o seu grupo de torção. Supondo que $T(A) \neq \{0\}$ prove que:
- Considerado como $\mathbb{Z}$ -módulo, A não é livre.
 - Não existe nenhum $\mathbb{Q}$ -espaço V tal que A seja um submódulo de V , considerado como $\mathbb{Z}$ -módulo.
- 5.2. Sejam A e $T(A)$ como em 5.1. Supondo que A seja finitamente gerado, use o Corolário (5.3) para provar que:
- A é soma direta de $T(A)$ e de um número finito de subgrupos cíclicos infinitos.
 - $T(A)$ é soma direta de subgrupos cíclicos finitos $Z_1, \dots, Z_s$ tais que a ordem de Z_j divide a de Z_{j+1} ($j = 1, \dots, s-1$).

- c) $T(A)$ é soma direta de subgrupos cíclicos $Z_1', \dots, Z_t'$ cujas ordens são potências de números primos.
- d) Existe $\alpha \in T(A)$ tal que $o(\alpha) = \text{MMC}\{o(\gamma) \mid \gamma \in T(A)\}$.
- 5.3. a) Conclua de 5.2.a) que um grupo abeliano A finitamente gerado será livre se e somente se não tiver torção (isto é, se $T(A) = \{0\}$).
- b) Prove que o grupo aditivo $\mathbb{Q}^+$ do corpo $\mathbb{Q}$ não tem torção mas não é livre. Calcule o posto de $\mathbb{Q}^+$ (considerado como $\mathbb{Z}$ -módulo).
- 5.4. Seja R um domínio. Prove que:
- a) Todo ideal não-nulo de R (considerado como submódulo do R -módulo R) tem posto 1.
- b) Se todo ideal de R for um R -módulo livre então R será um domínio principal.
- 5.5. Seja L uma extensão do corpo $\mathbb{Q}(i)$ dos números de Gauss, de grau $[L : \mathbb{Q}(i)] = m$. Prove que existem $\beta_1, \dots, \beta_m \in L$ tais que $\beta_1, \dots, \beta_m, i \cdot \beta_1, \dots, i \cdot \beta_m$ formem uma base integral de L .
- 5.6. Sejam R um domínio, $K = \mathbb{Q}(R)$ e M um R -módulo. Prove:
- a) A relação definida em $M \times (R \setminus \{0\})$ por
- $$(x, r) \sim (y, s) \Leftrightarrow t \cdot (s \cdot x - r \cdot y) = 0 \text{ para algum } t \in R \setminus \{0\}$$
- é uma relação de equivalência. Denotamos por x/r a classe determinada por (x, r) .
- b) A adição e a operação externa do R -módulo M estendem-se de maneira natural ao conjunto $V = \{x/r \mid x \in M, r \in R \setminus \{0\}\}$, tornando-o um K -espaço.
- c) A aplicação $f : M \rightarrow V$ definida por $x \mapsto x/1$ ($x \in M$) é um homomorfismo de M em V , considerado como R -módulo, com núcleo $T(M) = \{x \in M \mid t \cdot x = 0 \text{ para algum } t \in R \setminus \{0\}\}$.
- d) Se M for um R -módulo livre, então f será injetivo, e a imagem sob f de qualquer base do R -módulo M será uma base do K -espaço V .
- 5.7. Seja L um corpo de números algébricos. Prove:
- a) Um subanel S de L será uma "ordem" de L se e somente se existir um sistema de geradores $\gamma_1, \dots, \gamma_s$ do $\mathbb{Q}$ -espaço L tais que $S = \mathbb{Z} \cdot \gamma_1 + \dots + \mathbb{Z} \cdot \gamma_s$.
- b) Toda "ordem" de L contém uma "ordem" do tipo $\mathbb{Z}[\alpha]$, onde $\alpha \in I_L$ e $\mathbb{Q}(\alpha) = L$.

ANÉIS NOETHERIANOS E
DOMÍNIOS DE DEDEKIND

O exemplo do corpo quadrático $\mathbb{Q}(\sqrt{-5})$ mostra que o anel dos inteiros algébricos I_L de um corpo de números algébricos L nem sempre é fatorial (veja (2.4)). Para consertar esta falha, foi introduzido por Kummer a noção de “número ideal”, que deu origem à noção de “ideal”, devida a Dedekind. Em lugar da fatoração única em potências de elementos irredutíveis, válida apenas no caso de domínios fatoriais, prova-se que, em qualquer I_L , todo ideal não-nulo possui uma fatoração única em potências de ideais primos. Esta e outras propriedades de I_L generalizam-se facilmente a uma classe de domínios chamados “domínios de Dedekind”, como foi demonstrado por E. Noether.

O estudo de domínios de Dedekind, que será feito no §8, é o objetivo principal deste capítulo. Para isto necessitaremos de alguns resultados relacionados com o “Teorema Chinês de Restos”, que serão apresentados no §6, e de alguns fatos básicos sobre anéis noetherianos, a serem provados no §7.

§6. O Teorema Chinês de Restos

Seja R um anel. Para quaisquer ideais a, b de R , a *interseção* $a \cap b$ é o maior ideal de R que está contido em a e b , e a *soma* $a + b = \{a + b \mid a \in a, b \in b\}$ é o menor ideal de R que contém a e b . Estas noções generalizam-se, de maneira óbvia, à interseção e à soma de um conjunto qualquer de ideais de R .

O *produto* $a \cdot b$, definido como o conjunto das somas finitas $a_1 \cdot b_1 + \dots + a_r \cdot b_r$, onde $a_j \in a, b_j \in b, 1 \leq j \leq r \in \mathbb{N}$, é um ideal de R contido em $a \cap b$. Mais geralmente, definem-se o produto $\prod a_j$ de um número finito de ideais a_j e, em particular, as potências $a^0 = R, a^1 = a, a^2 = a \cdot a, \dots, a^m = \underbrace{a \cdot \dots \cdot a}_m$ de um ideal a .

É óbvio que, para cada uma destas operações, valem as leis de associatividade e comutatividade, e que vale a distributividade da multiplicação em relação à adição, isto é,

$$(a) \quad a \cdot (b + b') = a \cdot b + a \cdot b',$$

da qual decorre imediatamente que

$$(b) \quad (a \cap b) \cdot (a + b) \subseteq a \cdot b.$$

É óbvio também que valem as seguintes inclusões

$$(c) \quad a \cdot (b \cap b') \subseteq a \cdot b \cap a \cdot b',$$

$$(d) \quad a \cap (b + b') \supseteq (a \cap b) + (a \cap b'),$$

$$(e) \quad a + (b \cap b') \subseteq (a + b) \cap (a + b'),$$

mas nem sempre valem as igualdades, isto é, a distributividade da multiplicação em relação à interseção e as distributividades mútuas entre interseção e adição (veja Exercícios 6.1 e 6.2).

Dado qualquer ideal a de R , o conjunto

$$\sqrt{a} = \{r \in R \mid \text{existe } n \in \mathbb{N} \text{ tal que } r^n \in a\}$$

é um ideal de R e é chamado o *radical* de a . É óbvio que

$$(f) \quad a \subseteq \sqrt{a} = \sqrt{\sqrt{a}},$$

$$(g) \quad a \subseteq b \Rightarrow \sqrt{a} \subseteq \sqrt{b},$$

$$(h) \quad a = R \Leftrightarrow \sqrt{a} = R,$$

o que significa que a aplicação definida por $a \mapsto \sqrt{a}$ é uma operação de fecho no conjunto dos ideais de R , bem como no conjunto dos ideais de R que são distintos de R . Mostremos ainda:

$$(6.1) \quad (i) \quad \sqrt{a \cdot b} = \sqrt{a \cap b} = \sqrt{a} \cap \sqrt{b}.$$

$$(j) \quad \sqrt{a^n} = \sqrt{a} \text{ para qualquer } n \geq 1.$$

$$(k) \quad \sqrt{p} = p \text{ para qualquer ideal primo } p \text{ de } R.$$

$$(l) \quad \sqrt{a + b} = \sqrt{\sqrt{a} + \sqrt{b}}.$$

Demonstração. (i) Seja $r \in \sqrt{a \cap b}$, digamos $r^n \in a$, $r^m \in b$, onde $n, m \in \mathbb{N}$; então $r^{n+m} \in a \cdot b$, logo $r \in \sqrt{a \cdot b}$. As inclusões $\subseteq$ são óbvias.

(j) resulta imediatamente de (i).

(k) Se $r \in \sqrt{p}$ então $r^n \in p$ para algum $n \geq 1$; logo $r \in p$.

(l) Seja $r \in \sqrt{\sqrt{a} + \sqrt{b}}$; então existem $s \in \sqrt{a}$, $t \in \sqrt{b}$ e $n, k, \ell \in \mathbb{N}$

tais que $r^n = s + t$, $s^k \in \mathfrak{a}$ e $t^{\ell} \in \mathfrak{b}$. Logo $r^{n \cdot (k+\ell-1)} = (s+t)^{k+\ell-1} = s^k \cdot u + t^{\ell} \cdot v \in \mathfrak{a} + \mathfrak{b}$, para certos $u, v \in R$; portanto $r \in \sqrt{\mathfrak{a} + \mathfrak{b}}$. $\square$

Diremos que os ideais $\mathfrak{a}, \mathfrak{b}$ de R são *comaximais* se $\mathfrak{a} + \mathfrak{b} = R$. Obviamente, isto ocorrerá quando $\mathfrak{a}, \mathfrak{b}$ forem ideais maximais distintos ou, mais geralmente, quando $\mathfrak{a}$ for maximal e $\mathfrak{b} \not\subseteq \mathfrak{a}$. De (b) e da inclusão $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ resulta imediatamente:

(6.2) Se $\mathfrak{a}, \mathfrak{b}$ forem comaximais então $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.

Além disto, de (h), (l) e (j) concluímos:

(6.3) $\mathfrak{a}, \mathfrak{b}$ serão comaximais se e somente se $\sqrt{\mathfrak{a}}, \sqrt{\mathfrak{b}}$ forem comaximais. Neste caso, $\mathfrak{a}^m, \mathfrak{b}^n$ são comaximais para quaisquer $m, n \in \mathbb{N}$.

Dado um ideal $\mathfrak{a}$ de R , diremos que elementos $r, s \in R$ são *côngruos módulo $\mathfrak{a}$* , e escreveremos $r \equiv s \pmod{\mathfrak{a}}$, quando $r - s \in \mathfrak{a}$. Consideremos a seguinte questão: Dados ideais $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ e elementos $r_1, \dots, r_n$ de R , existe $r \in R$ tal que $r \equiv r_j \pmod{\mathfrak{a}_j}$ para $j = 1, \dots, n$? Ou seja, o "sistema de congruências" $X \equiv r_j \pmod{\mathfrak{a}_j} (j = 1, \dots, n)$ tem uma solução? No caso $n = 2$ obtemos a seguinte resposta:

(6.4) Sejam $\mathfrak{a}_1, \mathfrak{a}_2$ ideais de R e $r_1, r_2 \in R$. Então, existirá $r \in R$ tal que $r \equiv r_j \pmod{\mathfrak{a}_j} (j = 1, 2)$ se e somente se $r_1 \equiv r_2 \pmod{\mathfrak{a}_1 + \mathfrak{a}_2}$.

Demonstração. Se $r \equiv r_j \pmod{\mathfrak{a}_j} (j = 1, 2)$, então

$$r_2 - r_1 = (r - r_1) - (r - r_2) \in \mathfrak{a}_1 + \mathfrak{a}_2.$$

Por outro lado, se $r_1 \equiv r_2 \pmod{\mathfrak{a}_1 + \mathfrak{a}_2}$, então existirão $a_1 \in \mathfrak{a}_1$ e $a_2 \in \mathfrak{a}_2$ tais que $r_1 - r_2 = a_1 - a_2$; logo $r_1 - a_1 = r_2 - a_2 \equiv r_j \pmod{\mathfrak{a}_j} (j = 1, 2)$. $\square$

No caso especial em que $\mathfrak{a}_1, \mathfrak{a}_2$ são comaximais, a condição $r_1 \equiv r_2 \pmod{\mathfrak{a}_1 + \mathfrak{a}_2}$ é obviamente satisfeita por quaisquer $r_1, r_2 \in R$. Mais geralmente, para $n \geq 2$, obtemos o seguinte

(6.5) TEOREMA. Para quaisquer ideais $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ de R , com $n \geq 2$, as seguintes condições são equivalentes:

- (i) $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ são comaximais dois a dois.
- (ii) Para quaisquer $r_1, \dots, r_n \in R$ existe $r \in R$ tal que $r \equiv r_j \pmod{\mathfrak{a}_j} (j = 1, \dots, n)$.

Neste caso, $\mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n = \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$.

Demonstração. (i) $\Rightarrow$ (ii): Demonstraremos a última igualdade por indução em n . Como ela é válida para $n = 2$, devido a (6.2), supomos que $a_1 \cdot \dots \cdot a_{n-1} = a_1 \cap \dots \cap a_{n-1}$, onde $n > 2$. Afirmamos que os dois ideais $a_1 \cdot \dots \cdot a_{n-1}$ e a_n são comaximais. De fato, para cada $j < n$ existem $r_j \in a_j$ e $s_j \in a_n$ tais que $r_j + s_j = 1$; logo

$$r_1 \cdot \dots \cdot r_{n-1} = (1 - s_1) \cdot \dots \cdot (1 - s_{n-1}) = 1 + s$$

com $s \in a_n$; portanto $a_1 \cdot \dots \cdot a_{n-1} + a_n = R$. De (6.2) resulta que

$$(a_1 \cdot \dots \cdot a_{n-1}) \cdot a_n = (a_1 \cap \dots \cap a_{n-1}) \cap a_n.$$

Analogamente à construção do elemento $t_n = r_1 \cdot \dots \cdot r_{n-1} \in a_1 \cdot \dots \cdot a_{n-1}$ satisfazendo $t_n - 1 \in a_n$, construímos, para cada $j = 1, \dots, n$, um elemento $t_j \in a_1 \cdot \dots \cdot a_{j-1} \cdot a_{j+1} \cdot \dots \cdot a_n$ com $t_j - 1 \in a_j$. Para quaisquer $r_1, \dots, r_n \in R$, o elemento $r = r_1 \cdot t_1 + \dots + r_n \cdot t_n$ obviamente satisfaz a condição (ii).

(ii) $\Rightarrow$ (i): Para $r_1 = 1$ e $r_2 = 0$, concluímos de (6.4) que $1 \equiv 0 \pmod{a_1 + a_2}$; logo a_1, a_2 são comaximais. Analogamente, a_i, a_j são comaximais para qualquer par $i, j, i \neq j$. $\square$

De (6.5) e (6.3) segue imediatamente:

(6.6) COROLÁRIO. *Sejam $a_1, \dots, a_n$ ideais comaximais dois a dois, onde $n \geq 2$. Quaisquer que sejam $k_1, \dots, k_n \in \mathbb{N}$ e $r_1, \dots, r_n \in R$, existe $r \in R$ tal que $r \equiv r_j \pmod{a_j^{k_j}}$ ($j = 1, \dots, n$).*

Este corolário afirma que quaisquer elementos $r_1, \dots, r_n \in R$ podem ser “aproximados” simultaneamente por um elemento $r \in R$, em relação às topologias $a_1, \dots, a_n$ -ádicas, respectivamente (veja Atiyah-Macdonald [3], Chapter 10). Em outras palavras, a imagem de R pela “aplicação diagonal” $R \rightarrow R \times \dots \times R$ (definida por $r \mapsto (r, \dots, r)$) é densa no espaço

produto $\underbrace{R \times \dots \times R}_n$, no qual o j -ésimo fator R está munido da topologia a_j -ádica ($j = 1, \dots, n$).

O teorema (6.5) admite ainda uma outra reformulação interessante. Dados quaisquer ideais $a_1, \dots, a_n$ de R , consideremos o produto cartesiano $\mathfrak{R} = R/a_1 \times \dots \times R/a_n$ (o qual é um anel em relação às operações componente a componente) e o homomorfismo $R \rightarrow \mathfrak{R}$ definido por $r \mapsto (r + a_1, \dots, r + a_n)$ ($r \in R$). Este homomorfismo tem obviamente $a_1 \cap \dots \cap a_n$ como núcleo e, portanto, induz um homomorfismo injetivo de $R/(a_1 \cap \dots \cap a_n)$ em $\mathfrak{R}$.

(6.7) COROLÁRIO. Com as notações do teorema (6.5), as condições (i) e (ii) são também equivalentes à condição

(iii) O homomorfismo $R \rightarrow R/a_1 \times \dots \times R/a_n$ acima indicado é sobrejetivo.

Neste caso, este homomorfismo induz um isomorfismo de

$$R/(a_1 \cap \dots \cap a_n) = R/(a_1 \cdot \dots \cdot a_n) \text{ sobre } R/a_1 \times \dots \times R/a_n.$$

Demonstração. A equivalência de (ii) e (iii) resulta do fato que $(r_1 + a_1, \dots, r_n + a_n) \in \mathfrak{R}$ será imagem, sob o homomorfismo $R \rightarrow \mathfrak{R}$, de um elemento $r \in R$ se e somente se $r \equiv r_j \pmod{a_j}$ para $j = 1, \dots, n$. $\square$

No caso particular em que $R = \mathbb{Z}$, concluímos de (6.7) que, para quaisquer números $m_1, \dots, m_n \in \mathbb{N}$, primos dois a dois, o anel quociente $\mathbb{Z}/(m_1 \cdot \dots \cdot m_n)\mathbb{Z}$ é isomorfo a $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}$.

Até agora, o problema de resolver simultaneamente um sistema de congruências módulo ideais $a_1, \dots, a_n$ foi considerado apenas sob a hipótese de $a_1, \dots, a_n$ serem comaximais dois a dois. Sem esta hipótese, a generalização de (6.4) a um número finito $n > 2$ de ideais está estreitamente ligada à questão da distributividade da adição dos ideais em relação à interseção, como será mostrado a seguir.

(6.8) Sejam $a_1, \dots, a_n$ ideais de R , onde $n \geq 2$, e suponhamos que, para quaisquer $r_1, \dots, r_n \in R$ tais que

$$r_i \equiv r_j \pmod{a_i + a_j} \quad (i, j = 1, \dots, n; i \neq j),$$

exista um $r \in R$ tal que $r \equiv r_j \pmod{a_j}$ ($j = 1, \dots, n$). Então vale

$$(a_1 \cap \dots \cap a_{n-1}) + a_n = (a_1 + a_n) \cap \dots \cap (a_{n-1} + a_n).$$

Demonstração. Devido a (c), basta provar a inclusão inversa $\supseteq$. Seja $s \in (a_1 + a_n) \cap \dots \cap (a_{n-1} + a_n)$. Para $r_1 = \dots = r_{n-1} = s$ e $r_n = 0$, temos que $r_i \equiv r_j \pmod{a_i + a_j}$ ($i, j = 1, \dots, n; i \neq j$); logo, por hipótese, existe um $r \in R$ tal que $r - s \in a_1 \cap \dots \cap a_{n-1}$ e $r \in a_n$; portanto $s = -(r - s) + r \in (a_1 \cap \dots \cap a_{n-1}) + a_n$. $\square$

Note-se que, na afirmação de (6.8), os ideais $a_1, \dots, a_n$ podem ser permutados, uma vez que a hipótese, feita em (6.8), é simétrica em $1, \dots, n$.

Mostremos agora que, por outro lado, a validade da igualdade indicada em (6.8) para todo $k = 2, \dots, n$ é suficiente para a resolubilidade de sistemas de congruências do tipo considerado. Mais precisamente:

(6.9) Sejam $a_1, \dots, a_n$ ideais de R , com $n \geq 2$, tais que

$$(a_1 \cap \dots \cap a_{k-1}) + a_k = (a_1 + a_k) \cap \dots \cap (a_{k-1} + a_k) \quad (k = 2, \dots, n).$$

Então, para quaisquer $r_1, \dots, r_n \in R$ tais que

$$r_i \equiv r_j \pmod{a_i + a_j} \quad (i, j = 1, \dots, n; i \neq j),$$

existe um $r \in R$ tal que $r \equiv r_i \pmod{a_i} \quad (i = 1, \dots, n)$.

Demonstração. Devido a (6.4) podemos supor, por indução, que a afirmação seja válida para $n-1$, onde $n > 2$. Dados $r_1, \dots, r_n \in R$ tais que $r_i \equiv r_j \pmod{a_i + a_j} \quad (i, j = 1, \dots, n; i \neq j)$, existe um $r' \in R$ tal que $r' \equiv r_j \pmod{a_j} \quad (j = 1, \dots, n-1)$; logo $r' - r_n = (r' - r_j) + (r_j - r_n) \in a_j + a_n \quad (j = 1, \dots, n-1)$, e $r' - r_n \in (a_1 \cap \dots \cap a_{n-1}) + a_n$, devido à hipótese. De (6.4) resulta a existência de um $r \in R$ tal que $r \equiv r' \pmod{a_1 \cap \dots \cap a_{n-1}}$ e $r \equiv r_n \pmod{a_n}$; portanto $r \equiv r_i \pmod{a_i} \quad (i = 1, \dots, n)$. $\square$

Note-se que a igualdade indicada em (6.9) é trivial para $k = 2$.

Diremos que o anel R satisfaz o *Teorema Chinês de Restos*⁽¹⁾ para n ideais quaisquer, ou seja, "satisfaz CRT(n)", se a afirmação de (6.9) for válida para quaisquer ideais $a_1, \dots, a_n$ de R . Este nome explica-se pelo fato de matemáticos chineses, entre os séculos IV e VII, já terem conseguido resolver sistemas de congruências deste tipo, para o anel $R = \mathbb{Z}$. De (6.8) e (6.9) resulta imediatamente:

(6.10) Para qualquer anel R , as seguintes condições são equivalentes:

- (i) R satisfaz CRT(n) para todo $n \geq 2$.
- (ii) R satisfaz CRT(3).
- (iii) A adição dos ideais de R é distributiva em relação à interseção (isto é, vale sempre a igualdade em (e)).

⁽¹⁾ Alguns autores (por exemplo Lang [20], p. 63) entendem pelo "Teorema Chinês de Restos" o teorema (6.5), que é mais fraco que a afirmação de (6.9) mas, em compensação, vale sem nenhuma hipótese de distributividade.

Veremos no §8 que todo domínio de Dedekind satisfaz a condição de distributividade (6.10) (iii) e, portanto, o Teorema Chinês de Restos para qualquer $n \geq 2$. Quanto à caracterização de domínios que satisfazem a condição (e) (respectivamente (d), (c), (b)) com a igualdade em lugar da inclusão, veja Gilmer [9], §25, e Larsen-McCarthy [22], Chapter VI, Exercise 18).

Terminaremos este parágrafo indicando um fato sobre produtos de ideais, que não está ligado ao Teorema Chinês de Restos.

(6.11) *Sejam $\alpha_1, \dots, \alpha_r$ ideais e $\mathfrak{p}$ um ideal primo do anel R . Se $\alpha_1 \cdot \dots \cdot \alpha_r \subseteq$ (respectivamente $=$) $\mathfrak{p}$ então $\alpha_j \subseteq$ (respectivamente $=$) $\mathfrak{p}$ para algum $j \in \{1, \dots, r\}$.*

Demonstração. Suponhamos que para todo $j = 1, \dots, r$ tenhamos que $\alpha_j \not\subseteq \mathfrak{p}$, digamos $a_j \in \alpha_j \setminus \mathfrak{p}$. Então $a_1 \cdot \dots \cdot a_r \in \alpha_1 \cdot \dots \cdot \alpha_r \setminus \mathfrak{p}$, logo $\alpha_1 \cdot \dots \cdot \alpha_r \not\subseteq \mathfrak{p}$. A afirmação com a igualdade resulta de $\alpha_1 \cdot \dots \cdot \alpha_r \subseteq \alpha_j$ ($j = 1, \dots, r$). $\square$

EXERCÍCIOS

- 6.1. Prove que, no caso de um domínio principal R , em (b), (c), (d) e (e) vale a igualdade, quaisquer que sejam os ideais α , $\mathfrak{b}$, $\mathfrak{b}'$ de R .
- 6.2. Dê exemplo de um domínio R e de ideais $\alpha_1, \alpha_2, \alpha_3$ de R para os quais não valha a igualdade em (b) (respectivamente (c), (d), (e)). Além disto, indique elementos $r_1, r_2, r_3 \in R$ tais que $r_i \equiv r_j \pmod{\alpha_i + \alpha_j}$, para $i, j = 1, 2, 3$, $i \neq j$, mas que não exista nenhum $r \in R$ com $r \equiv r_j \pmod{\alpha_j}$ ($j = 1, 2, 3$).
- 6.3. Seja R um anel e α um ideal de R . Prove:
 - a) $\sqrt{\alpha}$ é igual à interseção de todos os ideais primos de R que contêm α .
 - b) $\sqrt{\alpha} = \alpha$ se e somente se α for uma interseção de ideais primos de R .
- 6.4. Conclua da proposição (6.7) que, para quaisquer $m, n \in \mathbb{N}$ tais que $\text{MDC}(m, n) = 1$, o grupo $U(\mathbb{Z}/mn\mathbb{Z})$ é isomorfo ao produto cartesiano $U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})$. Mostre, através de um contra-exemplo, que a hipótese $\text{MDC}(m, n) = 1$ é indispensável.
- 6.5. Interprete o Teorema Chinês de Restos (6.9) em termos do homomorfismo $R \rightarrow R/\alpha_1 \times \dots \times R/\alpha_n$.

6.6. Resolva o seguinte sistema de congruências

$$X \equiv k \pmod{k+1} \quad (k = 1, 2, 3, 4).$$

6.7. Seja $\mathcal{U}$ um conjunto de ideais do anel R . Indique, para os ideais em $\mathcal{U}$, condições de distributividade equivalentes à resolubilidade de todo sistema de congruências

$$X \equiv r_j \pmod{\alpha_j} \quad (j = 1, \dots, n)$$

tal que $r_i \equiv r_j \pmod{\alpha_i + \alpha_j}$ ($i, j = 1, \dots, n$; $i \neq j$), sendo $\{\alpha_1, \dots, \alpha_n\}$ qualquer subconjunto finito de $\mathcal{U}$.

6.8. Sejam $m_1, \dots, m_n$ números naturais, primos dois a dois. Prove que, para quaisquer $r_1, \dots, r_n \in \mathbb{Z}$, o sistema de congruências $X \equiv r_j \pmod{m_j}$ ($j = 1, \dots, n$) tem como solução qualquer $r \in \mathbb{Z}$ tal que $r \equiv \sum_{i=1}^n r_i \cdot k_i \cdot k'_i \pmod{m_1 \cdot \dots \cdot m_n}$, onde $k_i = m_1 \cdot \dots \cdot m_{i-1} \cdot m_{i+1} \cdot \dots \cdot m_n$ e $k_i \cdot k'_i \equiv 1 \pmod{m_i}$ ($i = 1, \dots, n$).

§7. Anéis noetherianos e módulos noetherianos

O objetivo principal deste parágrafo é mostrar que, para qualquer corpo de números algébricos L , o domínio I_L , embora nem sempre principal, possui apenas ideais finitamente gerados.

Um anel R tal que todos os seus ideais sejam finitamente gerados é chamado *noetheriano*. Convém estender esta definição a R -módulos, para qualquer anel R : Um R -módulo M será chamado *noetheriano* se todos os seus submódulos forem finitamente gerados. Obviamente, um anel R será noetheriano se e somente se, considerado como R -módulo, for noetheriano.

Para que um anel R (respectivamente um R -módulo M) seja noetheriano, é necessário e suficiente que os seus ideais (respectivamente submódulos) satisfaçam uma das seguintes condições, as quais introduzimos num contexto mais abstrato.

Seja $\mathcal{C}$ um conjunto munido de uma ordem (parcial) $\leq$. Diremos que $\mathcal{C}$ satisfaz a *condição maximal* se todo subconjunto não vazio $\mathcal{B}$ de $\mathcal{C}$ possuir (pelo menos) um elemento maximal, isto é, um $b_0 \in \mathcal{B}$ tal que não exista nenhum $b \in \mathcal{B}$ com $b_0 < b$. Diremos que $\mathcal{C}$ satisfaz a *condição de cadeia ascendente* (C.C.A.) se, para toda sequência $(a_j)_{j \in \mathbb{N}}$ tal que $a_0 \leq a_1 \leq a_2 \leq \dots$, existir $n \in \mathbb{N}$ tal que $a_n = a_{n+1} = a_{n+2} = \dots$; ou seja, se toda cadeia ascendente $a_0 \leq a_1 \leq a_2 \leq \dots$ for estacionária.

(7.1) As seguintes condições são equivalentes:

- (i) $\mathcal{C}$ satisfaz a condição maximal.
- (ii) $\mathcal{C}$ satisfaz a condição de cadeia ascendente.

Demonstração. (i) $\Rightarrow$ (ii): Seja $a_0 \leq a_1 \leq a_2 \leq \dots$ uma cadeia ascendente em $\mathcal{C}$. Então $\{a_j \mid j \in \mathbb{N}\}$ possui um elemento maximal, digamos a_n ; portanto, em $a_n \leq a_{n+1} \leq a_{n+2} \leq \dots$ valem as igualdades.

(ii) $\Rightarrow$ (i). Suponhamos que $\mathcal{C}$ possua um subconjunto não-vazio $\mathcal{B}$ sem elemento maximal; então $\mathcal{B}_a = \{b \in \mathcal{B} \mid a < b\}$ não é vazio, qualquer que seja $a \in \mathcal{B}$. Pelo axioma de escolha existe uma aplicação $\chi: \{\mathcal{B}_a \mid a \in \mathcal{B}\} \rightarrow \mathcal{B}$ tal que $\chi(\mathcal{B}_a) \in \mathcal{B}_a$ para todo $a \in \mathcal{B}$. Partindo de algum $a_0 \in \mathcal{B}$, definimos por indução $a_j = \chi(\mathcal{B}_{a_{j-1}})$ ($j = 1, 2, 3, \dots$). Obviamente temos que $a_0 < a_1 < a_2 < \dots$, em contradição com a condição (ii). $\square$

Aplicaremos esta proposição ao conjunto dos submódulos de um R -módulo M e ao conjunto dos ideais de um anel R , sendo ambos os conjuntos (parcialmente) ordenados pela inclusão.

(7.2) TEOREMA. Sejam M um R -módulo e $\mathcal{M}$ o conjunto dos submódulos de M . As seguintes condições são equivalentes:

- (i) M é um R -módulo noetheriano.
- (ii) $\mathcal{M}$ satisfaz a condição de cadeia ascendente.
- (iii) $\mathcal{M}$ satisfaz a condição maximal.

Demonstração. (i) $\Rightarrow$ (ii): Seja $M_0 \subseteq M_1 \subseteq M_2 \subseteq \dots$ uma cadeia ascendente em $\mathcal{M}$, e seja $M' = \bigcup_{j \in \mathbb{N}} M_j$. Então $M' \in \mathcal{M}$ e, por hipótese, é finitamente gerado; digamos $M' = R \cdot x_1 + \dots + R \cdot x_m$. Existe $k \in \mathbb{N}$ tal que $x_1, \dots, x_m \in M_k$; portanto $M' \subseteq M_k \subseteq M_{k+1} \subseteq \dots \subseteq M'$, e valem mesmo as igualdades.

(ii) $\Rightarrow$ (iii) resulta de (7.1).

(iii) $\Rightarrow$ (i): Dado $N \in \mathcal{M}$, seja $\mathcal{F}_N$ o conjunto dos submódulos finitamente gerados de M que estão contidos em N . Como $\mathcal{F}_N$ não é vazio (pois $(0) \in \mathcal{F}_N$), ele possui um elemento maximal, N' . Afirmamos que $N \subseteq N'$. De fato, para qualquer $y \in N$ temos que $N' \subseteq N' + R \cdot y \in \mathcal{F}_N$, e vale a igualdade, pois N' é maximal em $\mathcal{F}_N$; portanto $y \in N'$. Concluímos que $N = N'$ é finitamente gerado. $\square$

No caso particular em que $M = R$ obtemos o seguinte

(7.3) COROLÁRIO. Sejam R um anel e $\mathcal{I}$ o conjunto dos ideais de R . As seguintes condições são equivalentes:

- (i) R é um anel noetheriano.
- (ii) $\mathcal{I}$ satisfaz a condição de cadeia ascendente.
- (iii) $\mathcal{I}$ satisfaz a condição maximal.

Do teorema (7.2) obtemos ainda o seguinte resultado sobre a existência de submódulos maximais em qualquer módulo noetheriano:

(7.4) COROLÁRIO. Sejam M e $\mathcal{M}$ como em (7.2). Se M for noetheriano, então todo $N \in \mathcal{M} \setminus \{M\}$ estará contido em algum elemento maximal N' do conjunto $\mathcal{M} \setminus \{M\}$.

Demonstração. O conjunto $\{N'' \in \mathcal{M} \mid N \subseteq N'' \subset M\}$ não é vazio e, portanto, possui um elemento maximal N' ; este é também um elemento maximal de $\mathcal{M} \setminus \{M\}$. $\square$

No caso em que $M = R$ concluímos deste corolário que todo ideal α de R , distinto de R , está contido num ideal maximal de R . Observamos que este fato vale mesmo sem a hipótese de R ser noetheriano (veja §0).

Utilizaremos a C.C.A. para demonstrar o seguinte:

(7.5) TEOREMA. Sejam M um R -módulo e N um submódulo de M . As seguintes condições são equivalentes:

- (i) M é um R -módulo noetheriano.
- (ii) N e M/N são R -módulos noetherianos.

Demonstração. Observemos primeiro que o homomorfismo canônico κ de M sobre M/N define uma correspondência biunívoca, que preserva a inclusão, entre os submódulos de M que contêm N e os submódulos de M/N .

(i) $\Rightarrow$ (ii): Toda cadeia ascendente de submódulos de N (respectivamente de M/N) é igual (respectivamente corresponde, através da correspondência acima indicada,) a uma cadeia ascendente e, por hipótese, estacionária de submódulos de M ; portanto, é estacionária.

(ii) $\Rightarrow$ (i): Seja $M_0 \subseteq M_1 \subseteq \dots$ uma cadeia ascendente de submódulos de M . Então $M_0 \cap N \subseteq M_1 \cap N \subseteq \dots$ (respectivamente $\kappa M_0 \subseteq \kappa M_1 \subseteq \dots$) é uma cadeia ascendente de submódulos de N (respectivamente M/N).

Por hipótese existe $n \in \mathbb{N}$ tal que $M_k \cap N = M_{k+1} \cap N$ e $\kappa M_k = \kappa M_{k+1}$ para todo $k \geq n$. Afirmamos que $M_{k+1} \subseteq M_k$. De fato, para qualquer $x \in M_{k+1}$ existe $y \in M_k$ tal que $x + N = y + N$; logo $x - y \in M_{k+1} \cap N = M_k \cap N$, e assim $x \in M_k$. Concluimos que $M_k = M_{k+1}$ para todo $k \geq n$, isto é, a cadeia $M_0 \subseteq M_1 \subseteq \dots$ é estacionária. $\square$

Do teorema (7.5) obtemos dois importantes corolários.

(7.6) COROLÁRIO. *Sejam $M_1, \dots, M_n$ R -módulos noetherianos. Então $M_1 \times \dots \times M_n$ é um R -módulo noetheriano.*

Demonstração. Sendo trivial para $n = 1$, podemos supor que a afirmação valha para $n - 1$, sendo $n \geq 2$. O submódulo

$$N = (0) \times \dots \times (0) \times M_n \text{ de } M_1 \times \dots \times M_n$$

e o módulo quociente $(M_1 \times \dots \times M_n)/N$ são noetherianos, pois são isomorfos a M_n e a $M_1 \times \dots \times M_{n-1}$, respectivamente. De (7.5) concluimos que $M_1 \times \dots \times M_n$ é noetheriano. $\square$

De (7.6) concluimos em particular que, para qualquer anel noetheriano R , o R -módulo $\underbrace{R \times \dots \times R}_n$ é noetheriano. Mais geralmente provamos:

(7.7) COROLÁRIO. *Seja R um anel noetheriano. Então todo R -módulo finitamente gerado é noetheriano.*

Demonstração. Se $M = R \cdot x_1 + \dots + R \cdot x_m$, seja N o núcleo do homomorfismo de $\underbrace{R \times \dots \times R}_m$ sobre M definido por

$$(a_1, \dots, a_m) \mapsto a_1 \cdot x_1 + \dots + a_m \cdot x_m \quad (a_1, \dots, a_m \in R);$$

então M é isomorfo a $\underbrace{(R \times \dots \times R)}_m / N$. Por (7.6) e (7.5), M é noetheriano. $\square$

Este corolário afirma que se R for um anel noetheriano, então todo submódulo de qualquer R -módulo finitamente gerado será finitamente gerado. Deve-se observar que isto não será verdade quando R não for noetheriano; de fato, neste caso o próprio R , considerado como R -módulo, possui submódulos (isto é, ideais) não finitamente gerados.

A propriedade de um anel R ser noetheriano tem várias consequências importantes em relação aos seus ideais. Demonstraremos aqui apenas um teorema que afirma que todo ideal $\mathfrak{a}$ de R contém um produto finito de ideais primos e está contido na interseção deles.

(7.8) TEOREMA. *Seja R um anel noetheriano. Para todo ideal $\mathfrak{a}$ de R existem $n \in \mathbb{N}$ e ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ de R tais que $\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_n \subseteq \mathfrak{a} \subseteq \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$.*

Demonstração. Suponhamos que o conjunto $\mathscr{U}$ dos ideais $\mathfrak{a}$ de R que não têm a propriedade indicada, não seja vazio; pela condição maximal, $\mathscr{U}$ possui um elemento maximal, $\mathfrak{b}$. Obviamente, $\mathfrak{b}$ não é um ideal primo e $\mathfrak{b} \neq R$; portanto existem $x, y \in R \setminus \mathfrak{b}$ tais que $x \cdot y \in \mathfrak{b}$. Como $\mathfrak{b} \subset \mathfrak{b} + R \cdot x$ e $\mathfrak{b} \subset \mathfrak{b} + R \cdot y$, resulta da maximalidade de $\mathfrak{b}$ em $\mathscr{U}$ que existem ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ de R tais que

$$\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r \subseteq \mathfrak{b} + R \cdot x \subseteq \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r, \text{ e}$$

$$\mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_s \subseteq \mathfrak{b} + R \cdot y \subseteq \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s.$$

Concluimos que

$$\begin{aligned} \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r \cdot \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_s &\subseteq (\mathfrak{b} + R \cdot x) \cdot (\mathfrak{b} + R \cdot y) \subseteq \mathfrak{b} \subseteq \\ &\subseteq \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r \cap \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s, \end{aligned}$$

em contradição com $\mathfrak{b} \in \mathscr{U}$. Portanto, $\mathscr{U}$ é vazio. $\square$

(7.9) COROLÁRIO. *Seja R um anel noetheriano. Então todo ideal não-nulo $\mathfrak{a}$ de R contém o produto de um número finito de ideais primos não-nulos.*

Demonstração. Seja $\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_n \subseteq \mathfrak{a} \subseteq \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$ como em (7.8). De $\mathfrak{a} \neq (0)$ resulta que $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ são não-nulos. $\square$

Outros fatos referentes aos ideais em anéis noetherianos encontram-se em alguns dos exercícios deste parágrafo.

Num domínio noetheriano R , embora este não sendo necessariamente fatorial, todo elemento não-nulo possui uma fatoração em elementos irredutíveis; ou seja, a aplicação $f: U(R) \times \mathbb{N}^{(\mathscr{P})} \rightarrow R \setminus \{0\}$ (definida em §0, B) é sobrejetiva. Isto será mostrado a seguir, de uma maneira semelhante à demonstração do teorema (7.8).

(7.10) TEOREMA. *Seja R um domínio noetheriano e seja $\mathcal{P}$ um sistema de representantes dos elementos irredutíveis de R . Então, para todo elemento não-nulo $r \in R$, existem $n \in \mathbb{N}$, $z_1, \dots, z_n \in \mathcal{P}$ e $u \in U(R)$ tais que $r = u \cdot z_1 \cdot \dots \cdot z_n$.*

Demonstração. Suponhamos que exista em R um elemento não-nulo, r , que não tenha a propriedade indicada. Então, o conjunto $\mathcal{U}$ dos ideais principais $r \cdot R$, gerados por tais elementos, não é vazio e, pela condição maximal, possui um elemento maximal, $s \cdot R$. Obviamente, s não é irredutível e $s \notin U(R)$; portanto, existem $x, y \in R \setminus U(R)$ tais que $s = x \cdot y$. Como, $s \cdot R \subset x \cdot R$ e $s \cdot R \subset y \cdot R$, resulta da maximalidade de $s \cdot R$ que x e y têm a propriedade indicada; portanto $s = x \cdot y$ também a tem, em contradição com $s \cdot R \in \mathcal{U}$. $\square$

Finalmente, utilizaremos os resultados acima para mostrar que, para todo corpo de números algébricos L , o anel I_L é noetheriano. Mais precisamente, trataremos da seguinte situação mais geral: Em lugar da extensão $L | \mathbb{Q}$ consideramos uma extensão separável finita $L | Q(R)$, onde R é qualquer domínio noetheriano e integralmente fechado; além disto, consideraremos não somente o anel $I_L(R)$, mas também seus subanéis. O seguinte teorema pode ser considerado uma generalização parcial de (5.4).

(7.11) TEOREMA. *Sejam R um domínio noetheriano e integralmente fechado e L uma extensão separável de $K = Q(R)$, de grau n . Para qualquer subanel S de L que contém R , as seguintes condições são equivalentes:*

- (i) S é um R -módulo finitamente gerado.
- (ii) $S \subseteq I_L(R)$.

Neste caso, S é noetheriano como anel e como R -módulo.

Demonstração. (i) $\Rightarrow$ (ii) resulta de (1.3). (ii) $\Rightarrow$ (i): Por (4.7), S é submódulo de um R -módulo livre, M , de posto n . Como R é noetheriano e o R -módulo M é finitamente gerado, resulta de (7.7) que S é um R -módulo finitamente gerado e mesmo noetheriano. Todo ideal de S é um submódulo do R -módulo S ; logo toda cadeia ascendente de ideais de S é estacionária; portanto, S é um anel noetheriano. $\square$

Restringindo-nos ao caso de um corpo de números algébricos L e $R = \mathbb{Z}$, obtemos novamente o resultado (já provado no §5) que os subanéis S de L que são $\mathbb{Z}$ -módulos finitamente gerados coincidem com os subanéis de I_L . Da última afirmação de (7.11) obtemos o seguinte

(7.12) COROLÁRIO. *Seja L um corpo de números algébricos. Todo subanel de I_L é noetheriano como anel e como $\mathbb{Z}$ -módulo.*

Note-se que do teorema (7.11) resulta, em particular, que a propriedade de um domínio integralmente fechado ser noetheriano é preservada na passagem de $K = Q(R)$ a qualquer extensão separável finita L ; isto é, $I_L(R)$ também é noetheriano. Lembramos que o mesmo não vale para a propriedade de ser um domínio principal (veja (2.4)).

EXERCÍCIOS

- 7.1. Seja R um anel noetheriano. Prove que, para todo ideal α de R , existe $n \geq 1$ tal que $(\sqrt{\alpha})^n \subseteq \alpha$.
- 7.2. Seja M um R -módulo noetheriano. Prove que todo homomorfismo $\lambda: M \rightarrow M$ sobrejetivo é um automorfismo de M . (Sugestão: Considere o núcleo dos homomorfismos $\lambda, \lambda \circ \lambda, \lambda \circ \lambda \circ \lambda, \dots$).
- 7.3. Um anel R será chamado *artiniano* se o conjunto $\mathcal{I}$ dos seus ideais satisfizer a condição de cadeia *descendente* (C.C.D.) ou, equivalentemente, a condição *minimal*. (Estas condições obtêm-se da C.C.A. e da condição maximal, respectivamente, invertendo a ordem). Prove:
 - a) Todo corpo K , bem como o anel $\mathbb{Z}/n\mathbb{Z}$ para qualquer $n \geq 1$, é um anel noetheriano e artiniano.
 - b) $\mathbb{Z}$ não é artiniano.

Observação: Mostra-se que um anel R será artiniano se e somente se for noetheriano e todo ideal primo de R for um ideal maximal (veja Atiyah-Macdonald [3], Chapter 8).

- 7.4. Prove que toda imagem homomorfa de um anel noetheriano (respectivamente artiniano) é noetheriano (respectivamente artiniano).
- 7.5. Seja R um anel não-noetheriano e seja $\mathcal{U}$ o conjunto dos ideais não finitamente gerados de R .
 - a) Prove que $\mathcal{U}$ possui elementos maximais.
 - b) Prove que todo elemento maximal de $\mathcal{U}$ é um ideal primo de R .
 - c) Conclua que todo anel cujos ideais primos forem finitamente gerados será um anel noetheriano.
- 7.6. Indique um domínio R tal que nem todo elemento não-nulo $r \in R \setminus U(R)$ seja um produto de elementos irredutíveis de R .

7.7. Seja R um anel. Um ideal i de R será chamado *irredutível* se, para quaisquer ideais a, b de R , a igualdade $i = a \cap b$ implicar $i = a$ ou $i = b$.

- Prove que todo ideal primo é irredutível.
- Prove que se R for noetheriano então todo ideal de R será igual à interseção de um número finito de ideais irredutíveis.
- Determine todos os ideais irredutíveis de $\mathbb{Z}$.

Os seguintes exercícios podem ser considerados como sugestões para aprofundar os conhecimentos sobre anéis noetherianos.

7.8. (Teorema de base de Hilbert). Se R for anel noetheriano então o anel de polinômios $R[X]$ será noetheriano. (Veja Atiyah-Macdonald [3], Theorem 7.5).

7.9. (Teorema de interseção de Krull). Sejam R um anel noetheriano e a um ideal de R . Teremos que $\bigcap_{n \in \mathbb{N}} a^n = (0)$ se e somente se, para todo $a \in a$, o elemento $1 - a$ não for divisor de zero em R . Isto ocorrerá, em particular, quando R for um domínio e $a \neq R$. (Veja Zariski-Samuel [38], Chapter IV, §7, Theorem 12).

7.10. (Decomposição primária). Um ideal q de R será chamado *primário* se $q \neq R$ e, para quaisquer $r, s \in R$, de $r \cdot s \in q$ decorrer que $r \in q$ ou $s \in \sqrt{q}$. Prove:

- $\sqrt{q}$ é o menor ideal primo que contém q .
- Todo ideal a tal que $\sqrt{a}$ seja um ideal maximal é primário.
- Se $a = q_1 \cap \dots \cap q_n$ for uma decomposição primária *minimal* do ideal a (isto é, se $q_1, \dots, q_n$ forem ideais primários tais que $q_1 \cap \dots \cap q_{j-1} \cap q_{j+1} \cap \dots \cap q_n \not\subseteq q_j$ para todo $j = 1, \dots, n$ e $\sqrt{q_1}, \dots, \sqrt{q_n}$ forem distintos), então n e $\{\sqrt{q_1}, \dots, \sqrt{q_n}\}$ independem da decomposição escolhida.
- Se R for noetheriano então todo ideal irredutível de R será primário e todo ideal de R possuirá uma decomposição primária minimal. (Veja Atiyah-Macdonald [3], §4 e §7).

§8. Domínios de Dedekind

Um domínio R será chamado *domínio de Dedekind* se for integralmente fechado e noetheriano, e todo ideal primo não-nulo for maximal.

Obviamente todo corpo e todo domínio principal é de Dedekind. O anel de polinômios $\mathbb{Q}[X, Y]$ é um exemplo de um domínio fatorial

que não é de Dedekind; de fato, o ideal gerado por X é primo mas não é maximal.

Demonstraremos primeiro que a propriedade de um domínio R ser de Dedekind é preservada na passagem de $K = Q(R)$ a qualquer extensão separável finita L ; mais precisamente:

(8.1) **TEOREMA.** *Sejam R um domínio de Dedekind e L uma extensão finita e separável de $K = Q(R)$. Então $I_L(R)$ é um domínio de Dedekind.*

Demonstração. De (1.7) e (1.5) concluímos que $Q(I_L(R)) = L$ e que $I_L(R)$ é integralmente fechado. De (7.11) resulta que $I_L(R)$ é noetheriano, e de (1.13) resulta que todo ideal primo não-nulo de $I_L(R)$ é um ideal maximal. $\square$

No caso em que $R = \mathbb{Z}$ resulta imediatamente:

(8.2) **COROLÁRIO.** *Seja L um corpo de números algébricos. Então I_L é um domínio de Dedekind.*

O nosso objetivo é provar, em domínios de Dedekind R , a existência e a unicidade da fatoração de ideais não-nulos em ideais primos, já que a fatoração de elementos de $R \setminus \{0\}$ em elementos irredutíveis, embora sempre exista (veja (7.10)), nem sempre é única. Da mesma maneira que a fatoração em elementos irredutíveis é estendida aos elementos não-nulos do corpo $Q(R)$, admitindo-se potências negativas dos elementos irredutíveis, convém estender a fatoração em ideais primos aos ideais fracionários de R , que serão introduzidos a seguir.

Sejam R um domínio e $K = Q(R)$ o seu corpo de frações, e consideremos os submódulos do R -módulo K . É óbvio que as operações “interseção”, “soma” e “produto”, definidas no §6 para os ideais de R , estendem-se aos submódulos de K , continuando válidas as leis da associatividade e comutatividade bem como as propriedades (a)-(e). Além disto, definimos para qualquer submódulo M de K , o quociente $(R : M) = \{x \in K \mid x \cdot M \subseteq R\}$; ele é obviamente um submódulo de K e satisfaz:

- (8.3) a) $(R : M) \cdot M \subseteq R$ para qualquer submódulo M de K .
b) $R \subseteq (R : a)$ para qualquer ideal a de R .

Um submódulo M de K será chamado um *ideal fracionário* de R se existir $d \in R \setminus \{0\}$ tal que $d \cdot M \subseteq R$; neste caso, $d \cdot M$ é um ideal a de R

e $M = d^{-1} \cdot a$. Os ideais de R são exatamente os ideais fracionários que estão contidos em R . É óbvio que todo submódulo finitamente gerado de K é um ideal fracionário e que, por outro lado, num domínio noetheriano todo ideal fracionário é finitamente gerado. Verifica-se facilmente que a interseção, a soma e o produto de dois ideais fracionários é um ideal fracionário. Quanto ao quociente, é óbvio que $(R : (0)) = K$, e mostramos o seguinte:

(8.4) *Seja M um submódulo de K . Então:*

- a) *Se M for não-nulo então $(R : M)$ será um ideal fracionário de R .*
- b) *Se M for um ideal fracionário de R então $(R : M) \neq (0)$.*
- c) *Se $R \neq K$ então $(R : K) = (0)$, e K não é um ideal fracionário de R .*

Demonstração. a) Existem $c, d \in R \setminus \{0\}$ tais que $c^{-1} \cdot d \in M$, logo $0 \neq d \in M \cap R$. Por (8.3a), temos que $d \cdot (R : M) \subseteq R$; portanto, $(R : M)$ é um ideal fracionário de R .

b) Existe $d \in R \setminus \{0\}$ tal que $d \cdot M \subseteq R$; portanto $d \in (R : M)$.

c) Suponhamos que $(R : K) \neq (0)$, digamos $c^{-1} \cdot d \in (R : K)$, onde $c, d \in R \setminus \{0\}$. Temos que $d \in (R : K)$, logo $d^{-1} = d \cdot d^{-2} \in d \cdot K \subseteq R$, e assim $1 = d^{-1} \cdot d \in (R : K)$; portanto $K \subseteq R$, o que prova a primeira afirmação. Desta e de b) resulta a segunda afirmação. $\square$

Denotamos por $\mathcal{M}$ (respectivamente $\mathcal{F}$) o conjunto dos submódulos de K (respectivamente o conjunto dos ideais fracionários de R) não-nulos, munido da multiplicação. Obviamente $\mathcal{M}$ é um monóide (isto é, um semi-grupo com unidade) comutativo, e $\mathcal{F}$ é um submonóide de $\mathcal{M}$; ambos têm R como única unidade.

Diremos que $M \in \mathcal{M}$ é *invertível* se existir $N \in \mathcal{M}$ tal que $N \cdot M = R$. Neste caso, o inverso N de M é univocamente determinado, como mostraremos a seguir, e será denotado por M^{-1} .

(8.5) *Seja $M \in \mathcal{M}$ invertível. Então M é um R -módulo finitamente gerado, $(R : M)$ é o único inverso M^{-1} de M , e M, M^{-1} são ideais fracionários. Além disto, $x \cdot M^{-1}$ é um ideal de R para qualquer $x \in M$.*

Demonstração. De $N \cdot M = R$ decorre que $N \subseteq (R : M)$. Por outro lado, de (8.3a) resulta que $(R : M) = (R : M) \cdot M \cdot N \subseteq R \cdot N \subseteq N$; portanto $N = (R : M)$. Existem $y_1, \dots, y_m \in (R : M)$ e $z_1, \dots, z_m \in M$ tais que $1 = y_1 \cdot z_1 + \dots + y_m \cdot z_m$. Multiplicando esta igualdade por qualquer $x \in M$, obtemos que $x \in R \cdot z_1 + \dots + R \cdot z_m$; logo M é finitamente gerado e, por-

tanto, é um ideal fracionário. Por (8.4), $M^{-1} = (R : M)$ também o é. De $x \in M$ decorre que $x \cdot M^{-1} \subseteq M \cdot M^{-1} = R$; logo $x \cdot M^{-1}$ é um ideal de R . $\square$

A proposição (8.5) mostra que submódulos invertíveis de K são necessariamente ideais fracionários. Observemos ainda que se um ideal não-nulo $\mathfrak{a}$ for invertível, então o inverso $\mathfrak{a}^{-1} = (R : \mathfrak{a})$ não será em geral um ideal, mas apenas um ideal fracionário (veja (8.3b), (8.6) e Exercício 8.9).

Denotamos por $\mathcal{G}$ o conjunto dos ideais fracionários invertíveis. Obviamente, $\mathcal{G}$, munido da multiplicação, é o maior grupo contido no monóide $\mathcal{F}$ (e também no monóide $\mathcal{M}$). Em particular, para todo elemento não-nulo $x \in K$, temos que $R \cdot x \in \mathcal{G}$ e $(R \cdot x)^{-1} = R \cdot x^{-1}$; estes ideais fracionários principais não-nulos formam um subgrupo $\mathcal{H}$ de $\mathcal{G}$.

É claro que $\mathcal{F}$ será um grupo se e somente se $\mathcal{G} = \mathcal{F}$, se e somente se todo $M \in \mathcal{F}$ for invertível. Veremos em (8.9) que isto ocorrerá se e somente se R for um domínio de Dedekind.

Denotamos por $\mathcal{P}$ o conjunto dos ideais primos não-nulos de R . Recordemos que $\mathcal{P}$ contém, e no caso de um domínio de Dedekind coincide com, o conjunto dos ideais maximais de R (exceto no caso trivial $R = K$, no qual $\mathcal{P}$ é vazio e (0) é o único ideal maximal de R).

Sob certas hipóteses, a inclusão indicada em (8.3b) pode ser reforçada para ideais primos:

(8.6) *Seja R um domínio noetheriano tal que todo $\mathfrak{p} \in \mathcal{P}$ seja um ideal maximal. Então $R \subset (R : \mathfrak{p})$ para qualquer $\mathfrak{p} \in \mathcal{P}$.*

Demonstração. Escolhamos $d \in \mathfrak{p} \setminus \{0\}$. Por (7.9) existem $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathcal{P}$ tais que $\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r \subseteq R \cdot d \subseteq \mathfrak{p}$, e podemos supor que o número de fatores neste produto seja minimal. Por (6.11), $\mathfrak{p}$ contém um dos ideais $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, digamos $\mathfrak{p}_1$, e como $\mathfrak{p}_1$ é um ideal maximal, temos que $\mathfrak{p} = \mathfrak{p}_1$. Como $\mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_r \not\subseteq R \cdot d$, existe $c \in \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_r$ tal que $c \cdot d^{-1} \notin R$. Por outro lado, temos que $c \cdot \mathfrak{p} \subseteq \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r \subseteq R \cdot d$; logo $c \cdot d^{-1} \in (R : \mathfrak{p})$. $\square$

Denotando por $\mathcal{J}$ o conjunto de todos os ideais não-nulos de R , provaremos:

(8.7) Seja R um domínio de Dedekind. Então:

- a) Todo $p \in \mathcal{P}$ é invertível.
- b) Para todo $a \in \mathcal{J}$ existem $n \in \mathbb{N}$ e $p_1, \dots, p_n \in \mathcal{P}$ tais que $a = p_1 \cdot \dots \cdot p_n$.
- c) Todo $a \in \mathcal{P}$ é invertível.
- d) Todo $M \in \mathcal{F}$ é invertível.

Demonstração. a) Como $p \in \mathcal{P}$ é um ideal maximal de R e $p \subseteq (R : p) \cdot p \subseteq R$ por (8.3a), basta provar que $p \neq (R : p) \cdot p$. Suponhamos que $p = (R : p) \cdot p$ e escolhamos $d \in p \setminus \{0\}$. Seja $x \in (R : p)$; então $x \cdot p \subseteq p$; logo $x^m \cdot p \subseteq x^{m-1} \cdot p \subseteq \dots \subseteq x \cdot p \subseteq p \subseteq R$ para todo $m \in \mathbb{N}$; portanto $R[x] \cdot d \subseteq R$; isto é, $R[x]$ é um ideal fracionário de R . Como R é noetheriano, $R[x]$ é um R -módulo finitamente gerado, e de (1.1) concluímos que $x \in I_x(R) = R$. Resulta que $(R : p) \subseteq R$, o que é uma contradição com (8.6).

b) Para todo $m \in \mathbb{N}$, seja $\mathcal{J}_m$ o conjunto dos ideais não-nulos de R que contêm um produto de m elementos de $\mathcal{P}$; então $\mathcal{J}_0 = \{R\} \subseteq \mathcal{J}_1 \subseteq \mathcal{J}_2 \subseteq \dots$, e $\bigcup_{n \in \mathbb{N}} \mathcal{J}_n = \mathcal{J}$, devido a (7.9). Sendo a afirmação b) trivial para R , supomos-la válida para todo ideal não-nulo em $\mathcal{J}_{r-1}$, onde $r \geq 1$. Seja $a \in \mathcal{J}_r \setminus \{R\}$; digamos $p_1 \cdot \dots \cdot p_r \subseteq a$, onde $p_1, \dots, p_r \in \mathcal{P}$. Por (7.4), a está contido em algum $m \in \mathcal{P}$, e de (6.11) resulta que m contém um dos $p_1, \dots, p_r$, digamos $m \supseteq p_1$; temos até $m = p_1$, pois p_1 é um ideal maximal. Como m é invertível por a), temos que $p_2 \cdot \dots \cdot p_r \subseteq m^{-1} \cdot a \subseteq m^{-1} \cdot m \subseteq R$, logo $m^{-1} \cdot a \in \mathcal{J}_{r-1}$. Por hipótese existem $p'_1, \dots, p'_n \in \mathcal{P}$ tais que $m^{-1} \cdot a = p'_1 \cdot \dots \cdot p'_n$; logo $a = m \cdot p'_1 \cdot \dots \cdot p'_n$.

c) resulta imediatamente de a) e b).

d) Seja $M \in \mathcal{F}$, digamos $M = d^{-1} \cdot a$, onde $d \in R \setminus \{0\}$ e $a \in \mathcal{J}$. Como a e $R \cdot d$ são invertíveis, por c), M também o é. $\square$

Note-se que os $p_1, \dots, p_n \in \mathcal{P}$ indicados em (8.7b) não são necessariamente distintos. Juntando os iguais, obtemos uma fatoração $a = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$, com $k_1, \dots, k_r \in \mathbb{N} \setminus \{0\}$, onde $p_1, \dots, p_r$ são distintos dois a dois. As vezes convém escrever esta fatoração como produto formalmente infinito. Para isto, seja $\mathcal{P} = \{p_i \mid i \in I\}$, com os p_i distintos dois a dois, e denotamos por $\mathbb{N}^{(I)}$ (respectivamente $\mathbb{Z}^{(I)}$) o conjunto das famílias $(k_i)_{i \in I}$, com $k_i \in \mathbb{N}$ (respectivamente $\in \mathbb{Z}$) tais que $k_i = 0$ para quase todos os $i \in I$. A propriedade (8.7b) significa então que a aplicação $\mathbb{N}^{(I)} \rightarrow \mathcal{J}$, definida por $(k_i)_{i \in I} \mapsto \prod_{i \in I} p_i^{k_i}$, é sobrejetiva. Mostraremos a seguir que ela é mesmo bijetiva, ou seja, que a fatoração dos ideais $a \in \mathcal{J}$ é a única, e que esta fatoração única se estende aos ideais fracionários de R .

(8.8) TEOREMA. *Seja R um domínio de Dedekind. Então:*

- a) *Para todo $a \in \mathcal{F}$ existe $(k_i)_{i \in I} \in \mathbb{N}^{(I)}$, univocamente determinada, tal que*

$$a = \prod_{i \in I} p_i^{k_i}.$$
b) Para todo $M \in \mathcal{F}$ existe $(m_i)_{i \in I} \in \mathbb{Z}^{(I)}$, univocamente determinada, tal que

$$M = \prod_{i \in I} p_i^{m_i}.$$

Demonstração. a) A existência resulta de (8.7b). A unicidade será uma consequência da unicidade afirmada em b).

b) Seja $M \in \mathcal{F}$, digamos $M = d^{-1} \cdot a$, onde $a \in \mathcal{F}$ e $d \in R \setminus \{0\}$. Por a), temos que $a = \prod_{i \in I} p_i^{k_i}$ e $R \cdot d = \prod_{i \in I} p_i^{h_i}$, com $(k_i)_{i \in I}, (h_i)_{i \in I} \in \mathbb{N}^{(I)}$; portanto, $M = \prod_{i \in I} p_i^{k_i - h_i}$. Para mostrar a unicidade da fatoração de M , supomos que $M = \prod_{i \in I'} p_i^{m_i} = \prod_{i \in I''} p_i^{n_i}$; portanto $R = M \cdot M^{-1} = \prod_{i \in I'} p_i^{m_i - n_i}$, logo $\prod_{i \in I'} p_i^{m_i - n_i} = \prod_{i \in I''} p_i^{n_i - m_i}$, onde I' (respectivamente I'') é o conjunto dos $i \in I$ tais que $m_i >$ (respectivamente $<$) n_i . Se $I' \neq \emptyset$, então este produto estará contido em $p_{i'} R$ para algum $i' \in I'$; portanto $I'' \neq \emptyset$ e $p_{i'} \supseteq p_{i''}$ para algum $i'' \in I''$, por (6.11), o que é absurdo. Se $I'' \neq \emptyset$, obteremos uma contradição de maneira análoga. Resulta que $I' = I'' = \emptyset$, o que prova a unicidade afirmada. $\square$

Mencionamos sem demonstração que cada uma das condições a) e b) do teorema (8.8) é não apenas necessária mas também suficiente para o domínio R ser de Dedekind. Na verdade, para isto basta mesmo a existência da fatoração, podendo a unicidade ser obtida como consequência (veja Ribenboim [28], Chapter 7).

Mostraremos a seguir que os domínios de Dedekind podem ser caracterizados pela propriedade de todo ideal fracionário não-nulo ser invertível, ou seja, pela igualdade $\mathcal{F} = \mathcal{G}$. Mostraremos também que $\mathcal{G}$ é um grupo abeliano livre, com base (não necessariamente finita) $\mathcal{P}$. Para isto, observamos que $\mathbb{Z}^{(I)}$, munido da adição componente a componente, é um $\mathbb{Z}$ -módulo (ou, seja, um grupo abeliano) livre, tendo como base canônica o conjunto $\mathcal{E} = \{e_i \mid i \in I\}$, onde $e_i = (\delta_{i,j})_{j \in I}$.

(8.9) TEOREMA. *Para qualquer domínio R as seguintes condições são equivalentes:*

- (i) *R é um domínio de Dedekind.*
 (ii) *Todo $M \in \mathcal{F}$ é invertível.*

Neste caso, $\mathcal{F} = \mathcal{G}$ é um grupo abeliano, e a aplicação $\mathbb{Z}^{(I)} \rightarrow \mathcal{F}$, definida por $(m_i)_{i \in I} \mapsto \prod_{i \in I} p_i^{m_i}$, é um isomorfismo do grupo $\mathbb{Z}^{(I)}$ sobre o grupo $\mathcal{F}$, que aplica $\mathcal{E}$ sobre $\mathcal{P}$.

Demonstração. (i) $\Rightarrow$ (ii) já foi demonstrado em (8.7d).

(ii) $\Rightarrow$ (i): Todo ideal não-nulo de R é finitamente gerado, por (8.5); portanto R é noetheriano.

Seja $x \in I_K(R)$; então $R[x]$ é finitamente gerado por (1.1), logo é um ideal fracionário M de R . Obviamente $M \cdot M = M$, e como M é invertível, temos que $x \in M = R$. Portanto, R é integralmente fechado.

Dado $p \in \mathcal{P}$, seja α um ideal de R tal que $p \subset \alpha$; digamos que $a \in \alpha \setminus p$. De (8.3b) resulta $p = R \cdot p \subseteq \alpha^{-1} \cdot p \subseteq \alpha^{-1} \cdot \alpha = R$. Por outro lado, se $r \in \alpha^{-1} \cdot p$ então $a \cdot r \in \alpha \cdot \alpha^{-1} \cdot p = p$, logo $r \in p$; portanto $p = \alpha^{-1} \cdot p$, logo $\alpha = R$. Resulta que p é um ideal maximal de R . Concluimos que R é um domínio de Dedekind.

A igualdade $\mathcal{F} = \mathcal{G}$ resulta da definição de $\mathcal{G}$. De (8.8b) concluímos que a aplicação $\mathbb{Z}^{(I)} \rightarrow \mathcal{F}$ é bijetiva; ela é obviamente um isomorfismo que aplica $\mathcal{E}$ sobre $\mathcal{P}$. $\square$

Recordemos que, no conjunto $\mathcal{F}$ dos ideais fracionários não-nulos de um domínio R , a inclusão é uma ordem parcial e a soma (respectivamente a interseção) é o supremo (respectivamente ínfimo) em relação à inclusão. O fato de $\mathcal{F}$ possuir um submonóide distinguido, a saber o monóide $\mathcal{J}$ de todos os ideais não-nulos, sugere a introdução em $\mathcal{F}$ de uma divisibilidade, a ser definida da seguinte maneira: Sejam $M, N \in \mathcal{F}$. Diremos que M divide N (em símbolos: $M \mid N$) ou que N é um múltiplo de M , se $N = \alpha \cdot M$ para algum $\alpha \in \mathcal{J}$. Obviamente, $M \mid N$ implica $M \supseteq N$; portanto a divisibilidade em $\mathcal{F}$ é uma ordem parcial⁽¹⁾. A implicação inversa será válida quando M for invertível, como se vê na demonstração do seguinte

(8.10) COROLÁRIO. *Seja R um domínio de Dedekind, e sejam*

$$M = p_1^{g_1} \cdot \dots \cdot p_r^{g_r}, \quad N = p_1^{h_1} \cdot \dots \cdot p_r^{h_r} \in \mathcal{F}$$

(onde $g_1, \dots, g_r, h_1, \dots, h_r \in \mathbb{Z}$). Então

$$a) \quad M \supseteq N \Leftrightarrow M \mid N \Leftrightarrow [g_1 \leq h_1, \dots, g_r \leq h_r].$$

⁽¹⁾ Note que a divisibilidade num corpo K , definida através de um subanel R , é apenas uma quase-ordem parcial, pois $x \mid y$ e $y \mid x$ implica apenas $x \sim y$, ou seja $x \cdot y^{-1} \in U(R)$.

- b) $M + N = \text{MDC}(M, N) = p_1^{m_1} \cdot \dots \cdot p_r^{m_r}$, sendo $m_j = \min \{g_j, h_j\}$
 $(j = 1, \dots, r)$.
 c) $M \cap N = \text{MMC}(M, N) = p_1^{n_1} \cdot \dots \cdot p_r^{n_r}$, sendo $n_j = \max \{g_j, h_j\}$
 $(j = 1, \dots, r)$.
 d) $M \cdot N = p_1^{g_1+h_1} \cdot \dots \cdot p_r^{g_r+h_r}$.

Demonstração. a) De $M \supseteq N$ decorre $R = M \cdot M^{-1} \supseteq N \cdot M^{-1}$, uma vez que M é invertível. Portanto $N \cdot M^{-1}$ é um ideal $\alpha \in \mathcal{J}$, logo $N = \alpha \cdot M$, e assim $M \mid N$. O resto resulta da unicidade da fatoração (8.8b).

b) e c) são conseqüências imediatas de a). — d) é óbvio. $\square$

Este corolário mostra que é igual trabalhar com a inclusão ou com a divisibilidade no grupo $\mathcal{F} = \mathcal{G}$ dos ideais fracionários de um domínio de Dedekind. Historicamente, como a teoria dos ideais se desenvolveu a partir da fatoração, o aspecto da divisibilidade esteve em primeiro plano e realmente prevaleceu por muito tempo, dando origem a denominações como “ideal primo”, “ideal sem divisor (= teilerlos)”, “ideais sem divisor comum (= teilerfremd)”, sendo as últimas duas, hoje em dia, geralmente substituídos por “ideais maximais” e “ideais comaximais”, respectivamente. A parte da teoria dos ideais na qual predominam a divisibilidade e a multiplicação, a saber, a que trata de domínios de Dedekind e de várias generalizações deles, é conhecida como a “Teoria Multiplicativa dos Ideais” (veja Gilmer [9] e Larsen-McCarthy [22]).

Concluimos do corolário (8.10):

(8.11) **COROLÁRIO.** *Seja R um domínio de Dedekind. Então*

- a) *Para todo $\alpha \in \mathcal{J}$, o conjunto dos ideais de R que contém α é finito.*
 b) *Para todo $\alpha \in \mathcal{J}$, os ideais $\alpha \cdot p$, onde p percorre $\mathcal{P}$, são os elementos maximais do conjunto dos ideais de R que estão estritamente contidos em α .*
 c) *Em $\mathcal{F}$, a interseção e a adição são mutuamente distributivas, e a multiplicação é distributiva em relação à interseção. Além disto, temos que $(M \cap N) \cdot (M + N) = M \cdot N$ para quaisquer $M, N \in \mathcal{F}$.*

Demonstração. a) e b) resultam imediatamente de (8.10a). c) resulta de (8.10) e de relações conhecidas entre $\min \{.,.\}$, $\max \{.,.\}$ e a soma em $\mathbb{Z}$. $\square$

A propriedade (8.11c) significa que nas condições (b), (c), (d) e (e) de §6, estendidas aos ideais fracionários de R , vale sempre a igualdade. De (8.11c) e (6.10) resulta imediatamente:

(8.12) COROLÁRIO. *Todo domínio de Dedekind satisfaz o Teorema Chinês de Restos (isto é, CRT(n) para qualquer $n \geq 2$).*

Uma propriedade importante de domínios de Dedekind R é a de que todo ideal (e todo ideal fracionário) é gerado por dois elementos, podendo um deles ser arbitrariamente prescrito. Ela será obtida como conseqüência do seguinte

(8.13) TEOREMA. *Seja R um domínio de Dedekind. Para quaisquer $M \in \mathcal{F}$ e $b \in \mathcal{J}$ existe $x \in M$ tal que os ideais $x \cdot M^{-1}$, b sejam comaximais.*

Demonstração. Para qualquer $x \in M$, $x \cdot M^{-1}$ é um ideal de R , por (8.5).

Seja $b = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$, onde $k_1 \geq 1, \dots, k_r \geq 1, r \geq 0$. Sendo a afirmação trivial no caso em que $b = R$, podemos supor que $r \geq 1$. Para cada $j = 1, \dots, r$, seja $M_j = p_1 \cdot \dots \cdot p_{j-1} \cdot p_{j+1} \cdot \dots \cdot p_r \cdot M$. De (8.10a) resulta que $p_j \cdot M_j \subset M_j$; digamos que $x_j \in M_j \setminus p_j \cdot M_j$. Obviamente $x_j \in p_i \cdot M$ para $i \neq j$; por outro lado $x_j \notin p_j \cdot M$, pois, caso contrário, teríamos que $x_j \cdot M^{-1} \subseteq p_1 \cap \dots \cap p_r = p_1 \cdot \dots \cdot p_r$ (veja (6.5)), logo $x_j \in p_1 \cdot \dots \cdot p_r \cdot M = p_j \cdot M_j$, o que é absurdo. Seja $x = x_1 + \dots + x_r$; então $x \in M_1 + \dots + M_r \subseteq M$, logo $x \cdot M^{-1} \in \mathcal{J}$; digamos $x \cdot M^{-1} = p_1^{\ell_1} \cdot \dots \cdot p_s^{\ell_s}$, onde $\ell_1, \dots, \ell_s \in \mathbb{N}$ e $s \geq r$. Para todo $j = 1, \dots, r$ temos que $x \notin p_j \cdot M$, pois, caso contrário, teríamos que $x_j = x - (x_1 + \dots + x_{j-1} + x_{j+1} + \dots + x_r) \in p_j \cdot M$, o que é absurdo. Concluimos que $x \cdot M^{-1} \not\subseteq p_j$, ou seja, $x \cdot M^{-1}$ não é um múltiplo de p_j ; logo, $\ell_j = 0$, por (8.10a). Resulta que $\text{MDC}(x \cdot M^{-1}, b) = R$, ou seja, $x \cdot M^{-1} + b = R$, por (8.10b). $\square$

(8.14) COROLÁRIO. *Sejam R um domínio de Dedekind, M um ideal fracionário de R e $y \in M$, $y \neq 0$. Então existe $x \in M$ tal que $M = R \cdot x + R \cdot y$.*

Demonstração. Temos que $y \cdot M^{-1} \in \mathcal{J}$ por (8.5). Por (8.13) existe $x \in M$ tal que $x \cdot M^{-1} + y \cdot M^{-1} = R$; logo $R \cdot x + R \cdot y = M$. $\square$

O seguinte teorema esclarece a relação entre domínios principais, fatoriais e de Dedekind.

(8.15) TEOREMA. Para qualquer domínio R , as seguintes condições são equivalentes:

- (i) R é um domínio principal.
- (ii) R é um domínio fatorial e de Dedekind.

Demonstração. (i) $\Rightarrow$ (ii) já foi demonstrado.

(ii) $\Rightarrow$ (i): Devido a (8.7b), basta provar que todo $p \in \mathcal{P}$ é um ideal principal. Seja $a = z_1 \cdot \dots \cdot z_r$ uma fatoração em elementos irreduzíveis de algum $a \in p \setminus \{0\}$; então $r \geq 1$ e existe $j \in \{1, \dots, r\}$ tal que $z_j \in p$, ou seja, $R \cdot z_j \subseteq p$. Como R é fatorial, $R \cdot z_j$ é um ideal primo não-nulo, e como R é de Dedekind, $R \cdot z_j$ é um ideal maximal; portanto $R \cdot z_j$ é igual a p . $\square$

De (8.15) e (8.2) concluímos:

(8.16) COROLÁRIO. Seja L um corpo de números algébricos. Então I_L será um domínio principal se e somente se for fatorial.

Um caso importante em que as condições equivalentes de (8.15) são satisfeitas é indicado no seguinte teorema, cuja demonstração é feita por meio da versão fraca (6.5) do Teorema Chinês de Restos.

(8.17) TEOREMA. Todo domínio de Dedekind R que possui apenas um número finito de ideais primos é um domínio principal.

Demonstração. Devido a (8.7b) basta provar que todo $p \in \mathcal{P} = \{p_1, \dots, p_n\}$ é principal. Por (8.10a) temos que $p_1^2 \subset p_1$; digamos que $r_1 \in p_1 \setminus p_1^2$. Devido a (6.3), os ideais $p_1^2, p_2, \dots, p_n$ são comaximais dois a dois. Por (6.5) existe $r \in R$ tal que $r \equiv r_1 \pmod{p_1^2}$ e $r \equiv 1 \pmod{p_j}$ ($j = 2, \dots, n$); logo $r \in p_1 \setminus p_1^2$, $r \notin p_2, \dots, r \notin p_n$; ou seja, $R \cdot r$ é um múltiplo de p_1 , mas de nenhum dos ideais $p_1^2, p_2, \dots, p_n$. Portanto, na fatoração $R \cdot r = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$ temos que $k_1 = 1, k_2 = \dots = k_n = 0$, isto é, $R \cdot r = p_1$. Analogamente prova-se que $p_2, \dots, p_n$ são ideais principais de R . $\square$

Como já foi mencionado anteriormente, em qualquer domínio de Dedekind R os ideais fracionários principais formam um subgrupo $\mathcal{H}$ do grupo $\mathcal{F} = \mathcal{G}$. O grupo quociente $\mathcal{Cl} = \mathcal{G}/\mathcal{H}$ é chamado o grupo de classes de ideais de R . A denominação "classe de ideais" em lugar de "classe de ideais fracionários" é justificada pela seguinte razão: A aplicação definida por $a \mapsto a \cdot \mathcal{H}$ ($a \in \mathcal{G}$) é um homomorfismo de $\mathcal{G}$ sobre $\mathcal{Cl}$, e te-

remos que $a \cdot \mathcal{H} = b \cdot \mathcal{H}$ se e somente se os ideais $a, b \in \mathcal{I}$ forem *equivalentes* no sentido de existirem $c, d \in R \setminus \{0\}$ tais que $a \cdot c = b \cdot d$; portanto, os elementos de $\mathcal{H}$ podem ser identificados com as classes de equivalência de ideais $a \in \mathcal{I}$. A ordem (não necessariamente finita) de $\mathcal{H}$ é chamada o *número de classes* de R e usualmente denotada por h_R . Obviamente:

(8.18) *Um domínio de Dedekind R será um domínio principal se e somente se o grupo $\mathcal{H}$ for trivial, ou seja, se $h_R = 1$.*

No caso geral, o número h_R , indicando o número (cardinal) de classes de ideais distintas, pode ser considerado como uma “medida” que indica o quanto o domínio de Dedekind difere de um domínio principal. Veremos em §10 que, no caso em que $R = I_L$, onde L é um corpo de números algébricos, o número h_R é sempre finito.

Notemos ainda que, para qualquer domínio de Dedekind R , os homomorfismos canônicos de $U(R)$ em K^* , de K^* em $\mathcal{G}$ e de $\mathcal{G}$ em $\mathcal{H}$ (juntamente com dois homomorfismos triviais) formam uma sequência exata

$$(1) \rightarrow U(R) \rightarrow K^* \rightarrow \mathcal{G} \rightarrow \mathcal{H} \rightarrow (1),$$

o que significa que a imagem de cada homomorfismo coincide com o núcleo do homomorfismo seguinte.

EXERCÍCIOS

- 8.1. Seja p um número primo. Quais dos seguintes submódulos do $\mathbb{Z}$ -módulo $\mathbb{Q}$ são ideais fracionários de $\mathbb{Z}$?
 - a) $(\mathbb{Z} : p\mathbb{Z})$
 - b) $\bigcup_{n \in \mathbb{N}} (\mathbb{Z} : p^n \mathbb{Z}) = \{x \in \mathbb{Q} \mid p^n \cdot x \in \mathbb{Z} \text{ para algum } n \in \mathbb{N}\}$
 - c) $\mathbb{Z}_{p\mathbb{Z}} = \{a \cdot b^{-1} \mid a, b \in \mathbb{Z}, b \notin p\mathbb{Z}\}$.
- 8.2. Seja $R = \mathbb{Q}[X, Y]$ (anel de polinômios em duas indeterminadas X, Y). Indique
 - a) um ideal não-nulo α de R tal que $(R : \alpha) \cdot \alpha \neq R$;
 - b) um ideal não-nulo de R contido numa infinidade de ideais maximais de R .
- 8.3. Seja α um ideal invertível do domínio R . Prove que se $\alpha \neq R$ então $\alpha^n \subset \alpha^{n-1}$ para todo $n \in \mathbb{Z}$.

- 8.4. Sejam a, b ideais do domínio de Dedekind R . Prove que $a \cdot b = a \cap b$ se e somente se a, b forem comaximais.
- 8.5. Seja R um domínio de Dedekind. Demonstre o seguinte reforço parcial do Corolário (6.6): Quaisquer que sejam $p_1, \dots, p_n$ ideais primos não-nulos de R e distintos dois a dois, quaisquer que sejam os números $k_1, \dots, k_n \in \mathbb{N}$, e quaisquer que sejam os elementos $r_1, \dots, r_n \in R$, existe $r \in R$ tal que $r - r_j \in p_j^{k_j} \setminus p_j^{k_j+1}$ ($j = 1, \dots, n$).
- 8.6. Seja a um ideal não-nulo do domínio de Dedekind R e seja $\mathcal{P}'$ um conjunto finito de ideais primos não-nulos de R . Usando o exercício anterior, prove que:
- Existe $a \in a \setminus \{0\}$ tal que $R \cdot a = a \cdot c$, onde c é um ideal não divisível por nenhum $p \in \mathcal{P}'$.
 - Existe $x \in K \setminus \{0\}$ tal que $x \cdot a \subseteq R$ e $x \cdot a$ não seja divisível por nenhum $p \in \mathcal{P}'$.
 - Toda classe de ideais contém um ideal b tal que a, b sejam comaximais.
- 8.7. Utilize o item a) do exercício anterior para dar uma outra demonstração do teorema (8.13).
- 8.8. Seja a um ideal não-nulo do domínio de Dedekind R e seja $b \in a \setminus \{0\}$. Seja $\mathcal{P}'$ um conjunto finito de ideais primos não-nulos de R que contenha todos os ideais primos que dividem $R \cdot b$. Prove: Para qualquer $c \in a \setminus \{0\}$ tal que $c \cdot a^{-1}$ não seja divisível por nenhum $p \in \mathcal{P}'$, temos que $a = R \cdot b + R \cdot c$.
(Note que existe um elemento c deste tipo pelo item a) do exercício 8.6.)
- 8.9. Por um *anel de valorização* do corpo K entendemos um subanel R de K tal que $1 \in x \cdot R \cup x^{-1} \cdot R$, qualquer que seja $x \in K \setminus \{0\}$. Prove:
- R possui um único ideal maximal m (a saber, $m = R \setminus U(R)$).
 - No caso em que $R \neq K$, o ideal m será invertível se e somente se for principal, se e somente se $(R : m) \neq R$.
 - Todo ideal finitamente gerado de R é principal.
- 8.10. Seja K um corpo e seja v uma aplicação de K sobre $\mathbb{Z} \cup \{\infty\}$ tal que
- $$v(x \cdot y) = vx + vy \quad \text{e} \quad v(x + y) \geq \min \{vx, vy\}$$
- para quaisquer $x, y \in K$. Prove que:

- a) $R_v = \{x \in K \mid vx \geq 0\}$ é um anel de valorização de K , distinto de K , e $m_v = \{x \in K \mid vx \geq 1\}$ é seu ideal maximal.
- b) $m_v = R_v \cdot t$ para qualquer $t \in K$ tal que $vt = 1$.
- c) A aplicação definida por $n \mapsto m_v^n$ ($n \in \mathbb{Z}$) é um isomorfismo do grupo aditivo $\mathbb{Z}$ sobre o grupo multiplicativo $\mathcal{F} = \mathcal{G}$ dos ideais fracionários de R_v e induz um isomorfismo do monóide aditivo $\mathbb{N}$ sobre o monóide multiplicativo $\mathcal{J}$ dos ideais não-nulos de R_v .

A aplicação v é chamada uma *valorização discreta* de K .

8.11. Sejam R um domínio de Dedekind, $K = Q(R)$, e sejam $\mathcal{G}, \mathcal{P}$ como definidos no §8. Prove que, para todo $p \in \mathcal{P}$,

- a) existe um e um só homomorfismo ω de $\mathcal{G}$ sobre o grupo aditivo $\mathbb{Z}$ tal que $\omega p = 1$ e $\omega p' = 0$ para todo $p' \in \mathcal{P} \setminus \{p\}$. Ele é sobrejetivo e satisfaz

$$\omega(M + N) = \min \{\omega M, \omega N\}$$

$$\omega(M \cap N) = \max \{\omega M, \omega N\}.$$

- b) a aplicação $v : K \rightarrow \mathbb{Z} \cup \{\infty\}$ definida por $x \mapsto \omega(R \cdot x)$ ($x \in K \setminus \{0\}$) e $0 \mapsto \infty$ é uma valorização discreta de K , cujo anel de valorização R_v é igual à localização de R em relação a p .

8.12. Seja R um domínio, distinto do seu corpo de frações $K = Q(R)$. Prove que as seguintes condições são equivalentes:

- (i) R é noetheriano, integralmente fechado e possui apenas um ideal primo não-nulo.
- (ii) R é um domínio de Dedekind e possui apenas um ideal maximal.
- (iii) $R = R_v$ para alguma valorização discreta v de K .
- (iv) R é um anel de valorização noetheriano.
- (v) R é um domínio principal e possui apenas um ideal maximal.

CAPÍTULO III

CLASSES DE IDEAIS

O objetivo principal deste capítulo é mostrar que, para qualquer corpo de números algébricos L , o número de classes h_L , isto é, a ordem do grupo abeliano $\mathcal{C}$ das classes de ideais de I_L , é finito.

Como ferramenta será usada a norma de ideais $\mathfrak{N}$, que generaliza a norma absoluta $|\mathcal{N}_{L|\mathbb{Q}}|$. Do estudo desta norma, que será feito no §9, resulta também a “igualdade fundamental” $\sum e_i \cdot f_i = [L:\mathbb{Q}]$, que rege a decomposição de cada número primo p no anel I_L , representando assim o ponto de partida do Capítulo IV.

A finitude de h_L , a ser provada no §10, resultará da existência de uma cota superior para a norma de certos ideais, e é fácil obter tal cota através de uma aplicação simples do “princípio de gavetas”. Cotas melhores, obtidas por métodos geométricos (veja Capítulo VI) e, em particular, a “cota de Minkowski”, têm a vantagem de fornecer importantes estimativas para o discriminante d_L e podem ser utilizadas para calcular o número de classes h_L . Embora o cálculo de h_L , para um determinado corpo L , possa, em princípio, ser efetuado efetivamente (isto é, em um número finito de passos — veja Borevich-Shafarevich [6], Chapter 3, Section 7), tal cálculo será viável apenas em casos bem simples. Deve ser mencionado, porém, que, através do método analítico (envolvendo a função zeta de Dedekind) se obtém para h_L uma fórmula válida para qualquer corpo de números algébricos L , e fórmulas mais explícitas para corpos quadráticos e corpos ciclotômicos (veja Borevich-Shafarevich [6], Chapter 5).

§9. Norma de ideais

Lembramos que, no §5, foi usado o fato de que qualquer módulo livre M sobre um domínio R pode ser inerso num $Q(R)$ -espaço V . Neste parágrafo utilizaremos um outro método para passar de módulos a espaços vetoriais.

Sejam R um anel e $\mathfrak{m}$ um ideal maximal de R . Diremos que um R -módulo M é *anulado por* $\mathfrak{m}$ se $c \cdot x = 0$ para quaisquer $c \in \mathfrak{m}$ e $x \in M$. Neste

caso, M pode ser considerado como $R/\mathfrak{m}$ -espaço, sendo a operação externa $R/\mathfrak{m} \times M \rightarrow M$ bem-definida por

$$(\bar{r}, x) \mapsto r \cdot x \quad (\bar{r} \in R/\mathfrak{m}, x \in M),$$

onde $r \in R$ é um representante qualquer de $\bar{r}$ (uma vez que $r_1 \equiv r_2 \pmod{\mathfrak{m}}$ implica $r_1 \cdot x - r_2 \cdot x = (r_1 - r_2) \cdot x = 0$). Por outro lado, qualquer $R/\mathfrak{m}$ -espaço N pode ser considerado como R -módulo, com a operação externa $R \times N \rightarrow N$ definida por

$$(r, y) \mapsto (r + \mathfrak{m}) \cdot y \quad (r \in R, y \in N);$$

considerado como R -módulo, N é anulado por $\mathfrak{m}$. Resumindo:

(9.1) *Os R -módulos anulados por $\mathfrak{m}$ coincidem com os $R/\mathfrak{m}$ -espaços.*

Em particular, para todo ideal $\mathfrak{a}$ de R , o R -módulo quociente $\mathfrak{a}/(\mathfrak{m} \cdot \mathfrak{a})$ é anulado por $\mathfrak{m}$ e, portanto, pode ser considerado como $R/\mathfrak{m}$ -espaço.

(9.2) *Sejam R um domínio de Dedekind, $\mathfrak{m}$ um ideal maximal de R e $\mathfrak{a}$ um ideal não-nulo de R . Então $\mathfrak{a}/(\mathfrak{m} \cdot \mathfrak{a})$ é um $R/\mathfrak{m}$ -espaço de dimensão 1.*

Demonstração. De (8.11b) concluímos que $\mathfrak{m} \cdot \mathfrak{a} \subset \mathfrak{a}$ e que não existe nenhum ideal $\mathfrak{b}$ tal que $\mathfrak{m} \cdot \mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{a}$. Aplicando o homomorfismo canônico de R sobre $R/(\mathfrak{m} \cdot \mathfrak{a})$, ambos considerados como R -módulos, concluímos que $\mathfrak{a}/(\mathfrak{m} \cdot \mathfrak{a})$ é um R -módulo não-nulo minimal. De (9.1) resulta que $\mathfrak{a}/(\mathfrak{m} \cdot \mathfrak{a})$ é um $R/\mathfrak{m}$ -espaço minimal; portanto, tem dimensão 1. $\square$

No que se segue, seja L um corpo de números algébricos, de grau $[L:\mathbb{Q}] = n$. Denotaremos por R o anel I_L dos inteiros algébricos de L . Recordemos que R é um domínio de Dedekind e, em particular, que todo ideal primo não-nulo $\mathfrak{p}$ de R é um ideal maximal de R ; logo $R/\mathfrak{p}$ é um corpo, chamado o *corpo de restos* de R módulo $\mathfrak{p}$.

(9.3) *Seja $\mathfrak{p}$ um ideal primo não-nulo de R ; então:*

- a) $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, sendo p o único número primo em $\mathfrak{p}$.
- b) $R/\mathfrak{p}$ é uma extensão finita do corpo $\mathbb{F}_p$, de grau $[R/\mathfrak{p}:\mathbb{F}_p] \leq n$.

Demonstração. a) O ideal primo $\mathfrak{p} \cap \mathbb{Z}$ é não-nulo devido a (1.13a); logo é igual a $p\mathbb{Z}$ para algum número primo p . Obviamente, p é o único número primo em $\mathfrak{p}$.

b) A restrição a $\mathbb{Z}$ do homomorfismo canônico κ de R sobre $R/\mathfrak{p}$ tem como núcleo $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$; logo induz um isomorfismo (obviamente

o único) de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ sobre $\kappa\mathbb{Z}$. Identificando $\kappa\mathbb{Z}$ com $\mathbb{F}_p$, este torna-se um subcorpo de R/p . Por (5.6), existe uma base integral $\beta_1, \dots, \beta_n$ de L . Obviamente, $\kappa\beta_1, \dots, \kappa\beta_n$ é um sistema de geradores do $\mathbb{F}_p$ -espaço R/p ; logo $[R/p : \mathbb{F}_p] \leq n$. $\square$

O grau $[R/p : \mathbb{F}_p]$ será chamado o *grau de inércia* de p e denotado por $f(p)$.

Seja a um ideal não-nulo de R . Será denotado por $\mathfrak{N}a$, e chamado *norma do ideal* a , o número (cardinal) dos elementos de R/a . Mostremos primeiramente que este número é sempre finito e que a norma de ideais é multiplicativa.

- (9.4) a) Para todo ideal primo não-nulo p de R temos que $\mathfrak{N}p = p^f$, onde f é o grau de inércia de p e p o único número primo em p .
 b) Para todo ideal não-nulo a de R temos que $\mathfrak{N}a \in \mathbb{N} \setminus \{0\}$; em particular, $\mathfrak{N}a = 1$ se e somente se $a = R$.
 c) Para quaisquer ideais não-nulos a, b de R vale $\mathfrak{N}(a \cdot b) = \mathfrak{N}a \cdot \mathfrak{N}b$.

Demonstração. a) De $[R/p : \mathbb{F}_p] = f$ resulta que R/p tem p^f elementos.

b) e c): Afiramos que $\mathfrak{N}(p_1 \cdot \dots \cdot p_r) = \mathfrak{N}p_1 \cdot \dots \cdot \mathfrak{N}p_r$ para qualquer produto de r ideais primos não-nulos $p_1, \dots, p_r$ de R . Sendo trivial para $r = 0$, supomos que a afirmação seja válida para qualquer produto de $r - 1$ ideais primos não-nulos, sendo $r \geq 1$. Sejam $a = p_1 \cdot \dots \cdot p_{r-1}$ e $b = p_r$; então $a \cdot b \subseteq b$, e o anel quociente R/b é isomorfo a $(R/a)/(b/a)$. Por (9.2), b/a é um R/p_1 -espaço de dimensão 1, logo consiste de $\mathfrak{N}p_1$ elementos. Como R/b , por hipótese, consiste de $\mathfrak{N}p_2 \cdot \dots \cdot \mathfrak{N}p_r$ elementos, concluímos que R/a consiste de $\mathfrak{N}p_1 \cdot \dots \cdot \mathfrak{N}p_r$ elementos, ou seja, $\mathfrak{N}a = \mathfrak{N}p_1 \cdot \dots \cdot \mathfrak{N}p_r \in \mathbb{N} \setminus \{0\}$. Em particular, $\mathfrak{N}a = 1$ se e somente se $r = 0$, se e somente se $a = R$. As afirmações b) e c) resultam então do fato de todo ideal não-nulo de R ser um produto de ideais não-nulos, devido a (8.8). $\square$

De (9.4) obtemos facilmente as seguintes propriedades de $\mathfrak{N}$, que são semelhantes às propriedades da norma $\mathcal{N}_{L/\mathbb{Q}}$, indicadas em (1.11).

(9.5) Seja a um ideal não-nulo de R . Então:

- a) $\mathfrak{N}a \in a$, ou seja, o ideal principal $R \cdot \mathfrak{N}a$ é um múltiplo de a .
 b) Se $\mathfrak{N}a$ for um número primo então a será um ideal primo.
 c) Se a for um múltiplo do ideal b e $\mathfrak{N}a = \mathfrak{N}b$ então $a = b$.

Demonstração. a) O grupo aditivo de $R/\mathfrak{a}$ tem ordem $m = \mathfrak{N}\mathfrak{a}$; portanto $m \cdot \bar{1} = \bar{0}$, sendo $\bar{1}$ e $\bar{0}$ respectivamente a unidade e o zero do anel $R/\mathfrak{a}$. Resulta que $m \in \mathfrak{a}$, ou seja, $R \cdot m \subseteq \mathfrak{a}$, o que equivale a $\mathfrak{a} \mid R \cdot m$, devido a (8.10).

b) Se $\mathfrak{a}$ não for um ideal primo de R , então $\mathfrak{a} = R$ ou $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$, onde $\mathfrak{b}, \mathfrak{c}$ são ideais não-nulos e distintos de R . Em ambos os casos, $\mathfrak{N}\mathfrak{a}$ não é um número primo, devido a (9.4).

c) Existe um ideal não-nulo $\mathfrak{c}$ de R tal que $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$. De (9.4) concluímos que $\mathfrak{N}\mathfrak{a} = \mathfrak{N}\mathfrak{b} \cdot \mathfrak{N}\mathfrak{c}$, e que $\mathfrak{N}\mathfrak{a} = \mathfrak{N}\mathfrak{b}$ implica que $\mathfrak{N}\mathfrak{c} = 1$; logo $\mathfrak{c} = R$, e $\mathfrak{a} = \mathfrak{b}$. $\square$

De (9.5a) e (8.11a) resulta imediatamente:

(9.6) Para todo $m \in \mathbb{N} \setminus \{0\}$ existe somente um número finito de ideais não-nulos $\mathfrak{a}$ de R tais que $\mathfrak{N}\mathfrak{a} = m$.

O seguinte teorema relaciona a norma de ideais com o discriminante e mostra que ela generaliza a norma absoluta $|\mathcal{N}_{L|\mathbb{Q}}|$.

(9.7) TEOREMA. a) Todo ideal não-nulo $\mathfrak{a}$ de R é um $\mathbb{Z}$ -módulo livre de posto n , e para toda base $\alpha_1, \dots, \alpha_n$ deste $\mathbb{Z}$ -módulo temos que

$$\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = (\mathfrak{N}\mathfrak{a})^2 \cdot d_L.$$

b) Para todo elemento não-nulo $\alpha \in R$ temos que $\mathfrak{N}(R \cdot \alpha) = |\mathcal{N}_{L|\mathbb{Q}}\alpha|$.

Demonstração. a) Aplicando (5.1) ao $\mathbb{Z}$ -módulo livre R , obtemos uma base integral $\varepsilon_1, \dots, \varepsilon_n$ de L e números inteiros $a_1, \dots, a_q$, $q \leq n$, tais que $a_1 \cdot \varepsilon_1, \dots, a_q \cdot \varepsilon_q$ formem uma base do $\mathbb{Z}$ -módulo livre $\mathfrak{a}$. Por (5.2), o $\mathbb{Z}$ -módulo $R/\mathfrak{a}$ é isomorfo a $\mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_q\mathbb{Z} \times \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{n-q}$.

Como $\mathfrak{N}\mathfrak{a}$ é finita por (9.4), concluímos que $n = q$ e $\mathfrak{N}\mathfrak{a} = |a_1| \cdot \dots \cdot |a_n| = |a_1 \cdot \dots \cdot a_n|$. Logo

$$\text{disc}_{L|\mathbb{Q}}(a_1 \cdot \varepsilon_1, \dots, a_n \cdot \varepsilon_n) = (\det(a_i \cdot \delta_{ij}))^2 \cdot \text{disc}_{L|\mathbb{Q}}(\varepsilon_1, \dots, \varepsilon_n) = (\mathfrak{N}\mathfrak{a})^2 \cdot d_L.$$

Toda base $\alpha_1, \dots, \alpha_n$ do $\mathbb{Z}$ -módulo $\mathfrak{a}$ escreve-se como $\alpha_i = \sum_{j=1}^n c_{ij} \cdot (a_j \cdot \varepsilon_j)$,

com $c_{ij} \in \mathbb{Z}$ ($i, j = 1, \dots, n$) e $\det(c_{ij}) \in U(\mathbb{Z}) = \{1, -1\}$; portanto

$$\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = \text{disc}_{L|\mathbb{Q}}(a_1 \cdot \varepsilon_1, \dots, a_n \cdot \varepsilon_n).$$

b) Suponhamos que $\beta_1, \dots, \beta_n$ formem uma base integral de L . Então $\alpha \cdot \beta_1, \dots, \alpha \cdot \beta_n$ formam uma base do ideal principal $R \cdot \alpha$, considerado

como $\mathbb{Z}$ -módulo; logo $\text{disc}_{L|\mathbb{Q}}(\alpha \cdot \beta_1, \dots, \alpha \cdot \beta_n) = \mathfrak{N}(R \cdot \alpha)^2 \cdot d_L$, por a).

Por outro lado, existem $a_{ij} \in \mathbb{Z}$ tais que $\alpha \cdot \beta_i = \sum_{j=1}^n a_{ij} \cdot \beta_j$ ($i = 1, \dots, n$);

logo $\text{disc}_{L|\mathbb{Q}}(\alpha \cdot \beta_1, \dots, \alpha \cdot \beta_n) = \det(a_{ij})^2 \cdot d_L$ por (4.1), e $\det(a_{ij}) = \mathcal{N}_{L|\mathbb{Q}}\alpha$. Concluimos que $\mathfrak{N}(R \cdot \alpha) = |\mathcal{N}_{L|\mathbb{Q}}\alpha|$. $\square$

Como consequência deste teorema obtemos uma importante igualdade referente à decomposição em I_L dos números primos p , igualdade esta que será generalizada no Capítulo IV.

(9.8) COROLÁRIO. *Seja p um número primo e seja $R \cdot p = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ a fatoração de $R \cdot p$ em ideais primos distintos $p_1, \dots, p_r$, com $e_1 \geq 1, \dots, e_r \geq 1$. Então:*

- $p_1, \dots, p_r$ são os únicos ideais primos p de R tais que $p \in p$.
- $\sum_{j=1}^r e_j \cdot f_j = n$, onde f_j é o grau de inércia de p_j ($j = 1, \dots, r$).

Demonstração. a) Obviamente $p \in p_1^{e_1} \cdot \dots \cdot p_r^{e_r} \subseteq p_j$ para todo $j \in \{1, \dots, r\}$.

Por outro lado, se $p \in p$ então p dividirá $R \cdot p$, logo $p \in \{p_1, \dots, p_r\}$ devido à unicidade da fatoração.

b) De (9.4) e (9.7b) concluímos que

$$\mathfrak{N}(R \cdot p) = \prod_{j=1}^r \mathfrak{N}(p_j)^{e_j} = \prod_{j=1}^r p^{f_j \cdot e_j} \text{ e } \mathfrak{N}(R \cdot p) = |\mathcal{N}_{L|\mathbb{Q}} p| = p^n,$$

respectivamente; logo vale b). $\square$

Terminaremos este parágrafo mostrando, num exemplo, a utilidade da norma de ideal para determinar explicitamente a fatoração em ideais primos.

Observemos primeiramente que, quando o domínio R for fatorial, a fatoração $\alpha = \zeta_1 \cdot \dots \cdot \zeta_r$ (essencialmente única) em fatores irredutíveis $\zeta_1, \dots, \zeta_r$ fornecerá imediatamente a fatoração desejada de $R \cdot \alpha$, uma vez que $R \cdot \zeta_1, \dots, R \cdot \zeta_r$ são ideais primos não-nulos de R . Por outro lado, quando R não for fatorial, existirão elementos irredutíveis ζ que não são primos, ou seja, tais que $R \cdot \zeta$ seja um produto de mais de um ideal primo. Neste caso, a fatoração de $R \cdot \alpha$ em ideais primos pode ser obtida juntando-se as fatoraões dos ideais $R \cdot \zeta_1, \dots, R \cdot \zeta_r$, qualquer que seja a fatoração $\alpha = \zeta_1 \cdot \dots \cdot \zeta_r$ em fatores irredutíveis.

Consideremos como exemplo o corpo quadrático $L = \mathbb{Q}(\sqrt{-17})$. Seu anel dos inteiros algébricos $R = I_L = \mathbb{Z}[\sqrt{-17}]$ não é fatorial; por

exemplo, o número 18 tem duas fatorações distintas em fatores irredutíveis, a saber, $18 = 2 \cdot 3 \cdot 3 = (1 + \sqrt{-17}) \cdot (1 - \sqrt{-17})$. Sendo

$$p = R \cdot 2 + R \cdot (1 + \sqrt{-17}), \quad q = R \cdot 3 + R \cdot (1 + \sqrt{-17}) \quad e \\ r = R \cdot 3 + R \cdot (1 - \sqrt{-17}),$$

mostraremos;

- (9.9) a) p, q e r são ideais primos de R com $f(p) = f(q) = f(r) = 1$.
 b) $R \cdot 18 = p^2 \cdot q^2 \cdot r^2$.
 c) $R \cdot 2 = p^2$, $R \cdot 3 = q \cdot r$, $R \cdot (1 + \sqrt{-17}) = p \cdot q^2$,
 $R \cdot (1 - \sqrt{-17}) = p \cdot r^2$.

Demonstração. a) Obviamente $R/p = \{p, 1 + p\}$, $R/q = \{q, 1 + q, 2 + q\}$ e $R/r = \{r, 1 + r, 2 + r\}$; logo $\mathfrak{N}p = 2$, $\mathfrak{N}q = \mathfrak{N}r = 3$. De (9.5 b) resulta que p, q e r são ideais primos, e de (9.4a) concluímos que $f(p) = f(q) = f(r) = 1$.

b) De $3 \in q \cap r$ e $(1 + \sqrt{-17}) \cdot (1 - \sqrt{-17}) \in p^2$ resulta que $18 \in p^2 \cap q^2 \cap r^2 = p^2 \cdot q^2 \cdot r^2$; logo este ideal divide $R \cdot 18$. Como $\mathfrak{N}(p^2 \cdot q^2 \cdot r^2) = 2^2 \cdot 3^2 \cdot 3^2 = 18^2 = |\mathcal{N}_{L/\mathbb{Q}} 18| = \mathfrak{N}(R \cdot 18)$ por (9.4) e (9.7), concluímos que $p^2 \cdot q^2 \cdot r^2 = R \cdot 18$, devido a (9.5c).

c) Os ideais principais gerados por 2, 3, $1 + \sqrt{-17}$ e $1 - \sqrt{-17}$ dividem $R \cdot 18 = p^2 \cdot q^2 \cdot r^2$. Como $2 \notin q$ e $2 \notin r$, o ideal $R \cdot 2$ divide p^2 . De $\mathfrak{N}(R \cdot 2) = 4 = \mathfrak{N}p^2$ resulta que $R \cdot 2 = p^2$. Como $3 \in p \cap r = p \cdot r$, o ideal $R \cdot 3$ é um múltiplo de $q \cdot r$. De $\mathfrak{N}(R \cdot 3) = 9 = \mathfrak{N}(q \cdot r)$ resulta que $R \cdot 3 = q \cdot r$. Como $1 + \sqrt{-17} \in p \cap q$ mas $\notin r$, o ideal $R \cdot (1 + \sqrt{-17})$ é um múltiplo de $p \cdot q$ mas não de r ; logo é igual a um dos ideais $p \cdot q$, $p^2 \cdot q$, $p \cdot q^2$, $p^2 \cdot q^2$. Entre eles, $p \cdot q^2$ é o único ideal cuja norma é igual a $18 = |\mathcal{N}_{L/\mathbb{Q}}(1 + \sqrt{-17})| = \mathfrak{N}(R \cdot (1 + \sqrt{-17}))$; logo $R \cdot (1 + \sqrt{-17}) = p \cdot q^2$. Analogamente prova-se que $R \cdot (1 - \sqrt{-17}) = p \cdot r^2$. $\square$

Note-se que as igualdades $R \cdot 2 = p^2$ e $R \cdot 3 = q \cdot r$ estão em concordância com o corolário (9.8).

EXERCÍCIOS

Nos exercícios 9.1 a 9.5, seja L qualquer corpo de números algébricos, e seja $R = I_L$.

- 9.1. Prove (sem usar a norma de ideais) que todo número primo p está contido em pelo menos um ideal primo de R .

9.2. Indique, para cada $m \in \mathbb{N} \setminus \{0\}$, uma cota superior para o número dos ideais $\mathfrak{a}$ de R tais que $\mathfrak{N}\mathfrak{a} = m$.

9.3. Seja $\mathfrak{a}$ um ideal não-nulo de R . Prove que se existir $\alpha \in \mathfrak{a}$ tal que $\mathfrak{N}\mathfrak{a} = |\mathcal{N}_{L|\mathbb{Q}}\alpha|$ então $R \cdot \alpha = \mathfrak{a}$.

9.4. Sejam $\mathfrak{a}$ um ideal não-nulo de R , $\beta \in \mathfrak{a} \setminus \{0\}$, e $\mathcal{P}'$ um conjunto finito de ideais primos não-nulos de R com as seguintes propriedades:

- a) Todo ideal primo $\mathfrak{p}$ que divide $R \cdot \beta$ está em $\mathcal{P}'$.
- b) Para todo número primo p , $\mathcal{P}_p \cap \mathcal{P}' \neq \emptyset$ implica que $\mathcal{P}_p \subseteq \mathcal{P}'$, onde $\mathcal{P}_p$ é o conjunto dos ideais primos $\mathfrak{p}$ tais que $p \in \mathfrak{p}$.

Prove que, para qualquer $\alpha \in \mathfrak{a} \setminus \{0\}$ tal que $\alpha \cdot \alpha^{-1}$ não seja divisível por nenhum $p \in \mathcal{P}'$, vale

$$\mathfrak{N}\mathfrak{a} = \text{MDC}(\mathcal{N}_{L|\mathbb{Q}}\alpha, \mathcal{N}_{L|\mathbb{Q}}\beta).$$

(Note que existe um elemento α deste tipo pelo item a) do exercício 8.6.).

9.5. Sejam p um número primo e $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ os únicos ideais primos de R que contêm p .

- a) Prove que existe $\pi \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$ tal que $\pi \notin \mathfrak{p}_2 \cup \dots \cup \mathfrak{p}_r$, e que todo elemento π deste tipo satisfaz $\mathfrak{p}_1 = R \cdot p + R \cdot \pi$.
- b) Indique um elemento π deste tipo no caso em que $p = 2$ (respectivamente $p = 3$) e $L = \mathbb{Q}(\sqrt{-5})$.

9.6. Seja $R = \mathbb{Z}[i]$ (o anel dos inteiros de Gauss).

- a) Para todo número primo p indique a fatoração do ideal $R \cdot p$ em ideais primos de R .
- b) Para todo ideal primo $\mathfrak{p}$ de R determine o grau de inércia $f(\mathfrak{p})$.

9.7. Seja $R = \mathbb{Z}[\sqrt{-5}]$. Prove que $\mathfrak{p} = R \cdot 2 + R \cdot (1 + \sqrt{-5})$, $\mathfrak{q} = R \cdot 3 + R \cdot (1 + \sqrt{-5})$ e $\mathfrak{r} = R \cdot 3 + R \cdot (1 - \sqrt{-5})$ são ideais primos de R , e indique a fatoração em ideais primos dos ideais principais $R \cdot 6$, $R \cdot 2$, $R \cdot 3$, $R \cdot (1 + \sqrt{-5})$ e $R \cdot (1 - \sqrt{-5})$.

§10. Finitude do número de classes

Como no parágrafo anterior, denotaremos por $\hat{R}$ o anel dos inteiros algébricos I_L de um corpo de números algébricos L , de grau $n = [L : \mathbb{Q}]$. Além disto, $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ e $\mathcal{C}\mathcal{L}$ terão o mesmo significado que no §8, e $h_L = h_R$.

Recordemos que, para quaisquer $\alpha \in \mathcal{J}$ e $\alpha \in \mathfrak{a} \setminus \{0\}$, a norma $\mathfrak{N}\alpha$ divide $\mathfrak{N}(R \cdot \alpha) = |\mathcal{N}_{L|\mathbb{Q}}\alpha|$, e assim o quociente $(\mathfrak{N}\alpha)^{-1} \cdot \mathfrak{N}(R \cdot \alpha)$ é um número natural não-nulo; em particular, ele será igual a 1 se e somente se $\alpha = R \cdot \alpha$. Concluimos que

$$n(\alpha) = \min \{(\mathfrak{N}\alpha)^{-1} \cdot \mathfrak{N}(R \cdot \alpha) \mid \alpha \in \mathfrak{a} \setminus \{0\}\} \in \mathbb{N} \setminus \{0\},$$

qualquer que seja $\alpha \in \mathcal{J}$; em particular, $n(\alpha) = 1$ se e somente se $\alpha \in \mathcal{H}$. Resulta que R será um domínio principal, se e somente se $n(\alpha) = 1$ para todo $\alpha \in \mathcal{J}$.

Mostraremos que, para qualquer corpo de números algébricos L , o conjunto $\{n(\alpha) \mid \alpha \in \mathcal{J}\}$ é limitado.

(10.1) Existe $\rho > 0$ tal que $n(\alpha) \leq \rho$ para todo $\alpha \in \mathcal{J}$.

Demonstração. Sejam $\sigma_1, \dots, \sigma_n$ os isomorfismos de L em $\mathbb{C}$, e suponhamos que $\beta_1, \dots, \beta_n$ formem uma base integral de L . Mostraremos que $\rho = \prod_{j=1}^n \left(\sum_{i=1}^n |\sigma_j \beta_i| \right)$ tem a propriedade desejada. Para todo $\alpha \in \mathcal{J}$ existe $k \in \mathbb{N} \setminus \{0\}$ tal que $k^n \leq \mathfrak{N}\alpha < (k+1)^n$. Seja

$$\mathcal{S} = \left\{ \sum_{i=1}^n d_i \cdot \beta_i \mid d_i \in \{0, \dots, k\}; i = 1, \dots, n \right\};$$

obviamente $\mathcal{S} \subseteq R$. Como o número $(k+1)^n$ dos elementos de $\mathcal{S}$ é maior que o número $\mathfrak{N}\alpha$ das classes de $R \bmod \alpha$, existem (pelo "princípio de gavetas") dois elementos distintos $\lambda, \nu \in \mathcal{S}$ tais que $\lambda + \alpha = \nu + \alpha$. Obviamente $\lambda - \nu = \sum_{i=1}^n a_i \cdot \beta_i \in \alpha$, com $a_i \in \{-k, \dots, -1, 0, 1, \dots, k\}$ ($i = 1, \dots, n$); logo

$$\begin{aligned} |\mathcal{N}_{L|\mathbb{Q}}(\lambda - \nu)| &= \left| \prod_{j=1}^n \sigma_j(\lambda - \nu) \right| = \prod_{j=1}^n \left| \sum_{i=1}^n a_i \cdot \sigma_j \beta_i \right| \leq \\ &\leq \prod_{j=1}^n \left(\sum_{i=1}^n |a_i| \cdot |\sigma_j \beta_i| \right) \leq k^n \cdot \rho \leq \mathfrak{N}\alpha \cdot \rho; \end{aligned}$$

portanto $n(\alpha) \leq (\mathfrak{N}\alpha)^{-1} \cdot |\mathcal{N}_{L|\mathbb{Q}}(\lambda - \nu)| \leq \rho$. $\square$

Os números $n(\alpha)$ permitem ainda uma outra interpretação. Para toda classe $\mathfrak{B} \in \mathcal{C}\ell$ seja

$$m(\mathfrak{B}) = \min \{\mathfrak{N}b \mid b \in \mathcal{J} \cap \mathfrak{B}\}.$$

(10.2) Sejam $\mathfrak{B} \in \mathcal{C}\ell$ e $\alpha \in \mathcal{J}$ tais que $\alpha^{-1} \in \mathfrak{B}$. Então $m(\mathfrak{B}) = n(\alpha)$.

Demonstração. Escolhemos $b \in \mathcal{J} \cap \mathfrak{B}$ tal que $\mathfrak{N}b = m(\mathfrak{B})$. Por hipótese, existe $\xi \in L \setminus \{0\}$ tal que $\alpha^{-1} \cdot \xi = b$; logo $\xi \in R \cdot \xi = \alpha \cdot b \subseteq \alpha$, e assim $n(\alpha) \leq (\mathfrak{N}\alpha)^{-1} \cdot \mathfrak{N}(R \cdot \xi) = \mathfrak{N}b = m(\mathfrak{B})$. Por outro lado, seja $\alpha \in \alpha \setminus \{0\}$ tal que $n(\alpha) = (\mathfrak{N}\alpha)^{-1} \cdot \mathfrak{N}(R \cdot \alpha)$, e seja $b = \alpha^{-1} \cdot \alpha$. Então $b \in \mathfrak{B}$, $\alpha \cdot b = R \cdot \alpha$, logo $\mathfrak{N}\alpha \cdot \mathfrak{N}b = \mathfrak{N}(R \cdot \alpha)$; portanto, $m(\mathfrak{B}) \leq \mathfrak{N}b = (\mathfrak{N}\alpha)^{-1} \cdot \mathfrak{N}(R \cdot \alpha) = n(\alpha)$. $\square$

De (10.2) resulta imediatamente que os conjuntos $\{n(\alpha) \mid \alpha \in \mathcal{J}\}$ e $\{m(\mathfrak{B}) \mid \mathfrak{B} \in \mathcal{C}\ell\}$ coincidem; portanto, toda classe $\mathfrak{B} \in \mathcal{C}\ell$ possui um ideal b tal que $\mathfrak{N}b \leq \rho$, por (10.1). Por outro lado, concluímos de (9.6) que existe somente um número finito de ideais $b \in \mathcal{J}$ com norma $\mathfrak{N}b \leq \rho$, digamos $b_1, \dots, b_m$. Resulta que $\mathcal{C}\ell$ consiste das classes (não necessariamente distintas) $b_1 \cdot \mathcal{H}, \dots, b_m \cdot \mathcal{H}$; portanto:

(10.3) **TEOREMA.** O número de classes h_L é finito (a saber, $h_L \leq m$).

De (10.3) obtemos como consequência imediata:

(10.4) **COROLÁRIO.** Para todo $\alpha \in \mathcal{J}$, α^{h_L} é um ideal principal.

Para poder calcular o número de classes h_L , é necessário saber quais das classes $b_1 \cdot \mathcal{H}, \dots, b_m \cdot \mathcal{H}$ coincidem. Obviamente teremos que $b_i \cdot \mathcal{H} = b_j \cdot \mathcal{H}$ se e somente se o ideal fracionário $b_j \cdot b_i^{-1}$ for principal, o que pode ser verificado usando-se o teorema (1.17) (veja Exercício 10.1). Em particular, teremos que $h_L = 1$ se e somente se $b_1, \dots, b_m$ forem ideais principais. Condições suficientes para que isto ocorra são dadas na seguinte proposição.

(10.5) Teremos que $h_L = 1$ quando uma das seguintes condições for satisfeita:

- (i) Todo ideal primo não-nulo p de R com norma $\mathfrak{N}p \leq \rho$ é principal.
- (ii) Para qualquer número primo $p \leq \rho$, o ideal $R \cdot p$ é primo.

Demonstração. a) Todo ideal b com norma $\mathfrak{N}b \leq \rho$ é o produto de ideais primos p com $\mathfrak{N}p \leq \rho$. Supondo (i), estes são ideais principais; portanto, b também o é.

b) Seja p um ideal primo não-nulo com norma $\mathfrak{N}p \leq \rho$. Por (9.4), temos que $\mathfrak{N}p = p^f$ onde $f \geq 1$ e p é o único número primo em p ; logo $p \leq \rho$ e $R \cdot p \subseteq p$. Supondo (ii), concluímos que $R \cdot p = p$, uma vez que R é um domínio de Dedekind; portanto a condição (i) é satisfeita. Pela parte a) da demonstração temos que $h_L = 1$. $\square$

O cálculo de h_L acima esboçado, o qual sempre pode ser feito efetivamente (veja Borevich-Shafarevich [6], Chapter 3, Section 7), será tanto mais fácil, e as condições indicadas em (10.5) serão tanto mais fracas, quanto menor for a cota ρ . A melhor cota conhecida, válida para qualquer corpo de números algébricos L , é a *cota de Minkowski*, definida por

$$\mu_L = \left(\frac{4}{\pi}\right)^t \cdot \frac{n!}{n^n} \cdot \sqrt{|d_L|},$$

onde d_L é o discriminante de L e t é a metade do número (par) dos isomorfismos σ de L em $\mathbb{C}$ tais que $\sigma L \not\subseteq \mathbb{R}$ (veja §18). Ela é obtida usando-se métodos geométricos, que serão estudados no Capítulo VI (veja Exercício 17.9).

No caso em que L é um corpo *quadrático* $\mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$ (como definido em §2), temos que

$$\mu_L = \begin{cases} \frac{1}{2} \cdot \sqrt{|d_L|} & \text{quando } L \text{ for real (isto é, } d > 0) \\ \frac{2}{\pi} \cdot \sqrt{|d_L|} & \text{quando } L \text{ for imaginário (isto é, } d < 0) \end{cases}$$

sendo o discriminante d_L igual a $4d$ (respectivamente d) quando $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) mod 4. Consideremos os casos em que a cota μ_L é pequena:

a) Teremos que $\mu_L < 2$ se e somente se $-9 < d_L < 16$, se e somente se $d \in \{-7, -3, -2, -1, 2, 3, 5, 13\}$; neste caso trivialmente $h_L = 1$.

b) Teremos que $2 \leq \mu_L < 3$ se e somente se $-22 < d_L < -9$ ou $16 < d_L < 37$, o que ocorrerá se e somente se

$$d \in \{-19, -15, -11, -5, 6, 7, 17, 21, 29, 33\}.$$

Para determinar h_L neste caso, basta considerar o ideal $R \cdot 2$, o qual ou é primo ou é produto de dois ideais primos p_1, p_2 , não necessariamente distintos, com $\mathfrak{N}p_1 = \mathfrak{N}p_2 = 2$ (veja (9.8)). Se $R \cdot 2$ for um ideal primo ou p_1, p_2 forem ideais principais, então $h_L = 1$, por (10.5). Quando $R \cdot 2 = p_1 \cdot p_2$, então p_1 e p_2 serão os únicos ideais de R com norma igual a 2, logo $\mathcal{C}\ell = \{\mathcal{H}, p_1 \cdot \mathcal{H}, p_2 \cdot \mathcal{H}\}$; logo $h_L \leq 3$ (respectivamente ≤ 2) no caso em que $p_1 \neq$ (respectivamente $=$) p_2 . Por exemplo, no caso $d = -5$ temos que $p_1 = p_2 = R \cdot 2 + R \cdot (1 - \sqrt{-5})$ (veja Exercício 9.7. ou (15.1)); logo $h_L \leq 2$; realmente $h_L = 2$ devido a (2.4). (Veja também Ribenoim [28], Chapter 13, (7), e as listas de h_L indicadas em Borevich-Shafarevich [6], Tables.)

Além de ser útil para calcular o número de classes, a cota de Minkowski fornece também importantes resultados sobre o discriminante.

(10.6) TEOREMA. Para todo corpo de números algébricos L de grau $n = [L:\mathbb{Q}] \geq 2$ temos que

$$|d_L| \geq \left(\frac{\pi}{4}\right)^n \cdot \frac{n^{2n}}{(n!)^2} \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}.$$

Demonstração. Existe $b \in \mathcal{O}$ tal que $1 \leq \Re b \leq \mu_L$; logo $\sqrt{|d_L|} \geq \left(\frac{\pi}{4}\right)^t \cdot \frac{n^n}{n!}$.

Para $m \geq 2$ seja $\alpha_m = \left(\frac{\pi}{4}\right)^m \cdot \frac{m^{2m}}{(m!)^2}$; então $|d_L| \geq \alpha_n$, uma vez que $2t \leq n$ e $\frac{\pi}{4} < 1$. Como $\alpha_2 = \frac{\pi^2}{4}$ e $\frac{\alpha_{m+1}}{\alpha_m} = \frac{\pi}{4} \cdot \left(1 + \frac{1}{m}\right)^{2m} > \frac{\pi}{4} \cdot 3$ para todo $m \geq 2$, concluímos que

$$\alpha_n = \frac{\alpha_n}{\alpha_{n-1}} \cdot \frac{\alpha_{n-1}}{\alpha_{n-2}} \cdot \dots \cdot \frac{\alpha_3}{\alpha_2} \cdot \alpha_2 > \left(\frac{\pi}{4} \cdot 3\right)^{n-2} \cdot \frac{\pi^2}{4} = \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}. \quad \square$$

Este teorema mostra que o mínimo do valor absoluto dos discriminantes, $\min\{|d_L| \mid [L:\mathbb{Q}] = n\}$, cresce exponencialmente com o grau n . Como consequência imediata obtemos o seguinte corolário, devido a Hermite e Minkowski:

(10.7) COROLÁRIO. $|d_L| > 1$ para todo corpo de números algébricos $L \neq \mathbb{Q}$.

Mencionemos ainda sem demonstração, a qual pode ser feita por métodos geométricos, o seguinte teorema devido a Hermite (veja Samuel [30], Chapter IV, Theorem 3):

(10.8) TEOREMA. Para todo $d \in \mathbb{Z}$ existe apenas um número finito de corpos de números algébricos L com $d_L = d$.

Terminaremos este parágrafo abordando um problema que, aberto há várias décadas, foi resolvido somente em 1964. Trata-se de saber se todo corpo de números algébricos, L , está contido num corpo de números algébricos L' tal que $h_{L'} = 1$. Para tratar este problema, é natural usar o "corpo de classes de Hilbert", $H(L)$, uma certa extensão galoisiana

de L com grupo de Galois isomorfo a $\mathcal{G}$. O corpo $H(L)$ tem a propriedade de que todo ideal $\mathfrak{a}$ de I_L se torna principal em $I_{H(L)}$, isto é, $\mathfrak{a} \cdot I_{H(L)}$ é gerado por algum $\alpha \in I_{H(L)}$, embora $I_{H(L)}$ possa ter outros ideais não-principais. Obviamente $H(L) = L$ se e somente se $h_L = 1$. Usando a propriedade de que $K \subseteq K'$ implica $H(K) \cdot K' \subseteq H(K')$ e definindo $H_0(L) = L$, $H_{i+1}(L) = H(H_i(L))$ ($i \in \mathbb{N}$) e $H_\infty(L) = \bigcup_{i \in \mathbb{N}} H_i(L)$, mostramos:

(10.9) Para todo corpo de números algébricos L , as seguintes condições são equivalentes:

- (i) $[H_\infty(L) : L] < \infty$.
- (ii) A cadeia $L = H_0(L) \subseteq H_1(L) \subseteq H_2(L) \subseteq \dots$ é estacionária.
- (iii) Existe uma extensão finita L' de L tal que $h_{L'} = 1$.

Neste caso, $H_\infty(L)$ é a menor extensão L' de L tal que $h_{L'} = 1$.

Demonstração. (i) $\Rightarrow$ (ii) é óbvio.

(ii) $\Rightarrow$ (iii): Existe $m \in \mathbb{N}$ tal que $H_m(L) = H_{m+1}(L) = \dots = H_\infty(L)$. Seja $L' = H_\infty(L)$; então $H(L') = L'$, logo $h_{L'} = 1$.

(iii) $\Rightarrow$ (i): Por indução, podemos supor que $H_{j-1}(L) \subseteq L'$ para algum $j > 0$. Como $h_{L'} = 1$, temos que $H(L') = L'$; logo

$$H_j(L) \subseteq H_j(L) \cdot L' = H(H_{j-1}(L)) \cdot L' \subseteq H(L') = L'.$$

Concluimos que $H_\infty(L) \subseteq L'$, e que $H_\infty(L)$ é a menor extensão L' de L tal que $h_{L'} = 1$. $\square$

A proposição (10.9) mostra que o problema acima indicado é equivalente à questão de, para todo corpo de números algébricos L , a "torre de corpos de classes" $H_0(L) \subseteq H_1(L) \subseteq H_2(L) \subseteq \dots$ ser finita, e mostra ainda que, no caso afirmativo, esta torre fornece a menor extensão L' de L com $h_{L'} = 1$.

A resposta a este "problema de torres de corpos de classes", encontrada por Shafarevich e Golod em 1964, é negativa: Existem até corpos quadráticos L , por exemplo

$$\mathbb{Q}(\sqrt{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19}) \quad \text{e} \quad \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13}),$$

cujas torres de corpos de classes é infinita, ou seja, que não estão contidos em nenhum corpo de números algébricos L' com $h_{L'} = 1$. (Veja Roquette [29]).

EXERCÍCIOS

10.1. Seja $[L : \mathbb{Q}] = n$ e seja $\mathfrak{a}$ um ideal não-nulo de I_L tal que $\mathfrak{N}\mathfrak{a} = k$. Prove que $\mathfrak{a}$ será um ideal principal se e somente se $\mathfrak{a} \in \{R \cdot \alpha_1, \dots, R \cdot \alpha_m\}$, sendo $\alpha_1, \dots, \alpha_m \in I_L$ os elementos indicados no teorema (1.17).

10.2. Prove que os seguintes corpos quadráticos têm número de classes iguais a 1:

$$\mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163}).$$

10.3. Mostre que $\mathbb{Q}(\sqrt{10})$ tem número de classes igual a 2.

10.4. Mostre que o quinto corpo ciclotômico tem número de classes igual a 1.

10.5. a) Prove que todo corpo cúbico L tal que $|d_L| < 49$ tem número de classes igual a 1.

b) Prove que todo corpo cúbico totalmente real (isto é, com três isomorfismos distintos em $\mathbb{R}$) tal que $|d_L| < 81$ tem número de classes igual a 1.

10.6. Seja $L = \mathbb{Q}(\beta)$, sendo β uma raiz do polinômio $X^3 + X^2 - 2X + 8$.

a) Prove que $\mu_L < 7$ e que todo ideal primo não-nulo $\mathfrak{p}$ de I_L com $\mathfrak{N}\mathfrak{p} < 7$ é principal.

b) Conclua que I_L é um domínio principal. (Veja Weiss [37], 5.4.8.)

EXTENSÕES DE
DOMÍNIOS DE DEDEKIND

Usando-se a norma de ideais, foi mostrado no §9 que, para todo número primo p e todo corpo de números algébricos L , a fatoração de $p \cdot I_L = \mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r}$, em potências de ideais primos distintos $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ de I_L , satisfaz a igualdade fundamental $\sum_{i=1}^r e_i \cdot f_i = [L:\mathbb{Q}]$, onde $f_i = [I_L/\mathfrak{P}_i : \mathbb{F}_p]$.

O objetivo principal deste capítulo é generalizar esta igualdade para ideais primos $\mathfrak{p}$ de um domínio de Dedekind arbitrário R e para a extensão $S = I_L(R)$ de R , onde L é qualquer extensão finita e separável do corpo $K = Q(R)$. Isto será feito no §12, usando-se alguns fatos sobre anéis de frações, que serão apresentados no §11. Sob uma hipótese adicional, a saber, a da existência de um elemento $\beta \in S$ tal que $S = R[\beta]$, mostraremos no §13 que a fatoração de $\mathfrak{p} \cdot S$ em ideais primos $\mathfrak{P}_i$ de S pode ser obtida através da fatoração mod $\mathfrak{p} \cdot R[X]$ do polinômio minimal de β sobre K , a qual permite também indicar explicitamente os ideais primos $\mathfrak{P}_i$. Será provado também, sem esta hipótese, um resultado análogo, válido para quase todos os ideais primos de R , excluindo-se apenas os que dividem o discriminante; somente estes podem ser ramificados em L . Finalmente, serão estudados os ideais primos que são totalmente ramificados em L .

§11. Anéis de frações de um domínio

Inicialmente, indicamos alguns fatos sobre extensão e restrição de ideais, para qualquer par de anéis R, S com $R \subseteq S$.

Sejam S um anel qualquer e R um subanel de S . Denotamos por $\mathcal{I}$ (respectivamente $\mathcal{J}$) o conjunto de todos os ideais de R (respectivamente de S). Associando a cada $\alpha \in \mathcal{I}$ o ideal

$$\alpha \cdot S = \{a_1 \cdot \gamma_1 + \dots + a_s \cdot \gamma_s \mid a_1, \dots, a_s \in \alpha; \gamma_1, \dots, \gamma_s \in S; s \in \mathbb{N}\}.$$

obtemos uma aplicação $\varepsilon : \mathcal{J} \rightarrow \mathcal{J}$, chamada a *extensão de ideais* (de R a S), a qual obviamente satisfaz

$$\varepsilon(a + a') = \varepsilon a + \varepsilon a' \quad \text{e} \quad \varepsilon(a \cdot a') = \varepsilon a \cdot \varepsilon a' \quad (a, a' \in \mathcal{J}).$$

O subconjunto $\varepsilon(\mathcal{J})$ de $\mathcal{J}$ é chamado o conjunto dos *ideais estendidos*. Por outro lado, associando a cada $\mathfrak{A} \in \mathcal{J}$ a interseção $\mathfrak{A} \cap R$, obtemos uma aplicação $\rho : \mathcal{J} \rightarrow \mathcal{J}$, chamada a *restrição de ideais* (de S a R), a qual obviamente satisfaz

$$\rho(\mathfrak{A} \cap \mathfrak{A}') = \rho \mathfrak{A} \cap \rho \mathfrak{A}' \quad \text{e} \quad \rho(\sqrt{\mathfrak{A}}) = \sqrt{\rho \mathfrak{A}} \quad (\mathfrak{A}, \mathfrak{A}' \in \mathcal{J}).$$

O subconjunto $\rho(\mathcal{J})$ de $\mathcal{J}$ é chamado o conjunto dos *ideais restritos*.

É óbvio que as aplicações ε e ρ preservam a inclusão e têm as seguintes propriedades:

$$(\rho \circ \varepsilon)a \supseteq a \quad \text{e} \quad [(\rho \circ \varepsilon)a = a \Leftrightarrow a \in \rho(\mathcal{J})] \quad (a \in \mathcal{J})$$

$$(\varepsilon \circ \rho)\mathfrak{A} \subseteq \mathfrak{A} \quad \text{e} \quad [(\varepsilon \circ \rho)\mathfrak{A} = \mathfrak{A} \Leftrightarrow \mathfrak{A} \in \varepsilon(\mathcal{J})] \quad (\mathfrak{A} \in \mathcal{J})$$

$$\varepsilon \circ \rho \circ \varepsilon = \varepsilon \quad \text{e} \quad \rho \circ \varepsilon \circ \rho = \rho$$

$$\varepsilon \text{ injetiva} \Leftrightarrow [\rho \circ \varepsilon = \text{id}_{\mathcal{J}}] \Leftrightarrow \rho \text{ sobrejetiva}$$

$$\varepsilon \text{ sobrejetiva} \Leftrightarrow [\varepsilon \circ \rho = \text{id}_{\mathcal{J}}] \Leftrightarrow \rho \text{ injetiva}$$

ε e ρ induzem aplicações bijetivas, inversas entre si, entre os conjuntos $\rho(\mathcal{J})$ e $\varepsilon(\mathcal{J})$.

Como exemplos triviais, mencionamos os seguintes:

- A) Seja R um corpo e $S = R[X]$. Como $\mathcal{J}$ consiste apenas dos ideais (0) e R , a aplicação ρ é sobrejetiva e ε é injetiva.
 B) Seja R um domínio e $S = Q(R)$ o corpo de frações de R . Como $\mathcal{J}$ consiste apenas dos ideais (0) e S , a aplicação ε é sobrejetiva e ρ é injetiva.

Mostraremos a seguir que a afirmação em B) se generaliza ao caso de qualquer anel de frações de um domínio R .

Seja M um subconjunto multiplicativo do domínio R . Denotaremos, até (11.8), por $\mathcal{J}$ (respectivamente $\mathcal{J}$) o conjunto dos ideais de R (respectivamente R_M).

(11.1) a) Para todo $\mathfrak{A} \in \mathcal{J}$ temos que $(\mathfrak{A} \cap R) \cdot R_M = \mathfrak{A}$.

b) Para todo $a \in \mathcal{J}$ temos que $a \cdot R_M = \{a/m \mid a \in a, m \in M\}$; em particular, $a \cdot R_M = R_M$ se e somente se $a \cap M \neq \emptyset$.

Demonstração. a) Seja $\alpha \in \mathfrak{A}$, digamos $\alpha = c/m$, com $c \in R$, $m \in M$. Então, $m \cdot \alpha = c \in \mathfrak{A} \cap R$, logo $\alpha = c \cdot (1/m) \in (\mathfrak{A} \cap R) \cdot R_M$.

b) A primeira igualdade resulta do fato que, para quaisquer $a_i \in a$, $b_i \in R$ e $m_i \in M$ ($i = 1, \dots, s$), vale

$$\sum_{i=1}^s a_i \cdot (b_i/m_i) = a/m, \text{ onde } m = m_1 \cdot \dots \cdot m_s \in M \text{ e}$$

$$a = \sum_{i=1}^s a_i \cdot b_i \cdot m_1 \cdot \dots \cdot m_{i-1} \cdot m_{i+1} \cdot \dots \cdot m_s \in a.$$

Se $a \cdot R_M = R_M$, então existem $a \in a$ e $m \in M$ tais que $a/m = 1$, logo $a = m \in a \cap M$. Por outro lado, se $m \in a \cap M$ então $1 = m/m \in a \cdot R_M$. $\square$

Diremos que o ideal $a \in \mathcal{I}$ se perde em R_M quando $a \cdot R_M = R_M$. A parte b) da proposição (11.1) mostra que, no caso em que $M \notin U(R)$ (ou seja, $R_M \neq R$), existem sempre ideais a de R , distintos de R , que se perdem em R_M ; portanto, a aplicação ε não é injetiva.

A seguir mostraremos que os ideais primos de R_M estão em correspondência biunívoca com os ideais primos de R que não se perdem em R_M . Mais precisamente, denotando por $\mathcal{P}$ (respectivamente $\mathcal{Q}$) o conjunto de todos os ideais primos de R (respectivamente de R_M), e por $\mathcal{P}_M$ o conjunto $\{p \in \mathcal{P} \mid p \cap M = \phi\}$, provamos:

(11.2) TEOREMA. a) Para todo $\mathfrak{P} \in \mathcal{Q}$ temos que $\mathfrak{P} \cap R \in \mathcal{P}_M$ e $(\mathfrak{P} \cap R) \cdot R_M = \mathfrak{P}$.

b) Para todo $p \in \mathcal{P}_M$ temos que $p \cdot R_M \in \mathcal{Q}$ e $p \cdot R_M \cap R = p$.

c) As aplicações ε e ρ induzem aplicações bijetivas, inversas entre si, entre $\mathcal{P}_M$ e $\mathcal{Q}$.

Demonstração. a) Obviamente $\mathfrak{P} \cap R \in \mathcal{P}$ para qualquer $\mathfrak{P} \in \mathcal{Q}$. Por (11.1) temos que $(\mathfrak{P} \cap R) \cdot R_M = \mathfrak{P} \neq R_M$, logo $(\mathfrak{P} \cap R) \cap M = \phi$; portanto $\mathfrak{P} \cap R \in \mathcal{P}_M$.

b) Seja $p \in \mathcal{P}_M$; então $p \cdot R_M \neq R_M$. Para mostrar que $p \cdot R_M \in \mathcal{Q}$, consideramos elementos $a, b \in R$ e $m, n \in M$ tais que $(a/m) \cdot (b/n) \in p \cdot R_M$. Por (11.1b) existem $c \in p$ e $k \in M$ tais que $(a/m) \cdot (b/n) = c/k$; logo $a \cdot b \cdot k = m \cdot n \cdot c \in p$, e de $k \notin p$ decorre que $a \in p$ ou $b \in p$; portanto $a/m \in p \cdot R_M$ ou $b/n \in p \cdot R_M$. Todo $d \in p \cdot R_M \cap R$ é da forma c/m , onde $c \in p$ e $m \in M$, logo $m \cdot d = c$; de $m \notin p$ decorre que $d \in p$. Portanto, $p \cdot R_M \cap R = p$.

c) é uma consequência de a) e b). $\square$

É óbvio que, para todo $a \in \mathcal{I}$, a aplicação idêntica $R \rightarrow R_M$ induz um homomorfismo canônico de R/a em $R_M/a \cdot R_M$, o qual será injetivo se e somente se $a \cdot R_M \cap R = a$. Em particular:

(11.3) COROLÁRIO. Para todo $\mathfrak{p} \in \mathcal{P}_M$, o homomorfismo canônico $R/\mathfrak{p} \rightarrow R_M/\mathfrak{p} \cdot R_M$ é injetivo. Ele será bijetivo (e, portanto, um isomorfismo de $R/\mathfrak{p}$ sobre $R_M/\mathfrak{p} \cdot R_M$) quando $\mathfrak{p}$ for um ideal maximal.

Demonstração. A primeira afirmação resulta de (11.2 b). Se $\mathfrak{p} \in \mathcal{P}_M$ for um ideal maximal, então para todo $m \in M$ existem $c \in \mathfrak{p}$ e $a \in R$ tais que $1 = c + a \cdot m$; logo $1/m - a = c/m \in \mathfrak{p} \cdot R_M$. Resulta que, para todo $r \in R$, $r/m + \mathfrak{p} \cdot R_M$ é a imagem de $r \cdot a + \mathfrak{p}$ sob o homomorfismo indicado. $\square$

Em particular, para todo número primo p , o corpo $\mathbb{F}_p = \mathbb{Z}/p \cdot \mathbb{Z}$ é canonicamente isomorfo ao corpo $\mathbb{Z}_{(p)}/p \cdot \mathbb{Z}_{(p)}$, sendo $\mathbb{Z}_{(p)}$ a localização de $\mathbb{Z}$ pelo ideal maximal $p \cdot \mathbb{Z}$ de $\mathbb{Z}$.

Consideremos ainda o caso especial em que $M = R \setminus \mathfrak{p}_0$ para algum $\mathfrak{p}_0 \in \mathcal{P}$, ou seja, em que R_M é a localização de R em relação ao ideal primo $\mathfrak{p}_0$. Neste caso, os ideais de R que não se perdem em R_M são exatamente os contidos em $\mathfrak{p}_0$, e temos que $\mathcal{P}_M = \{\mathfrak{p} \in \mathcal{P} \mid \mathfrak{p} \subseteq \mathfrak{p}_0\}$. Obtemos como consequência imediata de (11.2) o seguinte

(11.4) COROLÁRIO. Seja $M = R \setminus \mathfrak{p}_0$, onde $\mathfrak{p}_0 \in \mathcal{P}$. Sob as aplicações ϵ e ρ , os ideais primos de R_M correspondem biunivocamente aos ideais primos de R que estão contidos em $\mathfrak{p}_0$. Em particular, $\mathfrak{p}_0 \cdot R_M$ é o único ideal maximal de R_M .

A seguir mostraremos que a construção do anel de frações comuta com a construção do fecho inteiro, no sentido do seguinte teorema, que generaliza a segunda igualdade de (1.7).

(11.5) TEOREMA. Sejam S um domínio, R um subanel de S e M um subconjunto multiplicativo de R . Então

$$I_S(R)_M = I_{S_M}(R_M).$$

Demonstração. Todo $s \in R' = I_S(R)$ satisfaz uma igualdade $s^k + a_1 \cdot s^{k-1} + \dots + a_k = 0$, com $a_1, \dots, a_k \in R$, $k \in \mathbb{N}$; logo $(s/m)^k + (a_1/m) \cdot (s/m)^{k-1} + \dots + a_k/m^k = 0$ para qualquer $m \in M$. Portanto, todo elemento de R'_M está em S_M e é inteiro sobre R_M ; logo $R'_M \subseteq I_{S_M}(R_M)$. Por outro lado, sejam $s \in S$ e $m \in M$ e suponhamos que s/m seja inteiro sobre R_M ; digamos $(s/m)^\ell + (b_1/m_1) \cdot (s/m)^{\ell-1} + \dots + b_\ell/m_\ell = 0$, onde $b_1, \dots, b_\ell \in R$, $m_1, \dots, m_\ell \in M$ e $\ell \in \mathbb{N}$. Multiplicando esta igualdade por $(m \cdot n)^\ell$, onde $n = m_1 \cdot \dots \cdot m_\ell$, obtemos que $(s \cdot n)^\ell + c_1 \cdot (s \cdot n)^{\ell-1} + \dots + c_\ell = 0$, com $c_1, \dots, c_\ell \in R$; logo $s \cdot n \in I_S(R) = R'$, e $s/m = (s \cdot n)/(m \cdot n) \in R'_M$. $\square$

Obtemos como consequência imediata o seguinte:

(11.6) COROLÁRIO. *Sejam S , R e M como em (11.5).*

- a) *Se S for inteiro sobre R então S_M será inteiro sobre R_M .*
- b) *Se R for integralmente fechado em S então R_M será integralmente fechado em S_M .*

Há outras propriedades importantes que se preservam na passagem de R ao anel de frações R_M :

(11.7) *Se R for um domínio noetheriano então todo anel de frações de R também o será.*

Demonstração. Para todo $\mathfrak{A} \in \mathcal{J}$, o ideal $\mathfrak{A} \cap R \in \mathcal{J}$ é finitamente gerado, digamos $\mathfrak{A} \cap R = R \cdot a_1 + \dots + R \cdot a_r$; logo $\mathfrak{A} = (\mathfrak{A} \cap R) \cdot R_M = R_M \cdot a_1 + \dots + R_M \cdot a_r$ é finitamente gerado. $\square$

(11.8) TEOREMA. *Sejam R um domínio de Dedekind e M um subconjunto multiplicativo de R ; então:*

- a) *R_M é um domínio de Dedekind.*

Além disto, para todo ideal primo não-nulo $\mathfrak{p}$ de R tal que $\mathfrak{p} \cap M = \emptyset$, temos que

- b) *os corpos $R/\mathfrak{p}$ e $R_M/\mathfrak{p} \cdot R_M$ são canonicamente isomorfos;*
- c) *$\mathfrak{p}^k \cdot R_M \cap R = \mathfrak{p}^k$ para todo $k \in \mathbb{N}$.*

Demonstração. a) R_M é noetheriano e integralmente fechado, por (11.7) e (11.6 b). Seja $\mathfrak{P} \in \mathcal{L}$, $\mathfrak{P} \neq (0)$. Por (11.2), $\mathfrak{P} \cap R$ é um ideal primo não-nulo e, portanto, um ideal maximal de R ; logo $\mathfrak{P}$ é um ideal maximal de R_M . Concluímos que R_M é um domínio de Dedekind.

b) Resulta de (11.3).

c) Seja $a \in \mathfrak{p}^k \cdot R_M \cap R$; por (11.1 b) existem $b \in \mathfrak{p}^k$ e $m \in M$ tais que $a = b/m$; logo $m \cdot a = b$. Como $\mathfrak{p}^k$ divide o ideal $b \cdot R$ e $\mathfrak{p}$ não divide $m \cdot R$, resulta de (8.8) que $\mathfrak{p}^k$ divide o ideal $a \cdot R$, logo $a \in \mathfrak{p}^k$. A inclusão inversa é óbvia. $\square$

As localizações de um domínio de Dedekind são até domínios principais. Este fato, indicado no seguinte corolário, será da maior importância nos parágrafos 12 e 13.

(11.9) COROLÁRIO. *Sejam R um domínio de Dedekind, $\mathfrak{p}_0$ um ideal primo não-nulo de R e $M = R \setminus \mathfrak{p}_0$. Então, R_M é um domínio principal, tendo um único ideal primo não-nulo, a saber, $\mathfrak{p}_0 \cdot R_M$.*

Demonstração. Por (11.4) e (11.8), $p_0 \cdot R_M$ é o único ideal maximal do domínio de Dedekind R_M e, portanto, seu único ideal primo não-nulo. Por (8.17), R_M é um domínio principal. $\square$

Observemos que o anel R_M considerado em (11.9) é um anel de valorização discreta, isto é, satisfaz as condições equivalentes indicadas no Exercício 8.12.

A noção de anel de frações é útil para estudar o relacionamento entre os ideais primos de R e os de S , no caso em que S for inteiro sobre R . Dado um ideal primo p de R , diremos que um ideal primo $\mathfrak{P}$ de S está acima de p quando $\mathfrak{P} \cap R = p$. Mais geralmente, denotando por $\mathcal{J}$ o conjunto de todos os ideais de S , interessamo-nos pelos $\mathfrak{A} \in \mathcal{J}$ tais que $\mathfrak{A} \cap R \subseteq p$.

(11.10) TEOREMA. *Sejam S um domínio, R um subanel de S tal que S seja inteiro sobre R , e p um ideal primo de R .*

- Para todo $\mathfrak{A} \in \mathcal{J}$ tal que $\mathfrak{A} \cap R \subseteq p$ existe um ideal primo $\mathfrak{P}$ de S , acima de p , tal que $\mathfrak{A} \subseteq \mathfrak{P}$.*
- Os ideais primos $\mathfrak{P}$ de S que estão acima de p são os elementos maximais do conjunto $\{\mathfrak{A} \in \mathcal{J} \mid \mathfrak{A} \cap R \subseteq p\}$.*

Demonstração. Seja $M = R \setminus p$. Notemos que $\mathfrak{A} \in \mathcal{J}$, $\mathfrak{A} \cap R \subseteq p$ implica que $\mathfrak{A} \cap M = \emptyset$, logo $\mathfrak{A} \cdot S_M \neq S_M$.

a) $\mathfrak{A} \cdot S_M$ está contido num ideal maximal $\mathfrak{N}$ de S_M . Como S_M é inteiro sobre R_M , por (11.6), resulta de (1.12 d) que $\mathfrak{N} \cap R_M$ é um ideal maximal de R_M ; logo coincide com $p \cdot R_M$. Concluimos que $\mathfrak{A} \subseteq \mathfrak{A} \cdot S_M \cap S \subseteq \mathfrak{N} \cap S$ e $(\mathfrak{N} \cap S) \cap R = (\mathfrak{N} \cap R_M) \cap R = p \cdot R_M \cap R = p$; portanto, o ideal primo $\mathfrak{P} = \mathfrak{N} \cap S$ de S tem as propriedades desejadas.

b) Seja $\mathfrak{P}$ um ideal primo de S que esteja acima de p . Então, $\mathfrak{P} \cdot S_M \neq S_M$, $p \cdot R_M \subseteq \mathfrak{P} \cdot S_M \cap R_M \neq R_M$, e vale a igualdade devido à maximalidade do ideal $p \cdot R_M$. Por (1.12 d), $\mathfrak{P} \cdot S_M$ é um ideal maximal de S_M . Suponhamos que $\mathfrak{P} \subseteq \mathfrak{A}$ para algum $\mathfrak{A} \in \mathcal{J}$ tal que $\mathfrak{A} \cap R \subseteq p$. Então $\mathfrak{P} \cdot S_M \subseteq \mathfrak{A} \cdot S_M \neq S_M$, e vale a igualdade devido à maximalidade de $\mathfrak{P} \cdot S_M$; portanto $\mathfrak{A} \subseteq \mathfrak{A} \cdot S_M \cap S = \mathfrak{P} \cdot S_M \cap S = \mathfrak{P}$. Resulta que $\mathfrak{P}$ é maximal no conjunto $\{\mathfrak{A} \in \mathcal{J} \mid \mathfrak{A} \cap R \subseteq p\}$. Por outro lado, se $\mathfrak{A}_0$ for um elemento maximal deste conjunto, então, por a), $\mathfrak{A}_0$ estará contido em, e pela maximalidade será mesmo igual a, um ideal primo $\mathfrak{P}$ de S acima de p . $\square$

Como consequência imediata deste teorema obtemos:

(11.11) COROLÁRIO. Sejam S , R e $\mathfrak{p}$ como em (11.10).

- a) Existe um ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$.
- b) Se $\mathfrak{P}_1, \mathfrak{P}_2$ forem ideais primos de S , acima de $\mathfrak{p}$ e tais que $\mathfrak{P}_1 \subseteq \mathfrak{P}_2$, então $\mathfrak{P}_1 = \mathfrak{P}_2$.
- c) Sejam $\mathfrak{p}_0$ e $\mathfrak{P}_0$ ideais primos de R e S , respectivamente, tais que $\mathfrak{P}_0$ esteja acima de $\mathfrak{p}_0$ e $\mathfrak{p}_0 \subseteq \mathfrak{p}$. Então existe um ideal primo $\mathfrak{P}$ de S , acima de $\mathfrak{p}$, tal que $\mathfrak{P}_0 \subseteq \mathfrak{P}$.

As afirmações a) e c) deste corolário costumam ser chamadas o teorema “lying-over” e “going-up”, respectivamente, enquanto b) afirma que os ideais primos de S acima de $\mathfrak{p}$ são incomparáveis dois a dois (em relação à inclusão).

Do teorema “lying-over” resulta, em particular, que todo ideal primo $\mathfrak{p}$ é um ideal restrito (isto é, $\mathfrak{p} = \mathfrak{U} \cap R$ para algum $\mathfrak{U} \in \mathcal{J}$) e, portanto, $\mathfrak{p} = \mathfrak{p} \cdot S \cap R$. Além disto, concluímos de (11.10):

(11.12) COROLÁRIO. Sejam S , R e $\mathfrak{p}$ como em (11.10). Então $\mathfrak{p} \cdot S$ é o menor elemento, e os ideais primos $\mathfrak{P}$ de S acima de $\mathfrak{p}$ são os elementos maximais, do conjunto $\{\mathfrak{U} \in \mathcal{J} \mid \mathfrak{U} \cap R = \mathfrak{p}\}$.

EXERCÍCIOS

- 11.1. Sejam S um anel, R um subanel de S e $\mathcal{J}$ (respectivamente $\mathcal{J}$) o conjunto dos ideais de R (respectivamente de S). Sejam $\mathfrak{a}_0 \in \mathcal{J}$ e $\mathfrak{U}_0 \in \mathcal{J}$. Prove:
 - a) Se $\{\mathfrak{U} \in \mathcal{J} \mid \mathfrak{U} \cap R = \mathfrak{a}_0\}$ for não-vazio, então terá um menor elemento, a saber, $\mathfrak{a}_0 \cdot S$.
 - b) Se $\{\mathfrak{a} \in \mathcal{J} \mid \mathfrak{a} \cdot S = \mathfrak{U}_0\}$ for não-vazio, então terá um maior elemento, a saber, $\mathfrak{U}_0 \cap R$.
- 11.2. Sejam S um domínio, R um subanel de S e $\mathfrak{p}$ um ideal primo de R tal que $\mathfrak{p} \cdot S \cap R = \mathfrak{p}$. Usando o anel de frações S_M , onde $M = R \setminus \mathfrak{p}$, prove que existe um ideal primo $\mathfrak{P}$ de S tal que $\mathfrak{P} \cap R = \mathfrak{p}$.
- 11.3. Dê uma demonstração de (11.7), usando a condição de cadeia ascendente (respectivamente a condição maximal).
- 11.4. Sejam R um domínio e $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideais primos de R . Prove:
 - a) $M = R \setminus (\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_r)$ é um subconjunto multiplicativo de R .
 - b) O ideal $\mathfrak{a}$ de R perder-se-á em R_M se e somente se $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ para todo $i = 1, \dots, r$.

- c) Se $p_1, \dots, p_r$ forem incomparáveis dois a dois (isto é, $p_i \nsubseteq p_j$ para $i \neq j$) então R_M terá exatamente r ideais maximais, a saber, $p_1 \cdot R_M, \dots, p_r \cdot R_M$.
- d) Se R for um domínio de Dedekind, então R_M será um domínio principal. Indique um sistema de representantes dos elementos irredutíveis de R .

11.5. Sejam R um anel e M um subconjunto multiplicativo de R .

- a) Defina o anel de frações R_M como quociente do conjunto $R \times M$ pela relação de equivalência

$$(r, m) \sim (r', m') \Leftrightarrow [n \cdot (r \cdot m' - r' \cdot m) = 0 \text{ para algum } n \in M],$$

munido de uma adição e uma multiplicação apropriadas.

- b) Prove que por $r \mapsto r/1$ ($r \in R$) define-se um homomorfismo $\lambda_M: R \rightarrow R_M$, com núcleo $\{r \in R \mid n \cdot r = 0 \text{ para algum } n \in M\}$.
- c) Prove que, para qualquer homomorfismo ϕ de R em um anel S tal que $\phi(M) \subseteq U(S)$, existe um e um só homomorfismo $\bar{\phi}: R_M \rightarrow S$ tal que $\bar{\phi} \circ \lambda_M = \phi$.

11.6. Procure generalizar, para anéis quaisquer, os fatos provados no §11 para domínios. Neste sentido, generalize também os Exercícios 11.2, 11.3, e 11.4. a)-c).

11.7. Seja p um número primo e $m \in \mathbb{Z} \setminus \{0\}$. Prove que $m \cdot \mathbb{Z}_{(p)} \cap \mathbb{Z} = p^k \cdot \mathbb{Z}$, onde $k = \max \{j \in \mathbb{N} \mid p^j \text{ divide } m\}$.

§12. Decomposição de ideais primos

Dados um domínio de Dedekind R e uma extensão finita e separável L do corpo $K = Q(R)$, recordamos que $S = I_L(R)$ também é um domínio de Dedekind (veja (8.1)). Estudaremos neste parágrafo, para os ideais primos não-nulos p de R , a *decomposição de p em L* , isto é, a fatoração do ideal estendido $p \cdot S$ em ideais primos $\mathfrak{P}$ de S .

Lembramos que, no fim do §11, foi estudado o relacionamento entre um ideal primo p de R e os ideais de S , num contexto mais geral, a saber, para quaisquer domínios $R \subseteq S$ tais que S fosse inteiro sobre R . Dos resultados lá obtidos será utilizado aqui apenas o fato de p ser um ideal restrito, que é uma consequência imediata do teorema "lying-over" (11.11a). A partir deste fato daremos uma prova direta das afirmações de (11.12) para domi-

nios de Dedekind, até numa versão reforçada. Mencionemos ainda que, de fato, *todo* ideal de R é restrito, ou seja, a “restrrição” $\rho : \mathcal{J} \rightarrow \mathcal{J}$ é sobrejetiva, o que pode ser provado de várias maneiras (veja Exercícios 12.2 e 12.3).

Sejam R, S, K, L como definidos acima, $n = [L : K]$, $\mathfrak{p}$ um ideal primo não-nulo de R , e $\mathcal{J}$ o conjunto dos ideais de S .

(12.1) *Seja $\mathfrak{p} \cdot S = \mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r}$, sendo $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ ideais primos de S distintos, e $e_1 \geq 1, \dots, e_r \geq 1$. Então:*

- a) $r \geq 1$.
- b) $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ são os ideais primos que estão acima de $\mathfrak{p}$.
- c) $\{\mathfrak{U} \in \mathcal{J} \mid \mathfrak{U} \cap R = \mathfrak{p}\} = \{\mathfrak{P}_1^{d_1} \cdot \dots \cdot \mathfrak{P}_r^{d_r} \mid 0 \leq d_i \leq e_i, (i = 1, \dots, r), d_1 + \dots + d_r \geq 1\}$.

Demonstração. a) Como $\mathfrak{p}$ é um ideal restrito (por (11.11a)), temos que $\mathfrak{p} \cdot S \cap R = \mathfrak{p}$, logo $\mathfrak{p} \cdot S \neq S$; portanto $\mathfrak{p} \cdot S$ é divisível por algum ideal primo $\mathfrak{P}$, isto é, $r \geq 1$.

c) O conjunto à direita consiste dos ideais $\mathfrak{U} \in \mathcal{J}$, $\mathfrak{U} \neq S$, que dividem $\mathfrak{p} \cdot S$. Para todo $\mathfrak{U}$ deste tipo temos que $\mathfrak{p} \subseteq \mathfrak{p} \cdot S \cap R \subseteq \mathfrak{U} \cap R \neq R$; logo $\mathfrak{p} = \mathfrak{U} \cap R$, devido à maximalidade de $\mathfrak{p}$. Por outro lado, de $\mathfrak{U} \cap R = \mathfrak{p}$ decorre que $\mathfrak{U} \neq S$ e $\mathfrak{p} \cdot S = (\mathfrak{U} \cap R) \cdot S \subseteq \mathfrak{U}$, logo $\mathfrak{U}$ divide-se $\mathfrak{p} \cdot S$.

b) é uma consequência imediata de c). $\square$

As afirmações a) e b) desta proposição generalizam obviamente a parte a) do Corolário (9.8)⁽¹⁾. Para podermos generalizar também a parte b) deste Corolário, isto é, a igualdade fundamental, consideramos, para todo ideal $\mathfrak{U}$ de S tal que $\mathfrak{U} \cap R = \mathfrak{p}$, o anel quociente $S/\mathfrak{U}$. Ele pode ser considerado como R -módulo e também como $R/\mathfrak{p}$ -espaço, uma vez que é anulado por $\mathfrak{p}$ (veja (9.1)).

(12.2) *Para todo ideal $\mathfrak{U}$ de S tal que $\mathfrak{U} \cap R = \mathfrak{p}$, o $R/\mathfrak{p}$ -espaço $S/\mathfrak{U}$ tem dimensão finita.*

Demonstração. Por (7.11), S é um R -módulo finitamente gerado. As classes mod $\mathfrak{U}$ de um sistema de geradores deste R -módulo for-

⁽¹⁾ Note-se que, em (9.8), a desigualdade $r \geq 1$ resulta da parte b) (igualdade fundamental) ou pode ser obtida diretamente de $\mathfrak{U}(\mathfrak{p} \cdot R) \neq 1$ ou de (1.12 b).

mam um sistema de geradores do R/p -espaço $S/\mathfrak{A}$ que, portanto, tem dimensão finita. $\square$

A dimensão de um R/p -espaço V será denotada por $\dim V$.

Mencionemos ainda que R/p pode ser identificado com a imagem de R sob o homomorfismo canônico de S sobre $S/\mathfrak{A}$ e, portanto, pode ser considerado como subcorpo do anel $S/\mathfrak{A}$. Em particular, para cada ideal primo $\mathfrak{P}$ de S que está acima de p , o corpo $S/\mathfrak{P}$ pode ser considerado como uma extensão do corpo R/p , de grau $[S/\mathfrak{P} : R/p] = \dim S/\mathfrak{P}$, o qual é chamado *grau de inércia* de $\mathfrak{P}$ e é denotado por $f(\mathfrak{P} | p)$. O maior número e tal que $\mathfrak{P}^e$ divida $p \cdot S$ é chamado o *índice de ramificação* de $\mathfrak{P}$ e é denotado por $e(\mathfrak{P} | p)$. Com as notações de (12.1) temos obviamente que $e(\mathfrak{P}_i | p) = e_i$ ($i = 1, \dots, r$).

A igualdade fundamental $\sum_{i=1}^r e_i \cdot f_i = n$ será obtida através de duas igualdades para $\dim S/p \cdot S$, indicadas no seguinte teorema. A segunda igualdade será inicialmente demonstrada sob a hipótese de S ser um R -módulo livre, hipótese esta que posteriormente será eliminada, usando-se o método de localização, isto é, a passagem aos anéis de frações R_M e S_M , onde $M = R \setminus p$. Note-se que a hipótese mencionada é sempre satisfeita no caso em que $R = \mathbb{Z}$, devido a (5.6), de modo que, neste caso, não há necessidade de localização.

(12.3) TEOREMA. *Sejam R um domínio de Dedekind, $S = I_L(R)$, onde L é uma extensão finita e separável de $K = Q(R)$, p um ideal primo não-nulo de R e $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ os ideais primos de S que estão acima de p . Então*

$$\sum_{i=1}^r e(\mathfrak{P}_i | p) \cdot f(\mathfrak{P}_i | p) = \dim S/p \cdot S = [L : K].$$

Demonstração. a) Sendo $e_i = e(\mathfrak{P}_i | p)$, consideramos a seguinte cadeia de ideais descendente:

$$S \supset \mathfrak{P}_1 \supset \dots \supset \mathfrak{P}_1^{e_1} \supset \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2 \supset \dots \supset \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \supset \dots \supset \mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r} = p \cdot S.$$

Seja $\mathfrak{A}$ um ideal desta cadeia, menos o último; então o ideal seguinte é $\mathfrak{A} \cdot \mathfrak{P}_i$ para certo $i \in \{1, \dots, r\}$. Por (9.2), $\mathfrak{A}/\mathfrak{A} \cdot \mathfrak{P}_i$ é um $S/\mathfrak{P}_i$ -espaço de dimensão 1 e, portanto, um R/p -espaço de dimensão $f(\mathfrak{P}_i | p)$. Sendo

$S/\mathfrak{A}$ e $S/\mathfrak{A} \cdot \mathfrak{P}_i$ $R/\mathfrak{p}$ -espaços de dimensão finita, por (12.2), temos que $\dim S/\mathfrak{A} \cdot \mathfrak{P}_i - \dim S/\mathfrak{A} = \dim \mathfrak{A}/\mathfrak{A} \cdot \mathfrak{P}_i = f(\mathfrak{P}_i | \mathfrak{p})$, uma vez que $S/\mathfrak{A}$ é isomorfo a $(S/\mathfrak{A} \cdot \mathfrak{P}_i)/(\mathfrak{A}/\mathfrak{A} \cdot \mathfrak{P}_i)$. Somando estas igualdades, onde $\mathfrak{A}$ percorre todos os ideais da cadeia menos o último, obtemos a primeira igualdade do teorema.

b) Provaremos a segunda igualdade sob a hipótese de que o R -módulo S , o qual tem posto n (veja §5), é livre, isto é, possui uma base $\beta_1, \dots, \beta_n$. Denotando por κ o homomorfismo canônico de S sobre $S/\mathfrak{p} \cdot S$, temos que $\kappa\beta_1, \dots, \kappa\beta_n$ formam um sistema de geradores do $R/\mathfrak{p}$ -espaço $S/\mathfrak{p} \cdot S$; afirmamos que estes elementos são linearmente independentes. De fato, sejam $a_1, \dots, a_n \in R$ tais que $\sum_{i=1}^n \kappa a_i \cdot \kappa\beta_i = 0$, então

$$\sum_{i=1}^n a_i \cdot \beta_i \in \mathfrak{p} \cdot S; \text{ logo existem } m \in \mathbb{N}, c_j \in \mathfrak{p} \text{ e } b_{j,i} \in R (i = 1, \dots, n; j = 1, \dots, m)$$

tais que $\sum_{i=1}^n a_i \cdot \beta_i = \sum_{j=1}^m c_j \cdot \left(\sum_{i=1}^n b_{j,i} \cdot \beta_i \right)$. Da independência linear de

$\beta_1, \dots, \beta_n$ concluímos que $a_i = \sum_{j=1}^m c_j \cdot b_{j,i} \in \mathfrak{p}$, logo $\kappa a_i = 0$ ($i = 1, \dots, n$).

Resulta que $\kappa\beta_1, \dots, \kappa\beta_n$ é uma base de $R/\mathfrak{p}$ -espaço $S/\mathfrak{p} \cdot S$; assim $\dim S/\mathfrak{p} \cdot S = n$.

c) Para provar a segunda igualdade do teorema no caso geral, consideramos os anéis de frações R_M e S_M , onde $M = R \setminus \mathfrak{p}$. Obviamente $K = Q(R_M)$, $L = Q(S_M)$, e temos que $S_M = I_L(R_M)$, por (11.5). Por (11.9), R_M é um domínio principal, tendo $\mathfrak{p} \cdot R_M$ como único ideal primo não-nulo; de (5.4) resulta que o R_M -módulo S_M é livre. Da proposição (12.4), que será indicada e provada em seguida, concluímos que $\mathfrak{P}_1 \cdot S_M, \dots, \mathfrak{P}_r \cdot S_M$ são os ideais primos de S_M que estão acima de $\mathfrak{p} \cdot R_M$ e que $e(\mathfrak{P}_i \cdot S_M | \mathfrak{p} \cdot R_M) = e(\mathfrak{P}_i | \mathfrak{p})$ e $f(\mathfrak{P}_i \cdot S_M | \mathfrak{p} \cdot R_M) = f(\mathfrak{P}_i | \mathfrak{p})$ ($i = 1, \dots, r$).

Pelo que foi demonstrado anteriormente, concluímos que

$$\begin{aligned} [L : K] &= d_M = \sum_{i=1}^r e_i(\mathfrak{P}_i \cdot S_M | \mathfrak{p} \cdot R_M) \cdot f_i(\mathfrak{P}_i \cdot S_M | \mathfrak{p} \cdot R_M) = \\ &= \sum_{i=1}^r e(\mathfrak{P}_i | \mathfrak{p}) \cdot f(\mathfrak{P}_i | \mathfrak{p}) = \dim S/\mathfrak{p} \cdot S, \end{aligned}$$

sendo d_M a dimensão do $(R_M/\mathfrak{p} \cdot R_M)$ -espaço $S_M/\mathfrak{p} \cdot S_M$. $\square$

A prova deste teorema será completa após demonstrarmos o seguinte:

(12.4) Com as notações de (12.1) e $M = R/\mathfrak{p}$ temos:

- a) $\mathfrak{p} \cdot S_M = (\mathfrak{P}_1 \cdot S_M)^{e_1} \cdot \dots \cdot (\mathfrak{P}_r \cdot S_M)^{e_r}$ sendo $\mathfrak{P}_1 \cdot S_M, \dots, \mathfrak{P}_r \cdot S_M$ os ideais primos de S_M , distintos, acima de $\mathfrak{p} \cdot R_M$.
- b) A aplicação idêntica $S \rightarrow S_M$ induz, para $i = 1, \dots, r$, um isomorfismo de $S/\mathfrak{P}_i$ sobre $S_M/\mathfrak{P}_i \cdot S_M$, sob o qual $R/\mathfrak{p}$ é aplicado sobre $R_M/\mathfrak{p} \cdot R_M$.
- c) $e(\mathfrak{P}_i \cdot S_M | \mathfrak{p} \cdot R_M) = e(\mathfrak{P}_i | \mathfrak{p})$ e $f(\mathfrak{P}_i \cdot S_M | \mathfrak{p} \cdot R_M) = f(\mathfrak{P}_i | \mathfrak{p})$ ($i = 1, \dots, r$).

Demonstração. a) Como $\mathfrak{P}_1 \cap M = \dots = \mathfrak{P}_r \cap M = \phi$, resulta de (11.2) que $\mathfrak{P}_1 \cdot S_M, \dots, \mathfrak{P}_r \cdot S_M$ são ideais primos de S_M distintos. Da multiplicatividade da extensão de ideais concluímos que $\mathfrak{p} \cdot S_M = (\mathfrak{p} \cdot S) \cdot S_M = (\mathfrak{P}_1 \cdot S_M)^{e_1} \cdot \dots \cdot (\mathfrak{P}_r \cdot S_M)^{e_r}$. O resto resulta de (12.1), aplicado aos anéis R_M e $S_M = I_L(R_M)$.

b) Resulta de (11.3) e do fato de $\mathfrak{p}$ e $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ serem ideais maximais de R e S , respectivamente.

c) É uma consequência imediata de a) e b). $\square$

Mencionemos ainda que, pela versão fraca do Teorema Chinês de Restos (6.7), existe um isomorfismo canônico de $S/\mathfrak{p} \cdot S = S/(\mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r})$ sobre o produto cartesiano $S/\mathfrak{P}_1^{e_1} \times \dots \times S/\mathfrak{P}_r^{e_r}$, o qual induz a aplicação diagonal de $R/\mathfrak{p}$ sobre $R/\mathfrak{p} \times \dots \times R/\mathfrak{p}$. Considerado como $R/\mathfrak{p}$ -espaço, $S/\mathfrak{P}_i^{e_i}$ tem a dimensão $e(\mathfrak{P}_i | \mathfrak{p}) \cdot f(\mathfrak{P}_i | \mathfrak{p})$, o que se prova analogamente à parte a) da demonstração de (12.3). Desta maneira, obtém-se novamente a primeira igualdade do teorema (12.3).

Observemos ainda que a igualdade fundamental permite vários tipos de decomposição de $\mathfrak{p}$; convém dar nomes aos casos extremos. Diremos que o ideal primo $\mathfrak{p}$ de R é

- a) *totalmente decomposto* em L , quando $r = n$, ou seja, $e(\mathfrak{P} | \mathfrak{p}) = f(\mathfrak{P} | \mathfrak{p}) = 1$ para todo ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$.
- b) *totalmente inerte* em L , quando $r = 1$ e $e(\mathfrak{P}_1 | \mathfrak{p}) = 1$, ou seja, $f(\mathfrak{P} | \mathfrak{p}) = n$ para algum ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$.
- c) *totalmente ramificado* em L , quando $r = 1$ e $f(\mathfrak{P}_1 | \mathfrak{p}) = 1$, ou seja, $e(\mathfrak{P} | \mathfrak{p}) = n$ para algum ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$.

No caso $n = 2$, estes três casos são obviamente os únicos.

Pode-se provar que, se $\mathfrak{p}$ não for o único ideal primo de R , então para quaisquer $r, e_1, \dots, e_r, f_1, \dots, f_r \geq 1$ existirá uma extensão finita e separável L de K tal que a decomposição de $\mathfrak{p}$ em L seja do tipo $\mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r}$ com $f(\mathfrak{P}_i | \mathfrak{p}) = f_i$ ($i = 1, \dots, r$). (Veja Endler [8], §27).

EXERCÍCIOS

Nos exercícios 12.1 a 12.5, manteremos as notações do §12.

- 12.1. Sejam $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ os ideais primos de S que estão acima de $\mathfrak{p}$. Prove:
- Existe $\beta \in S$ tal que $\beta \in \mathfrak{P}_1$, $\beta \notin \mathfrak{P}_1^2$, $\beta \notin \mathfrak{P}_2, \dots, \beta \notin \mathfrak{P}_r$.
 - Para todo elemento β deste tipo temos que $\mathfrak{P}_1 = \mathfrak{p} \cdot S + \beta \cdot S$.
- 12.2. Seja $\mathfrak{a}$ um ideal de R e seja $0 \neq c \in \mathfrak{a} \cdot S \cap R$, digamos $c = \sum_{j=1}^m a_j \cdot \beta_j$ com $a_1, \dots, a_m \in \mathfrak{a}$ e $\beta_1, \dots, \beta_m \in S$.
- Sob a hipótese de L ser uma extensão normal de K , prove que existe um polinômio homogêneo $H \in R[X_1, \dots, X_m]$, de grau $n = [L:K]$, tal que $c^n \in H(a_1, \dots, a_m)$, e conclua que $c \in \mathfrak{a}$.
 - Prove que $\mathfrak{a} \cdot S \cap R = \mathfrak{a}$ vale mesmo sem a hipótese de L ser normal sobre K .
- 12.3. a) Usando (12.1), prove que $\mathfrak{a} \cdot S \neq \mathfrak{b} \cdot S$ para quaisquer ideais distintos $\mathfrak{a}, \mathfrak{b}$ de R .
- b) Conclua que $\mathfrak{a} \cdot S \cap R = \mathfrak{a}$ para qualquer ideal $\mathfrak{a}$ de R .
- c) Seja $\mathfrak{a} = \mathfrak{p}_1^{g_1} \cdot \dots \cdot \mathfrak{p}_r^{g_r}$ onde $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ são ideais primos de R distintos e $g_1 \geq 1, \dots, g_r \geq 1$. A partir das decomposições de $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ em L , determine todos os ideais $\mathfrak{U}$ de S tais que $\mathfrak{U} \cap R = \mathfrak{a}$.
- d) Prove que, para quaisquer ideais $\mathfrak{U}, \mathfrak{B}$ de S tais que $\mathfrak{U} \cap R, \mathfrak{B} \cap R$ sejam comaximais, temos que $\mathfrak{U} \cdot \mathfrak{B} \cap R = (\mathfrak{U} \cap R) \cdot (\mathfrak{B} \cap R)$.
- e) Mostre, através de um exemplo, que nem sempre $\mathfrak{U}^2 \cap R = (\mathfrak{U} \cap R)^2$.
- 12.4. Sendo $M = R/\mathfrak{p}$, prove que a aplicação idêntica $S \rightarrow S_M$ induz um isomorfismo de $S/\mathfrak{p} \cdot S$ sobre $S_M/\mathfrak{p} \cdot S_M$.
- 12.5. Sejam L um corpo entre K e L , $S' = I_L(R)$, e sejam $\mathfrak{p}, \mathfrak{P}', \mathfrak{P}$ ideais primos de R, S', S , respectivamente. Supondo que $\mathfrak{P}$ esteja acima de $\mathfrak{P}'$, prove:
- $\mathfrak{P}$ estará acima de $\mathfrak{p}$ se e somente se $\mathfrak{P}'$ estiver acima de $\mathfrak{p}$.
 - Neste caso temos que $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{P}') \cdot e(\mathfrak{P}'|\mathfrak{p})$ e $f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{P}') \cdot f(\mathfrak{P}'|\mathfrak{p})$ (multiplicatividade do índice de ramificação e do grau de inércia).
- 12.6. Indique os números primos p tais que o ideal primo $\mathfrak{p} \cdot \mathbb{Z}$ de $\mathbb{Z}$ seja decomposto (respectivamente inerte, respectivamente ramificado) no corpo dos números de Gauss $\mathbb{Q}(i)$.

§13. Um teorema de Kummer. Ramificação

Sejam novamente R um domínio de Dedekind, L uma extensão finita e separável de $K = Q(R)$, de grau n , e $S = I_L(R)$. No parágrafo anterior foi mostrado que todo ideal primo não-nulo $\mathfrak{p}$ de R se decompõe em L de acordo com a igualdade fundamental.

Neste parágrafo demonstraremos um teorema, devido a Kummer, que permite indicar explicitamente tal decomposição a partir da fatoração $\text{mod } \mathfrak{p} \cdot R[X]$ do polinômio minimal $P_{\beta|K}$, sendo β qualquer elemento em S tal que $S = R[\beta]$; obviamente temos então que $L = K(\beta)$. Note-se que a existência de tal elemento é uma hipótese adicional que nem sempre é satisfeita, mesmo no caso em que $R = \mathbb{Z}$ (veja o final do §5). Ela certamente será satisfeita quando $R = \mathbb{Z}$ e L for um corpo quadrático ou ciclotômico (veja (2.3) e (3.12)). Recordamos que, por (4.10), a igualdade $S = R[\beta]$ será válida se e somente se $1, \beta, \dots, \beta^{n-1}$ formarem uma base do R -módulo S .

Para todo polinômio $F = \sum_{i=1}^r a_i X^i \in R[X]$ denotaremos por $\bar{F}$ o polinômio $\sum_{i=1}^r (a_i + \mathfrak{p}) \cdot X^i \in (R/\mathfrak{p})[X]$ (sendo $\mathfrak{p}$ fixo).

(13.1) TEOREMA. *Suponhamos que $S = R[\beta]$. Seja $P = P_{\beta|K}$ e sejam $P_1, \dots, P_r$ polinômios mônicos em $R[X]$ tais que $\bar{P} = \bar{P}_1^{e_1} \cdot \dots \cdot \bar{P}_r^{e_r}$ seja a fatoração de $\bar{P}$ em polinômios irredutíveis distintos em $(R/\mathfrak{p})[X]$. Então:*

- a) $\mathfrak{p} \cdot S = \mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r}$, onde $\mathfrak{P}_j = \mathfrak{p} \cdot S + P_j(\beta) \cdot S$ ($j=1, \dots, r$) são os ideais primos de S , distintos, acima de $\mathfrak{p}$; logo $e(\mathfrak{P}_j | \mathfrak{p}) = e_j$ ($j=1, \dots, r$).
- b) $S/\mathfrak{P}_j = (R/\mathfrak{p})(\bar{\beta}_j)$, sendo $\bar{\beta}_j$ uma raiz de $\bar{P}_j$; logo $f(\mathfrak{P}_j | \mathfrak{p}) = \partial P_j$ ($j=1, \dots, r$).

Demonstração. Provamos inicialmente a existência de ideais primos $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ de S , distintos e acima de $\mathfrak{p}$, que satisfazem b). Para $j=1, \dots, r$ seja $\bar{\beta}_j$ uma raiz de $\bar{P}_j$ (num fecho algébrico de $R/\mathfrak{p}$); logo $\bar{P}_j$ é o polinômio minimal de $\bar{\beta}_j$ sobre $R/\mathfrak{p}$. O homomorfismo λ_j de $R[X]$ sobre $(R/\mathfrak{p})[\bar{\beta}_j]$, definido por $F \mapsto \bar{F}(\bar{\beta}_j)$ ($F \in R[X]$), induz um homomorfismo $\bar{\lambda}_j$ de $R[X]/(P)$ sobre $(R/\mathfrak{p})[\bar{\beta}_j]$, uma vez que $\lambda_j P = 0$. Por outro lado, o homomorfismo κ de $R[X]$ sobre $R[\beta]$, definido por $F \mapsto F(\beta)$ ($F \in R[X]$), tem como núcleo o ideal principal (P) de $R[X]$, devido a (1.9a); portanto, κ induz um isomorfismo $\bar{\kappa}$ de $R[X]/(P)$ sobre $R[\beta]$. Resulta que $\mu_j = \bar{\lambda}_j \circ \bar{\kappa}^{-1}$ é um homomorfismo de $S = R[\beta]$ sobre $(R/\mathfrak{p})[\bar{\beta}_j]$, e obviamente temos

que $\mu_j(F(\beta)) = \bar{F}(\bar{\beta}_j)$ para todo $F \in R[X]$. Como $(R/p)[\bar{\beta}_j]$ é um corpo, o núcleo de μ_j é um ideal maximal $\mathfrak{P}_j$ de S , e μ_j induz um isomorfismo $\bar{\mu}_j$ de $S/\mathfrak{P}_j$ sobre $(R/p)[\bar{\beta}_j]$. De $\mathfrak{p} \subseteq \mathfrak{P}_j \cap R \neq R$ e da maximalidade de $\mathfrak{p}$ decorre que $\mathfrak{P}_j$ está acima de $\mathfrak{p}$. Como a restrição de μ_j ao subanel R de S coincide com o homomorfismo canônico de R sobre R/p , concluímos que $\bar{\mu}_j$ é um R/p -isomorfismo de $S/\mathfrak{P}_j$ sobre $(R/p)[\bar{\beta}_j]$; logo $S/\mathfrak{P}_j = (R/p)[\bar{\beta}_j]$ para uma certa raiz $\bar{\beta}_j \in S/\mathfrak{P}_j$ de $\bar{P}_j$; portanto $f(\mathfrak{P}_j | \mathfrak{p}) = f_j$. De $\mu_j(P_i(\beta)) = 0 \neq \mu_j(P_i(\beta))$, para $i \neq j$, resulta que $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ são distintos dois a dois.

a) Obviamente $\mathfrak{p} \cdot S + P_j(\beta) \cdot S \subseteq \mathfrak{P}_j$ ($j = 1, \dots, r$). Para provar a inclusão inversa, seja $\alpha \in \mathfrak{P}_j$, digamos $\alpha = G(\beta)$, com $G \in R[X]$. Como $\bar{G}(\bar{\beta}_j) = \mu_j(G(\beta)) = 0$ e $\bar{P}_j$ é o polinômio minimal de $\bar{\beta}_j$ sobre R/p , existe $H \in R[X]$ tal que $\bar{G} = \bar{P}_j \cdot \bar{H}$; logo $G - P_j \cdot H$ tem seus coeficientes em $\mathfrak{p}$, e $\alpha = (G - P_j \cdot H)(\beta) + P_j(\beta) \cdot H(\beta) \in \mathfrak{p} \cdot S + P_j(\beta) \cdot S$.

Afirmamos que $\mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p} \cdot S$. De fato, uma vez que $(\mathfrak{A} + \mathfrak{B}) \cdot (\mathfrak{A} + \mathfrak{B}') \subseteq \mathfrak{A} + \mathfrak{B} \cdot \mathfrak{B}'$ para quaisquer ideais $\mathfrak{A}, \mathfrak{B}, \mathfrak{B}'$ de S , temos que $\mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p} \cdot S + \gamma \cdot S$, onde $\gamma = P_1(\beta)^{e_1} \cdot \dots \cdot P_r(\beta)^{e_r}$. Como o polinômio $P_1^{e_1} \cdot \dots \cdot P_r^{e_r} - P$ tem seus coeficientes em $\mathfrak{p}$ e $P(\beta) = 0$, temos que $\gamma = (P_1^{e_1} \cdot \dots \cdot P_r^{e_r} - P)(\beta) \in \mathfrak{p} \cdot S$; portanto $\mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p} \cdot S$; ou seja, $\mathfrak{P}_1^{e_1} \cdot \dots \cdot \mathfrak{P}_r^{e_r}$ é um múltiplo de $\mathfrak{p} \cdot S$. Concluímos que $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ são os únicos ideais primos de S que estão acima de $\mathfrak{p}$ e que $e(\mathfrak{P}_j | \mathfrak{p}) \leq e_j$ ($j = 1, \dots, r$); portanto $\sum_{j=1}^r e(\mathfrak{P}_j | \mathfrak{p}) \cdot f(\mathfrak{P}_j | \mathfrak{p}) \leq \sum_{j=1}^r e_j \cdot \partial P_j = \partial P = n$. Da igualdade fundamental (12.3) resulta que nestas desigualdades valem as igualdades, o que completa a demonstração de a). $\square$

No seguinte corolário, aplicamos este teorema aos casos extremos da decomposição:

(13.2) COROLÁRIO. Com a hipótese e as notações de (13.1) temos que:

- $\mathfrak{p}$ será totalmente decomposto em L se e somente se $\bar{P}$ se fatorar em $(R/p)[X]$ em fatores lineares distintos $X - (a_j + \mathfrak{p})$ ($j = 1, \dots, n$); neste caso $\mathfrak{p} \cdot S = \mathfrak{P}_1 \cdot \dots \cdot \mathfrak{P}_n$, sendo $\mathfrak{P}_j = \mathfrak{p} \cdot S + (\beta - a_j) \cdot S$ ($j = 1, \dots, n$) ideais primos de S , distintos.
- $\mathfrak{p}$ será totalmente inerte em L se e somente se $\bar{P}$ for irredutível em $(R/p)[X]$; neste caso, $\mathfrak{p} \cdot S$ é um ideal primo de S .
- $\mathfrak{p}$ será totalmente ramificado em L se e somente se $\bar{P}$ for uma potência n -ésima em $(R/p)[X]$, isto é, $\bar{P} = (X - (a + \mathfrak{p}))^n$ para algum $a \in R$; neste caso $\mathfrak{p} \cdot S = \mathfrak{P}^n$, sendo $\mathfrak{P} = \mathfrak{p} \cdot S + (\beta - a) \cdot S$ um ideal primo de S .

Diremos que o ideal primo não-nulo $\mathfrak{p}$ de R é *ramificado* em L quando existir um ideal primo $\mathfrak{P}$ de S acima de $\mathfrak{p}$ tal que $e(\mathfrak{P}|\mathfrak{p}) > 1$ ou que a extensão $S/\mathfrak{P}$ de $R/\mathfrak{p}$ seja inseparável. A segunda parte desta condição poderá ser omitida quando $R/\mathfrak{p}$ for um corpo perfeito, pois neste caso toda extensão algébrica de $R/\mathfrak{p}$ é separável. Isto ocorre, por exemplo, no caso em que $R = I_L$, sendo L qualquer corpo de números algébricos. Note-se porém que, em geral, a separabilidade da extensão L de K não implica a da extensão $S/\mathfrak{P}$ de $R/\mathfrak{p}$.

Mostraremos a seguir que, para saber se $\mathfrak{p}$ é ramificado ou não em L , basta considerar o discriminante $\text{disc}(P_{\mathfrak{p}|K})$ ou, equivalentemente, o ideal discriminante $\mathfrak{d}_{S|R}$.

(13.3) COROLÁRIO. Com a hipótese e as notações de (13.1), as seguintes condições são equivalentes:

- (i) $\mathfrak{p}$ é ramificado em L .
- (ii) O polinômio $\bar{P}_{\mathfrak{p}|K} \in (R/\mathfrak{p})[X]$ é inseparável.
- (iii) $\text{disc}(P_{\mathfrak{p}|K}) \in \mathfrak{p}$.
- (iv) $\mathfrak{p}$ divide $\mathfrak{d}_{S|R}$.

Demonstração. Seja $P = P_{\mathfrak{p}|K}$. (i) $\Leftrightarrow$ (ii): Por (13.1), $\mathfrak{p}$ será ramificado em L se e somente se, na fatoração $\bar{P} = \bar{P}_1^{e_1} \cdots \bar{P}_r^{e_r}$, tivermos que $e_j > 1$ ou $\bar{P}_j$ for inseparável para algum $j \in \{1, \dots, r\}$; isto ocorrerá se e somente se $\bar{P}$ for inseparável.

(ii) $\Leftrightarrow$ (iii): Por §0, A), existe $D \in \mathbb{Z}[X_1, \dots, X_n]$ tal que $\text{disc}(P) = D(a_1, \dots, a_n)$, onde $P = X^n + a_1 X^{n-1} + \dots + a_n$; portanto

$$\text{disc}(\bar{P}) = D(a_1 + \mathfrak{p}, \dots, a_n + \mathfrak{p}) = D(a_1, \dots, a_n) + \mathfrak{p}.$$

Concluimos que $\text{disc}(P) \in \mathfrak{p}$ se e somente se $\text{disc}(\bar{P}) = 0$, o que ocorrerá se e somente se $\bar{P}$ for inseparável.

(iii) $\Leftrightarrow$ (iv) resulta do fato de $\mathfrak{d}_{S|R}$ ser o ideal principal de R gerado por $\text{disc}_{L|K}(1, \beta, \dots, \beta^{n-1}) = \text{disc}(P)$ (veja (4.9)). $\square$

Como já foi mencionado anteriormente, a hipótese da existência de um elemento β tal que $S = R[\beta]$ nem sempre é satisfeita. Mostraremos a seguir que esta hipótese pode ser evitada, utilizando-se o método da localização. Mais precisamente, escolhendo qualquer elemento primitivo $\gamma \in S$ da extensão $L|K$, relacionaremos a decomposição de $\mathfrak{p}$ em L com a fatoração mod $\mathfrak{p} \cdot R[X]$ do polinômio minimal $P_{\gamma|K}$, para quase todos os ideais primos não-nulos $\mathfrak{p}$ de R ; de fato, basta excluir os $\mathfrak{p}$ tais que

$\text{disc}(P_{\gamma|K}) \in \mathfrak{p}$ ou, equivalentemente, que $\mathfrak{p}$ seja um divisor do ideal $\text{disc}(P_{\gamma|K}) \cdot R$.

(13.4) COROLÁRIO. *Seja $\gamma \in S$ tal que $L = K(\gamma)$, seja $\mathfrak{p}$ um ideal primo não-nulo de R tal que $\text{disc}(P_{\gamma|K}) \notin \mathfrak{p}$ e seja $M = R \setminus \mathfrak{p}$.*

Então

- a) $1, \gamma, \dots, \gamma^{n-1}$ formam uma base do R_M -módulo S_M ;
- b) $\mathfrak{p}$ não é ramificado em L ;
- c) o polinômio $\bar{P}_{\gamma|K} \in (R/\mathfrak{p})[X]$ é separável.
- d) *Sejam $P_1, \dots, P_r$ polinômios mônicos em $R[X]$ tais que $\bar{P}_{\gamma|K} = \bar{P}_1 \cdot \dots \cdot \bar{P}_r$, seja a fatoração de $\bar{P}_{\gamma|K}$ em polinômios irredutíveis em $(R/\mathfrak{p})[X]$; então valem as afirmações a) e b) de (13.1), com $e_1 = \dots = e_r = 1$ e γ em lugar de β .*

Demonstração. a) Temos que $S_M = I_L(R_M)$, por (11.5). Por (11.9), R_M é um domínio principal; logo S_M , considerado como R_M -módulo, possui uma base $\beta_1, \dots, \beta_n$, por (5.4). Existem $a_{ij} \in R_M$ tais que $\gamma^{i-1} = \sum_{j=1}^n a_{ij} \cdot \beta_j$ ($i = 1, \dots, n$); logo $\text{disc}(P_{\gamma|K}) = \text{disc}_{L|K}(1, \gamma, \dots, \gamma^{n-1}) = \det(a_{ij})^2 \cdot \text{disc}_{L|K}(\beta_1, \dots, \beta_n)$, por (4.3) e (4.1). Como $\text{disc}(P_{\gamma|K}) \in R \setminus \mathfrak{p} \subseteq R_M \setminus \mathfrak{p} \cdot R_M$ é invertível em R_M , $\det(a_{ij})$ também o é. De (4.9) concluímos que $1, \gamma, \dots, \gamma^{n-1}$ é uma base do R_M -módulo S_M . Portanto podemos aplicar (13.1) e (13.3) a R_M, S_M e γ (em lugar de R, S e β).

b) Usando (13.3), de $\text{disc}(P_{\gamma|K}) \notin \mathfrak{p} \cdot R_M$ concluímos que $\mathfrak{p} \cdot R_M$ não é ramificado em L . De (12.4) resulta que $\mathfrak{p}$ não é ramificado em L .

c) De (13.3) resulta que $P_{\gamma|K} \bmod \mathfrak{p} \cdot R_M$ é um polinômio separável em $(R_M/\mathfrak{p} \cdot R_M)[X]$. Como $R_M/\mathfrak{p} \cdot R_M$ é canonicamente isomorfo a $R/\mathfrak{p}$, por (11.8), podemos identificar $(R_M/\mathfrak{p} \cdot R_M)[X]$ com $(R/\mathfrak{p})[X]$. Logo $\bar{P}_{\gamma|K}$ é um polinômio separável em $(R/\mathfrak{p})[X]$.

d) Observamos primeiramente que $\mathfrak{U} \cdot S_M \cap S = \mathfrak{U}$ para qualquer ideal $\mathfrak{U}$ de S que contém $\mathfrak{p} \cdot S$. De fato, seja $\delta \in \mathfrak{U} \cdot S_M \cap S$, digamos $\delta = \alpha/m$ com $\alpha \in \mathfrak{U}$ e $m \in M$; como $\mathfrak{p}$ é um ideal maximal de R , existem $c \in \mathfrak{p}$ e $r \in R$ tais que $1 = c + r \cdot m$, logo temos que $\delta = c \cdot \delta + r \cdot m \cdot \delta = c \cdot \delta + r \cdot \alpha \in \mathfrak{U}$. De (13.1a) concluímos que $\mathfrak{p} \cdot S_M = \mathfrak{Q}_1 \cdot \dots \cdot \mathfrak{Q}_r$, onde $\mathfrak{Q}_j = \mathfrak{p} \cdot S_M + P_j(\gamma) \cdot S_M = (\mathfrak{p} \cdot S + P_j(\gamma) \cdot S) \cdot S_M$ ($j = 1, \dots, r$) são os ideais primos de S_M , distintos, acima de $\mathfrak{p} \cdot R_M$. De (12.4) resulta que $\mathfrak{Q}_j = \mathfrak{P}_j \cdot S_M$ ($j = 1, \dots, r$) e $\mathfrak{p} \cdot S = \mathfrak{P}_1 \cdot \dots \cdot \mathfrak{P}_r$, sendo $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ os ideais primos de S , distintos, acima de $\mathfrak{p}$. Por (11.2), temos que $\mathfrak{P}_j = \mathfrak{Q}_j \cap S = (\mathfrak{p} \cdot S + P_j(\gamma) \cdot S) \cdot S_M \cap S = \mathfrak{p} \cdot S + P_j(\gamma) \cdot S$ ($j = 1, \dots, r$). Finalmente, de (13.1b) resulta que $S_M/\mathfrak{Q}_j = (R_M/\mathfrak{p} \cdot R_M)(\bar{\gamma}_j)$, sendo $\bar{\gamma}_j$ uma raiz de $\bar{P}_j$, e de (12.4) concluímos que $S/\mathfrak{P}_j = (R/\mathfrak{p})(\bar{\gamma}_j)$ ($j = 1, \dots, r$). $\square$

Obviamente, o conjunto dos ideais primos $\mathfrak{p}$ de R tais que $\text{disc}(P_{\gamma|K}) \in \mathfrak{p}$ depende da escolha do elemento primitivo $\gamma \in S$. Para cada escolha de γ este conjunto é finito, pois consiste de divisores do ideal $\mathfrak{d}_{R[\gamma]|R}$, o qual é o ideal principal de R gerado por $\text{disc}(P_{\gamma|K}) = \text{disc}_{L|K}(1, \gamma, \dots, \gamma^{n-1})$ (veja (4.10)). Mostraremos que este conjunto contém todos os ideais primos não-nulos de R que são ramificados em L . De fato, como consequência de (13.4) obtemos o seguinte Corolário, cuja segunda parte pode ser considerada como generalização parcial de (13.3).

(13.5) COROLÁRIO. *Existe apenas um número finito de ideais primos $\mathfrak{p}$ não-nulos de R que são ramificados em L .*

Cada $\mathfrak{p}$ deste tipo divide $\mathfrak{d}_{R[\gamma]|R}$, qualquer que seja $\gamma \in S$ tal que $L = K(\gamma)$, e, portanto, divide também o máximo divisor $\mathfrak{d}'_{S|R}$ destes ideais.

Note-se que $\mathfrak{d}'_{S|R}$ é o ideal de R gerado pelo conjunto dos discriminantes $\text{disc}(F_{\gamma,L|K}) = \text{disc}_{L|K}(1, \gamma, \dots, \gamma^{n-1})$, onde γ percorre S ; ele é um múltiplo de, mas nem sempre é igual a, o ideal discriminante $\mathfrak{d}_{S|R}$, como mostra o exemplo indicado no final do §5. Pode-se mostrar que $\mathfrak{d}'_{S|R} = \mathfrak{d}_{S|R} \cdot \alpha^2$ para certo ideal α de R (veja Lang [21], Chapter III, §3). Mencionamos ainda, também sem demonstração, que a afirmação do Corolário (13.5) pode ser reforçada da seguinte maneira: Os ideais primos não-nulos ramificados em L são exatamente os que dividem o ideal discriminante $\mathfrak{d}_{S|R}$. (Veja Samuel [30], Chapter V, ou Zariski-Samuel [38], Chapter V, §11, onde o ideal discriminante $\mathfrak{d}_{S|R}$ é obtido a partir do "diferente" $\mathfrak{D}_{S|R}$, um certo ideal de S .)

Observamos ainda que, no caso em que L é um corpo de números algébricos e $R = \mathbb{Z}$, as considerações acima permitem algumas simplificações. Todo ideal primo não-nulo $\mathfrak{p}$ de $\mathbb{Z}$ é gerado por um número primo p ; portanto $R/\mathfrak{p} = \mathbb{F}_p$. Além disto, em (13.1), o ideal primo $\mathfrak{P}_f = \mathfrak{p} \cdot S + P_f(\beta) \cdot S$ ocorrendo na fatoração de $\mathfrak{p} \cdot S = \mathfrak{p} \cdot I_L$, escreve-se como $(p, P_f(\beta)) \cdot I_L$, isto é, é gerado por dois elementos, a saber p e $P_f(\beta)$. Uma simplificação semelhante pode ser feito em (13.4).

Finalmente, consideramos de novo o caso de $\mathfrak{p}$ ser totalmente ramificado em L , que já foi tratado em (13.2c) sob a hipótese de que $S = R[\beta]$ para algum $\beta \in S$. É natural perguntar se esta hipótese pode ser evitada também neste caso, embora não seja possível aplicar o método usado em (13.4), uma vez que $\text{disc}(P_{\gamma|K}) \in \mathfrak{p}$ para todo elemento primitivo $\gamma \in S$. O seguinte teorema, que generaliza o "critério de Eisenstein", fornece uma condição suficiente para que $\mathfrak{p}$ seja totalmente ramificado em L .

(13.6) TEOREMA. Sejam $\mathfrak{p}$ um ideal primo de R e $L = K(\gamma)$, onde $\gamma \in S$ é uma raiz de um polinômio $P = X^n + a_1 \cdot X^{n-1} + \dots + a_n \in R[X]$ tal que $a_1, \dots, a_n \in \mathfrak{p}$ e $a_n \notin \mathfrak{p}^2$.

Então, P é irredutível em $K[X]$, $n = [L:K]$, e $\mathfrak{p} \cdot S = \mathfrak{P}^n$, onde $\mathfrak{P} = \mathfrak{p} \cdot S + \gamma \cdot S$ é um ideal primo de S ; logo $\mathfrak{p}$ é totalmente ramificado em L .

Demonstração. Sejam $\mathfrak{P}$ um ideal primo de S , acima de $\mathfrak{p}$, e $e = e(\mathfrak{P}|\mathfrak{p})$. Por hipótese, temos que $a_n \cdot R = \mathfrak{p} \cdot b$, onde b é um ideal de R , não divisível por $\mathfrak{p}$; de (12.1) resulta que $a_n \cdot S = \mathfrak{P}^e \cdot \mathfrak{B}$, onde $\mathfrak{B}$ é um ideal de S , não divisível por $\mathfrak{P}$. Obviamente $\gamma^n = -(a_1 \cdot \gamma^{n-1} + \dots + a_n) \in \mathfrak{p} \cdot S \subseteq \mathfrak{P}$; logo $\gamma \in \mathfrak{P}$, e assim $\gamma^n \in \mathfrak{P}^n$ e $\{a_1 \cdot \gamma^{n-1}, \dots, a_{n-1} \gamma\} \subseteq (\mathfrak{p} \cdot S) \cdot \mathfrak{P} \subseteq \mathfrak{P}^{e+1}$. Como $\mathfrak{P}^{e+1}$ não divide $a_n \cdot S$, temos que $\gamma^n + a_1 \cdot \gamma^{n-1} + \dots + a_{n-1} \cdot \gamma = -a_n \notin \mathfrak{P}^{e+1}$, logo $\gamma^n \notin \mathfrak{P}^{e+1}$; portanto $n \leq e$. Sendo P um múltiplo (em $K[X]$) do polinômio $P_{\gamma|K}$, temos que $[L:K] = \partial P_{\gamma|K} \leq \partial P = n$. De (12.3) resulta que, nas desigualdades $[L:K] \leq n \leq e$, valem as igualdades e que $\mathfrak{p} \cdot S = \mathfrak{P}^n$. De $\mathfrak{P}^n = \mathfrak{p} \cdot S \subseteq \mathfrak{p} \cdot S + \gamma \cdot S \subseteq \mathfrak{P}$ decorre que $\mathfrak{p} \cdot S + \gamma \cdot S = \mathfrak{P}^m$ para algum $m \in \{1, \dots, n\}$. Temos que $m = 1$, pois caso contrário teríamos que $\gamma \in \mathfrak{P}^2$; logo $\gamma^n \in \mathfrak{P}^{2n} \subseteq \mathfrak{P}^{e+1}$, uma contradição. $\square$

Mostraremos ainda que a condição indicada no teorema (13.6) não é somente suficiente mas também necessária para que $\mathfrak{p}$ seja totalmente ramificado em L . Mais precisamente, veremos que a ramificação total de $\mathfrak{p}$ em L implica que $L|K$ é gerada por uma raiz de um polinômio de Eisenstein, no caso em que $\mathfrak{p}$ é o único ideal primo não-nulo de R . No caso geral, convém usar o método de localização, isto é, de passar dos anéis R, S aos anéis de frações R_M, S_M , onde $M = R \setminus \mathfrak{p}$. Tal passagem preserva a ramificação total, como mostra a seguinte proposição, que é uma consequência imediata de (12.4) e (8.17).

(13.7) Sejam $\mathfrak{p}$ um ideal primo não-nulo de R , totalmente ramificado em L , $\mathfrak{P}$ o único ideal primo de S que está acima de $\mathfrak{p}$, e $M = R \setminus \mathfrak{p}$. Então:

- a) $\mathfrak{p} \cdot R_M$ é totalmente ramificado em L , sendo $\mathfrak{P} \cdot S_M$ o único ideal primo de S_M que está acima de $\mathfrak{p} \cdot R_M$.
- b) R_M e S_M são domínios principais que possuem apenas um ideal primo não-nulo, a saber, $\mathfrak{p} \cdot R_M$ e $\mathfrak{P} \cdot S_M$, respectivamente.

O seguinte teorema pode ser considerado como o recíproco do teorema (13.6); ele será usado no §22 no estudo dos grupos de ramificação.

(13.8) TEOREMA. Com as notações de (13.7), seja π um gerador do ideal $\mathfrak{p} \cdot S_M$, e seja $n = [L : K]$. Então:

- a) $L = K(\pi)$.
- b) $1, \pi, \pi^2, \dots, \pi^{n-1}$ formam uma base do R_M -módulo S_M .
- c) $P_{\pi|K} = X^n + c_{n-1} \cdot X^{n-1} + \dots + c_0$, onde $c_0, \dots, c_{n-1} \in \mathfrak{p} \cdot R_M$, $c_0 \notin (\mathfrak{p} \cdot R_M)^2$.

Demonstração. Por (13.7b) e (8.8), todo ideal fracionário não-nulo de R_M (respectivamente de S_M) escreve-se como potência $(\mathfrak{p} \cdot R_M)^k$ (respectivamente $(\mathfrak{p} \cdot S_M)^k = \pi^k \cdot S_M$) para algum $k \in \mathbb{Z}$ univocamente determinado. Em particular, para qualquer $\alpha \in K \setminus \{0\}$ definimos va pela igualdade $\alpha \cdot R_M = (\mathfrak{p} \cdot R_M)^{va}$; além disto, seja $v0 = \infty$. Quaisquer que sejam $i, j \in \{0, \dots, n-1\}$, $i \neq j$, e $a, b \in K \setminus \{0\}$, temos que $n \cdot va + i \neq n \cdot vb + j$; de fato, caso contrário teríamos que $|i - j| = n \cdot |vb - va|$, em contradição com $0 < |i - j| < n$. Mais geralmente, sejam $a_0, \dots, a_{n-1} \in K$, nem todos iguais a zero, e seja $m = \min \{n \cdot va_i + i \mid 0 \leq i \leq n-1\}$, digamos $m = n \cdot va_{i_0} + i_0$ para um certo $i_0 \in \{0, \dots, n-1\}$; então $m < n \cdot va_i + i$ para todo $i \in \{0, \dots, i_0-1, i_0+1, \dots, n-1\}$. Como $\mathfrak{p} \cdot S_M = (\mathfrak{p} \cdot S_M)^n = \pi^n \cdot S_M$ por (13.7a), temos que $a_i \cdot \pi^i \cdot S_M = \pi^{n \cdot va_i + i} \cdot S_M \subseteq \pi^{m+1} \cdot S_M$ para todo $i \in \{0, \dots, i_0-1, i_0+1, \dots, n-1\}$ tal que $a_i \neq 0$, e $a_{i_0} \cdot \pi^{i_0} \cdot S_M = \pi^m \cdot S_M$. Escrevendo $\alpha = \sum_{i=0}^{n-1} a_i \cdot \pi^i$, concluímos que $\alpha \in \pi^m \cdot S_M \setminus \pi^{m+1} \cdot S_M$; logo $\alpha \cdot S_M = \pi^m \cdot S_M$ e, em particular, $\alpha \neq 0$.

a) Do fato de $(a_0, \dots, a_{n-1}) \neq (0, \dots, 0)$ implicar que $\sum_{i=0}^{n-1} a_i \cdot \pi^i \neq 0$, concluímos que $1, \pi, \dots, \pi^{n-1}$ são linearmente independentes sobre K e, como $[L : K] = n$, formam uma base de $L|K$; portanto $L = K(\pi)$.

b) Obviamente, $\sum_{i=0}^{n-1} R_M \cdot \pi^i \subseteq S_M$. Para obter a igualdade, basta provar que, se $a_0, \dots, a_{n-1} \in K$ são tais que $\sum_{i=0}^{n-1} a_i \cdot \pi^i \in S_M \setminus \{0\}$, então $a_0, \dots, a_{n-1} \in R_M$. Pelo que foi demonstrado acima, o ideal de S_M gerado por $\alpha = \sum_{i=0}^{n-1} a_i \cdot \pi^i$ é da forma $\pi^m \cdot S_M$, sendo $m = \min \{n \cdot va_i + i \mid 0 \leq i \leq n-1\}$.

Se $\alpha \in S_M$, então $m \geq 0$; logo $va_i \geq -\frac{i}{n} > -1$ e assim $va_i \geq 0$, $a_i \in R_M$, para todo $i \in \{0, \dots, n-1\}$.

c) Seja $P_{\pi|K} = X^n + c_{n-1} \cdot X^{n-1} + \dots + c_0$, com $c_0, \dots, c_{n-1} \in K$. Como $\pi^n = - \sum_{i=0}^{n-1} c_i \cdot \pi^i$, temos que $\min\{n \cdot vc_i + i \mid 0 \leq i \leq n-1\} = n$; logo $n \cdot vc_i \geq n - i > 0$ e assim $vc_i > 0$, $c_i \in \mathfrak{p} \cdot R_M$, para todo $i \in \{0, \dots, n-1\}$. Como $n \cdot vc_i + i > n$ para $1 \leq i \leq n-1$, temos que $n \cdot vc_0 = n$; logo $vc_0 = 1$ e assim $c_0 \notin (\mathfrak{p} \cdot R_M)^2$. $\square$

Mencionemos ainda que, sob a hipótese do teorema (13.8) e, mais geralmente, no caso em que existe apenas um ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$, o anel de frações S_M coincide com a localização de S em relação a $\mathfrak{P}$, isto é, com o anel de frações S_N onde $N = S \setminus \mathfrak{P}$. De fato, temos que $M = R \setminus \mathfrak{p} \subseteq N = S \setminus \mathfrak{P} \subseteq S_M \setminus \mathfrak{P} \cdot S_M = U(S_M)$ e, portanto,

$$S_M \subseteq S_N \subseteq (S_M)_N \subseteq (S_M)_{U(S_M)} = S_M.$$

EXERCÍCIOS

- 13.1. Seja $L = \mathbb{Q}(\sqrt{-5})$ (respectivamente $= \mathbb{Q}(\sqrt{5})$).
- Para $p \in \{2, 3, 5, 7\}$, determine a fatoração de $\mathfrak{p} \cdot I_L$ em ideais primos de I_L através da fatoração mod p do polinômio minimal $P_{\beta|K}$, onde $\beta = \sqrt{-5}$ (respectivamente $\frac{1+\sqrt{5}}{2}$).
 - Em lugar de β , utilize outros elementos primitivos $\gamma \in I_L$ de L com a mesma finalidade.
- 13.2. Seja L qualquer corpo de números algébricos. Para todo número primo p indique um elemento $\gamma \in I_L$ tal que $L = \mathbb{Q}(\gamma)$ e p divida $\text{disc}(P_{\gamma|K})$.
- 13.3. Seja $L = \mathbb{Q}(\zeta)$, sendo ζ uma raiz primitiva p -ésima da unidade, para algum número primo $p \neq 2$. Utilizando o teorema (13.6), prove que $\mathfrak{p} \cdot I_L = \mathfrak{P}^{p-1}$, sendo $\mathfrak{P}$ o ideal primo de I_L gerado por $\zeta - 1$.
- 13.4. Seja $L = \mathbb{Q}(\alpha)$, sendo α uma raiz do polinômio $X^3 - X - 1$. Usando o Exercício 4.5., prove que:
- $2 \cdot I_L$ e $3 \cdot I_L$ são ideais primos de I_L .
 - $\mathfrak{P}_1 = 5 \cdot I_L + (\alpha - 2) \cdot I_L = (\alpha - 2) \cdot I_L$ e $\mathfrak{P}_2 = 5 \cdot I_L + (\alpha^2 + 2\alpha + 3) \cdot I_L$ são os ideais primos de I_L que estão acima de $5 \cdot \mathbb{Z}$, e temos que $e(\mathfrak{P}_1 | 5 \cdot \mathbb{Z}) = e(\mathfrak{P}_2 | 5 \cdot \mathbb{Z}) = f(\mathfrak{P}_1 | 5 \cdot \mathbb{Z}) = 1$, $f(\mathfrak{P}_2 | 5 \cdot \mathbb{Z}) = 2$.

- c) $\mathfrak{P}'_1 = 23 \cdot I_L + (\alpha - 10) \cdot I_L$ e $\mathfrak{P}'_2 = 23 \cdot I_L + (\alpha - 3) \cdot I_L = (\alpha - 3) \cdot I_L$ são os ideais primos de I_L que estão acima de $23 \cdot \mathbb{Z}$, e temos que $e(\mathfrak{P}'_1 | 23 \cdot \mathbb{Z}) = 2$, $e(\mathfrak{P}'_2 | 23 \cdot \mathbb{Z}) = f(\mathfrak{P}'_1 | 23 \cdot \mathbb{Z}) = f(\mathfrak{P}'_2 | 23 \cdot \mathbb{Z}) = 1$.
- d) $23 \cdot \mathbb{Z}$ é o único ideal primo de $\mathbb{Z}$ que é ramificado em I_L . (Veja Ribenboim [28], Chapter 13 (2).)
- 13.5. Seja $L = \mathbb{Q}(\alpha)$, sendo α uma raiz do polinômio $X^3 - 3 \cdot X + 9$. Usando o Exercício 4.4., prove que:
- a) Para todo número primo $p \notin \{3, 7, 11\}$, o ideal primo $p \cdot \mathbb{Z}$ não é ramificado em I_L .
- b) $2 \cdot I_L$ é um ideal primo de I_L e $f(2 \cdot I_L | 2 \cdot \mathbb{Z}) = 3$.
- c) $17 \cdot I_L = \mathfrak{P}_1 \cdot \mathfrak{P}_2$ onde $\mathfrak{P}_1, \mathfrak{P}_2$ são ideais primos de I_L tais que $f(\mathfrak{P}_1 | 17 \cdot \mathbb{Z}) = 1$, $f(\mathfrak{P}_2 | 17 \cdot \mathbb{Z}) = 2$. (Veja Ribenboim [28], Chapter 13 (2).)
- 13.6. Seja γ uma raiz do polinômio $X^n - c \in \mathbb{Z}[X]$ e seja p um número primo tal que $p | c$ mas $p^2 \nmid c$. Prove que $p \cdot \mathbb{Z}$ é totalmente ramificado em $\mathbb{Q}(\gamma)$.
(Note-se que podem existir outros primos que são totalmente ramificados em L ; veja Ribenboim [28], Chapter 13, (5).)
- 13.7. Seja $K = K_0(\gamma)$, onde K_0 é um corpo imperfeito de característica p e γ transcendente sobre K_0 ; seja $L = K(\alpha)$, onde α é uma raiz do polinômio $P = X^p - \gamma \cdot X + c$ para algum $c \in K_0 \setminus K_0^\times$; e sejam $R = K_0[\gamma]$ e $S = I_L(R)$. Prove que:
- a) P é irredutível em $K[X]$.
- b) $\gamma \cdot R$ é totalmente inerte em L (isto é, $\gamma \cdot S$ é um ideal primo de S).
- c) $\gamma \cdot R$ é ramificado em L .
- 13.8. Generalize o Corolário (13.4) para o caso de um elemento $\gamma \in S$ e um ideal primo não-nulo $\mathfrak{p}$ de R tais que $1, \gamma, \dots, \gamma^{n-1}$ formem uma base do R_M -módulo S_M , onde $M = R \setminus \mathfrak{p}$.

DECOMPOSIÇÃO EM CORPOS CICLOTÔMICOS E QUADRÁTICOS

A decomposição de números primos p em L , ou seja, a fatoração de $p \cdot I_L$ em ideais primos de I_L , será estudada, neste capítulo, para dois tipos de corpos de números algébricos, a saber, para corpos ciclotômicos e corpos quadráticos. O objetivo principal é indicar, para cada L , um número $m > 1$ com as seguintes propriedades: Os números primos p que dividem m são exatamente os que são ramificados em L , enquanto que, para todo p que não divide m , o tipo de decomposição de p em L depende apenas da classe $p + m \cdot \mathbb{Z} \in U(\mathbb{Z}/m \cdot \mathbb{Z})$.

Para corpos ciclotômicos, esta “lei de decomposição” será demonstrada diretamente, no §14. Para corpos quadráticos $L = \mathbb{Q}(\sqrt{d})$, provaremos primeiramente, no §15, um resultado devido a Kummer, que relaciona o tipo de decomposição de p em L com a classe $d \bmod p$ (respectivamente $d \bmod 8$), para p ímpar (respectivamente $p = 2$). Para poder passar às classes $p \bmod m$, onde m será o discriminante $d_L (= 4 \cdot d$ ou $= d$, conforme o caso), precisaremos da lei de reciprocidade quadrática, a ser demonstrada no §16.

Para simplificar a notação, escreveremos $e(\mathfrak{P})$ (respectivamente $f(\mathfrak{P})$) em lugar de $e(\mathfrak{P} | p)$ (respectivamente $f(\mathfrak{P} | p)$), e nas expressões “ $\mathfrak{P}$ acima de $p \cdot \mathbb{Z}$ ” e “ $p \cdot \mathbb{Z}$ ramificado (respectivamente decomposto, respectivamente inerte) em L ” substituiremos $p \cdot \mathbb{Z}$ por p .

§14. Decomposição em corpos ciclotômicos

Sejam $L_m = \mathbb{Q}(\zeta_m)$ o m -ésimo corpo, e $\Phi_m = P_{\zeta_m | \mathbb{Q}}$ o m -ésimo polinômico ciclotômico, sendo ζ_m uma raiz primitiva m -ésima da unidade, e seja $I_m = I_{L_m}$ o anel dos inteiros algébricos de L_m . O objetivo deste parágrafo é determinar os números primos p que são ramificados em L_m e determinar, para cada p não-ramificado em L_m , a sua decomposição em L_m .

Consideremos primeiramente a decomposição de 2 em L_4 e, para cada número primo p ímpar, a decomposição de p em L_p .

(14.1) TEOREMA. *Sejam p um número primo ímpar (respectivamente $p = 2$) e $m = p$ (respectivamente $m = 4$). Então, p é totalmente ramificado em L_m , a saber, $p \cdot I_m = \mathfrak{P}^{(m)}$, sendo $\mathfrak{P} = (1 - \zeta_m) \cdot I_m$ o único ideal primo de I_m que está acima de p .*

Demonstração. Escreveremos L, I, ζ em lugar de L_m, I_m, ζ_m .

- a) Seja $p = 2$; então $L = \mathbb{Q}(i)$, e $I = \mathbb{Z}[i]$ é fatorial por (2.5) e (2.6). Como $1 - i$ é irredutível em I e $2 = i \cdot (1 - i)^2$, por (2.9), temos que $2 \cdot I = \mathfrak{P}^2$, sendo $\mathfrak{P} = (1 - i) \cdot I$ o único ideal primo de I , acima de 2.
- b) Seja p ímpar; então $p \cdot I = ((1 - \zeta) \cdot I)^{p-1}$, por (3.11). Seja $\mathfrak{P}_1^{k_1} \cdot \dots \cdot \mathfrak{P}_s^{k_s}$ a fatoração de $(1 - \zeta) \cdot I$ em I ; então $p \cdot I = \mathfrak{P}_1^{k_1 \cdot (p-1)} \cdot \dots \cdot \mathfrak{P}_s^{k_s \cdot (p-1)}$, e de (9.8) (ou (12.3)) resulta que $p - 1 = [L : \mathbb{Q}] = \sum_{j=1}^s k_j \cdot (p - 1) \cdot f(\mathfrak{P}_j)$; logo $s = 1$ e $k_1 = 1$; portanto $(1 - \zeta) \cdot I = \mathfrak{P}_1$ é o único ideal primo de I , acima de p . $\square$

Uma outra demonstração no caso $p \neq 2$, usando o Teorema (13.6), é sugerida no Exercício 13.3.

A seguir, consideraremos o m -ésimo corpo ciclotômico L_m para qualquer $m > 1$. Sem perda de generalidade podemos supor que $2 \nmid m$ ou $4 \mid m$, pois se m for ímpar então $L_{2m} = L_m$.

Denotaremos por κ_p o homomorfismo canônico de $\mathbb{Z}[X]$ sobre $\mathbb{F}_p[X]$.

(14.2) TEOREMA. *Seja $m > 1$ ímpar ou divisível por 4. Para todo número primo p , as seguintes condições são equivalentes:*

- (i) p é ramificado em L_m .
- (ii) p divide $\text{disc}(\Phi_m)$.
- (iii) O polinômio $\kappa_p \Phi_m \in \mathbb{F}_p[X]$ é inseparável.
- (iv) p divide m .

Neste caso, temos que $e(\mathfrak{P}) > 1$ para todo ideal primo $\mathfrak{P}$ de I_m que está acima de p .

Demonstração. (i) $\Rightarrow$ (ii) resulta de (13.4).

(ii) $\Rightarrow$ (iii): Veja a prova da equivalência (ii) $\Leftrightarrow$ (iii) em (13.3).

(iii) $\Rightarrow$ (iv): Se $p \nmid m$ então o polinômio $\kappa_p(X^m - 1)$ será separável, pois ele e sua derivada, $\kappa_p(m \cdot X^{m-1})$, são primos entre si. Como Φ_m divide $X^m - 1$ em $\mathbb{Z}[X]$, o polinômio $\kappa_p \Phi_m$ divide $\kappa_p(X^m - 1)$ em $\mathbb{F}_p[X]$ e, portanto, é separável.

(iv) $\Rightarrow$ (i): Seja $L' = L_p$ (respectivamente $= L_4$) no caso em que p é ímpar (respectivamente $p = 2$); então $L' \subseteq L_m$. De (14.1) resulta que $p \cdot I' = \mathfrak{p}^r$, onde $\mathfrak{p}$ é o único ideal primo de $I' = I_L$ que está acima de p e $r \geq 2$. Para todo ideal primo $\mathfrak{P}$ de I_m , acima de p , temos que $\mathfrak{P} \cap I' = \mathfrak{p}$, logo $p \cdot I_m \subseteq \mathfrak{P}$. Concluimos que $p \cdot I_m = \mathfrak{p}^r \cdot I_m = (p \cdot I_m)^r \subseteq \mathfrak{P}^r$; logo $\mathfrak{P}$ divide $p \cdot I_m$, ou seja, $e(\mathfrak{P}) \geq r \geq 2$. $\square$

Mantendo a hipótese de que $2 \nmid m$ ou $4 \mid m$, concluímos deste teorema que os números primos p não-ramificados em L_m são exatamente os que não dividem m . (Note que se m for ímpar então 2 não será ramificado em $L_m = L_{2m}$). Para estes números primos p mostraremos a seguir que o tipo da sua decomposição em L_m depende somente da classe $p \bmod m$.

(14.3) TEOREMA. *Sejam $m > 1$, p um número primo que não divide m , e $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ os ideais primos de I_m , distintos, acima de p . Então temos que $e(\mathfrak{P}_j) = 1$, $f(\mathfrak{P}_j) = f$ ($j = 1, \dots, r$) e $r = \frac{\varphi(m)}{f}$, onde f é a ordem de $p + m \cdot \mathbb{Z}$ no grupo $U(\mathbb{Z}/m \cdot \mathbb{Z})$.*

Demonstração. Escreveremos L, I, ζ em lugar de L_m, I_m, ζ_m . De (14.2) resulta que $e(\mathfrak{P}_1) = \dots = e(\mathfrak{P}_r) = 1$. Seja $\mathfrak{P} \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$, e seja λ o homomorfismo canônico de I sobre $I/\mathfrak{P}$. Como $1, \zeta, \dots, \zeta^{m-1}$ são as raízes de $X^m - 1$, os elementos $\lambda 1, \lambda \zeta, \dots, \lambda \zeta^{m-1}$ são as raízes de $\kappa_p(X^m - 1)$; elas são distintas duas a duas, uma vez que $\kappa_p(X^m - 1)$ e sua derivada $\kappa_p(m \cdot X^{m-1})$ são primos entre si. Obviamente, elas formam um subgrupo, de ordem m , do grupo multiplicativo do corpo $I/\mathfrak{P}$; logo m divide $\mathfrak{N}\mathfrak{P} - 1$. Sendo $f' = f(\mathfrak{P})$, temos que $\mathfrak{N}\mathfrak{P} = p^{f'}$, por (9.4); logo $p^{f'} \equiv 1 \bmod m$, e assim $f \leq f'$.

Para provar que $f' \leq f$, basta mostrar que todo $\bar{\alpha} \in I/\mathfrak{P}$ é uma das (no máximo p^f) raízes do polinômio $X^{p^f} - X \in \mathbb{F}_p[X]$.

Recordemos primeiro que $\text{disc}(\Phi_m) = \text{disc}_{L/\mathbb{Q}}(1, \zeta, \dots, \zeta^{\varphi(m)-1}) = k_\zeta^2 \cdot d_L$, sendo k_ζ o índice de ζ . Por (14.2) temos que $p \nmid \text{disc}(\Phi_m)$, logo $p \nmid k_\zeta$ e assim $k_\zeta \notin \mathfrak{P}$. Por (5.8), α possui um representante α no subanel $\mathbb{Z}[\zeta]$ de I , digamos $\alpha = \sum_{j=0}^s a_j \cdot \zeta^j$, com $a_0, \dots, a_s \in \mathbb{Z}$. Temos que $\alpha^p - \alpha \in p \cdot \mathbb{Z} \subseteq \mathfrak{P}$, para todo $\alpha \in \mathbb{Z}$, e $(\beta + \gamma)^p - (\beta^p + \gamma^p) \in p \cdot I \subseteq \mathfrak{P}$, para quaisquer $\beta, \gamma \in I$; de $p^f \equiv 1 \bmod m$ decorre $\zeta^{p^f} = \zeta$; portanto temos que

$$\alpha^{p^f} \equiv \sum_{j=0}^s (a_j \cdot \zeta^j)^{p^f} \equiv \sum_{j=0}^s a_j \cdot \zeta^j = \alpha \bmod \mathfrak{P},$$

ou seja, $\bar{\alpha} = \lambda\alpha$ é uma das raízes do polinômio $X^{p^f} - X \in \mathbb{F}_p[X]$. Concluímos que $f(\mathfrak{P}_1) = \dots = f(\mathfrak{P}_r) = f$, e de (11.8) (ou (12.3)) resulta que $\varphi(m) = [L : \mathbb{Q}] = r \cdot f$. $\square$

A afirmação deste teorema, juntamente com uma parte de (14.2), pode ser reformulada da seguinte maneira:

(14.4) **COROLÁRIO.** *Os números primos p que, sob o homomorfismo canônico de $\mathbb{Z}$ sobre $\mathbb{Z}/m \cdot \mathbb{Z}$, são levados em $U(\mathbb{Z}/m \cdot \mathbb{Z})$, são exatamente os que não são ramificados em L_m .*

O tipo de decomposição p em L_m depende apenas da classe $p + m \cdot \mathbb{Z}$; de fato, a ordem $f = o(p + m \cdot \mathbb{Z})$ é igual a $f(\mathfrak{P})$, para qualquer um dos $\frac{\varphi(m)}{f}$ ideais primos $\mathfrak{P}$ de I_m que estão acima de p .

Os ideais primos de I_m que estão acima de p podem ser indicados explicitamente, através da fatoração mod p do m -ésimo polinômio cíclico (veja Exercício 3.6). De fato, se $p \nmid m$ então $p \nmid \text{disc } \phi_m$ por (14.2); portanto obtemos de (13.4) o seguinte:

(14.5) **COROLÁRIO.** *Supondo que $p \nmid m$, sejam $P_1, \dots, P_r$ polinômios mônicos em $\mathbb{Z}[X]$ tais que $\kappa_p \phi_m = \kappa_p P_1 \cdot \dots \cdot \kappa_p P_r$, seja a fatoração de $\kappa_p \phi_m$ em polinômios irredutíveis em $\mathbb{F}_p[X]$. Então temos que*

- a) $p \cdot I_m = \mathfrak{P}_1 \cdot \dots \cdot \mathfrak{P}_r$, onde $\mathfrak{P}_j = (p, P_j(\zeta_m))$ ($j = 1, \dots, r$) são os ideais primos de I_m distintos, acima de p ;
- b) $I_m/\mathfrak{P}_j = \mathbb{F}_p(\bar{\gamma}_j)$ para alguma raiz $\bar{\gamma}_j$ de $\kappa_p P_j$ ($j = 1, \dots, r$).

Discutiremos ainda a questão de saber quais são os tipos de decomposição em L_m que realmente ocorrem. Para isto, observamos primeiramente que existirá em $U(\mathbb{Z}/m \cdot \mathbb{Z})$ um elemento de ordem f se e somente se f for um divisor de $\tilde{m} = \text{MMC}\{o(\alpha) \mid \alpha \in U(\mathbb{Z}/m \cdot \mathbb{Z})\}$ (veja Exercício 5.2.d)). Note-se que $\tilde{m}$ divide $\varphi(m)$, e que $\tilde{m} = \varphi(m)$ se e somente se $U(\mathbb{Z}/m \cdot \mathbb{Z})$ for cíclico, o que ocorrerá se e somente se m for uma potência de um número primo ímpar ou $m = 4$ (excluindo novamente o caso em que $m \equiv 2 \pmod{4}$. Veja Ribenboim [28], Chapter 3). Utilizando, sem demonstração, o Teorema de Dirichlet sobre progressões aritméticas que afirma que em cada classe $a + m \cdot \mathbb{Z} \in U(\mathbb{Z}/m \cdot \mathbb{Z})$ existe uma infinidade de números primos (Borevich-Shafarevich [6], Chapter 5, Section 3), obtemos as seguintes afirmações:

(14.6) COROLÁRIO. *Existirá um número primo que se decompõe em L_m em $\frac{\varphi(m)}{r}$ ideais primos distintos se, e somente se, r for um divisor de $\tilde{m}$. Neste caso, existirá uma infinidade de números primos deste tipo.*

(14.7) COROLÁRIO. a) *Existe uma infinidade de números primos que são totalmente decompostos em L_m .*

b) *Supondo que $2 \nmid m$ ou $4 \nmid m$, existirá um número primo que é totalmente inerte em L_m se, e somente se, m for uma potência de um número primo ímpar ou $m = 4$; neste caso, existirá uma infinidade de números primos deste tipo.*

Por exemplo, em $U(\mathbb{Z}/7 \cdot \mathbb{Z})$, as classes mod 7 dos números primos 2, 3, 11, 13, 29 têm ordem 3, 6, 3, 2, 1, respectivamente. Portanto, 3 é totalmente inerte e 29 é totalmente decomposto em L_7 , enquanto que 2 e 11 se decompõem em dois, e 13 se decompõe em três ideais primos distintos. O único número primo que é ramificado em L_7 é 7, a saber, $7 \cdot I_7 = \mathfrak{P}^6$ com $\mathfrak{P} = (1 - \zeta_7)$. Em $U(\mathbb{Z}/28 \cdot \mathbb{Z})$, as classes mod 28 dos números primos 3, 11, 13, 29 têm ordem 6, 6, 2, 1, respectivamente; portanto 29 é totalmente decomposto em L_{28} , enquanto que 3 e 11 se decompõem em dois, e 13 se decompõe em seis ideais primos distintos. Não existe nenhum número primo totalmente inerte em L_{28} , e 2 e 7 são os únicos ramificados em L_{28} .

EXERCÍCIOS

- 14.1. Seja $L = \mathbb{Q}(i)$. Prove que $\mathfrak{P} = (1 - i) \cdot I_L$ é um ideal primo de I_L e $2 \cdot I_L = \mathfrak{P}^2$, usando a igualdade fundamental (em lugar do fato de I_L ser fatorial, o que foi usado na demonstração de (14.1)).
- 14.2. Dê uma prova simplificada do Teorema (14.3), usando (13.4) e o Exercício 3.6.
- 14.3. Determine a ordem de cada classe $\theta \in U(\mathbb{Z}/10 \cdot \mathbb{Z})$ e indique um número primo p tal que $p + 10 \cdot \mathbb{Z} = \theta$.
- 14.4. a) Prove que $\text{MMC}\{\phi(\theta) \mid \theta \in U(\mathbb{Z}/100 \cdot \mathbb{Z})\} = 20$, e para cada $d \in \{1, 2, 4, 5, 10, 20\}$, procure um número primo p_d tal que $\phi(p_d + 100 \cdot \mathbb{Z}) = d$.

- b) Seja $I' = \mathbb{Z}[i]$. Prove que $7 \cdot I'$, $(100 + i) \cdot I'$ e $(10 - 7i) \cdot I'$ são ideais primos de I' que se decompõem em L_{100} em dez, vinte, e dez ideais primos distintos, respectivamente.
- 14.5. a) Indique dois números primos p_1, p_2 tais que, para todo número primo p , existam mais do que um ideal primo de I_{p_1, p_2} , acima de p .
- b) Quaisquer que sejam os números primos p_1, p_2, p_3 , distintos dois a dois, prove que para todo número primo p existem mais do que um ideal primo de I_{p_1, p_2, p_3} , acima de p .

§15. Decomposição em corpos quadráticos

Seja $L = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde d é um número inteiro livre de quadrados (isto é, $d \in \mathcal{D}$ na notação do §2). Estudaremos neste parágrafo a decomposição em L de cada número primo p .

Recordamos que p será ramificado em L se e somente se for um divisor do discriminante d_L (veja (13.3)) e que $d_L = 4 \cdot d$ (respectivamente $= d$) quando $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) mod 4; além disto, $d_L = \text{disc}_{L/\mathbb{Q}}(1, \beta) = \text{disc}(P_{\beta/\mathbb{Q}})$ quando $1, \beta$ formarem uma base integral de L (veja §4).

Consideramos, em particular, a base distinguida $1, \delta$ de L , onde $\delta = \sqrt{d}$, $P_{\delta/\mathbb{Q}} = X^2 - d$ no caso em que $d \equiv 2$ ou 3 mod 4, e $\delta = \frac{1 + \sqrt{d}}{2}$, $P_{\delta/\mathbb{Q}} = X^2 - X - \frac{d-1}{4}$ no caso em que $d \equiv 1$ mod 4 (veja (2.3)). Para todo número primo p , denotamos por κ_p o homomorfismo canônico de $\mathbb{Z}[X]$ sobre $\mathbb{F}_p[X]$.

(15.1) TEOREMA. *Seja $P = P_{\delta/\mathbb{Q}}$. Para todo número primo p , as seguintes condições são equivalentes:*

- (i) p é ramificado em L .
- (ii) O polinômio $\kappa_p P \in \mathbb{F}_p[X]$ é inseparável.
- (iii) p é um divisor do discriminante d_L .
- (iv) p satisfaz uma das seguintes condições:
 - a) $p = 2$ e $d \equiv 3$ mod 4, ou
 - b) p divide d .

Neste caso temos que $p \cdot I_L = \mathfrak{P}^2$ e $f(\mathfrak{P}) = 1$, onde $\mathfrak{P}$ é o único ideal primo de I_L que está acima de p ; além disto,

$$\begin{aligned}\kappa_p P &= (X - \kappa_p 1)^2 \text{ e } \mathfrak{P} = (p, \delta - 1) \text{ quando } p = 2 \text{ e } d \equiv 3 \pmod{4}; \\ \kappa_p P &= X^2 \text{ e } \mathfrak{P} = (p, \delta) \text{ quando } p \nmid d \text{ e } d \equiv 2 \text{ ou } 3 \pmod{4}; \\ \kappa_p P &= \left(X - \kappa_p \left(\frac{d-1}{2} \right) \right)^2 \text{ e } \mathfrak{P} = \left(p, \delta - \frac{d-1}{2} \right) \text{ quando } p \mid d \text{ e } d \equiv 1 \pmod{4}.\end{aligned}$$

Demonstração. A equivalência das condições (i), (ii) e (iii) resulta de (13.3).

A equivalência entre (iii) e (iv) resulta de que $d_L = 4 \cdot d$ (respectivamente $= d$) no caso em que $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) $\pmod{4}$.

Se $d \equiv 3 \pmod{4}$, então obviamente $X^2 - \kappa_2 d = (X - \kappa_2 1)^2$. Se p dividir d e $d \equiv 2$ ou $3 \pmod{4}$, então $X^2 - \kappa_p d = X^2$. No caso em que $d \equiv 1 \pmod{4}$, temos que $P = X^2 - X - k$, sendo $k \in \mathbb{Z}$ tal que $d = 1 + 4k$. Se p dividir d , então $4k \equiv -1 \pmod{p}$ e $4k^2 \equiv -k \pmod{p}$; logo

$$\kappa_p P = X^2 + \kappa_p(4k) \cdot X + \kappa_p(4k^2) = (X - \kappa_p(2k))^2 = \left(X - \kappa_p \left(\frac{d-1}{2} \right) \right)^2.$$

O resto resulta de (13.1). $\square$

Concluímos deste teorema que os números primos *não*-ramificados em L são os números primos ímpares que não dividem d , bem como o número 2 no caso em que $d \equiv 1 \pmod{4}$. A seguir discutiremos a questão de saber quais desses números primos são decompostos e quais são inertes em L .

Sejam p um número primo ímpar e $c \in \mathbb{Z}$, não divisível por p . Diremos que p é um *resto quadrático* $\pmod{p}$ se existir um $a \in \mathbb{Z}$ tal que $c \equiv a^2 \pmod{p}$, isto é, se a classe $c + p \cdot \mathbb{Z} \in \mathbb{F}_p^*$ for um quadrado em $\mathbb{F}_p^*$; caso contrário, c é chamado um *não-resto quadrático* $\pmod{p}$. Recordamos que $\mathbb{F}_p^*$ é um grupo cíclico, de ordem $p-1$, e que os quadrados em $\mathbb{F}_p^*$ formam o único subgrupo de $\mathbb{F}_p^*$ de ordem $\frac{p-1}{2}$.

(15.2) **TEOREMA.** *Seja $P = P_{\delta|\mathbb{Q}}$. Para todo número primo p , as seguintes condições são equivalentes:*

- (i) p é decomposto em L .
- (ii) O polinômio $\kappa_p P \in \mathbb{F}_p[X]$ é separável e redutível.
- (iii) p satisfaz uma das seguintes condições:
 - a) $p = 2$ e $d \equiv 1 \pmod{8}$, ou
 - b) p é ímpar e d é resto quadrático $\pmod{p}$.

Neste caso temos que $p \cdot I_L = \mathfrak{P} \cdot \mathfrak{P}'$ e $f(\mathfrak{P}) = f(\mathfrak{P}') = 1$, onde $\mathfrak{P}$ e $\mathfrak{P}'$ são os únicos ideais primos de I_L que estão acima de p ; além disto,

$\kappa_p P = X \cdot (X - \kappa_p 1)$ e $\mathfrak{P} = (p, \delta)$, $\mathfrak{P}' = (p, \delta - 1)$ quando $p = 2$, $d \equiv 1 \pmod{8}$;

$\kappa_p P = (X - \kappa_p a) \cdot (X + \kappa_p a)$ e $\mathfrak{P} = (p, \delta - a)$, $\mathfrak{P}' = (p, \delta + a)$ quando p for ímpar e $d \equiv 2$ ou $3 \pmod{4}$, sendo $a \in \mathbb{Z}$ tal que $d \equiv a^2 \pmod{p}$;

$\kappa_p P = (X - \kappa_p g) \cdot (X - \kappa_p(1 - g))$ e $\mathfrak{P} = (p, \delta - g)$, $\mathfrak{P}' = (p, \delta - 1 + g)$ quando p for ímpar e $d \equiv 1 \pmod{4}$, sendo $g \in \mathbb{Z}$ tal que $d \equiv (2g + 1)^2 \pmod{p}$.

Demonstração. (i) $\Leftrightarrow$ (ii) resulta de (13.1).

(ii) $\Rightarrow$ (iii): Existem $a, b \in \mathbb{Z}$ tais que $\kappa_p P = (X - \kappa_p a) \cdot (X - \kappa_p b)$ e $a \not\equiv b \pmod{p}$. De (15.1) resulta que p não divide d e que $d \equiv 2$ ou $3 \pmod{4}$ implica $p \neq 2$. No caso em que $d \equiv 2$ ou $3 \pmod{4}$, temos que $a + b \equiv 0 \pmod{p}$ e $a^2 \equiv -a \cdot b \equiv d \pmod{p}$; logo d é um resto quadrático $\pmod{p}$. No caso em que $d \equiv 1 \pmod{4}$, temos que $a + b \equiv 1 \pmod{p}$ e $a^2 - a \equiv -a \cdot b \equiv \frac{d-1}{4} \pmod{p}$. Para $p = 2$ temos que $a^2 \equiv a \pmod{2}$, logo $\frac{d-1}{4} \equiv 0 \pmod{2}$, e assim $d \equiv 1 \pmod{8}$. Se $p \neq 2$, então $(2a-1)^2 = 4 \cdot (a^2 - a) + 1 \equiv d \pmod{p}$, logo d é um resto quadrático $\pmod{p}$.

(iii) $\Rightarrow$ (ii): Suponhamos que $p = 2$ e $d \equiv 1 \pmod{8}$. Então $\frac{d-1}{4} \equiv 0 \pmod{2}$, logo $\kappa_2 P = X \cdot (X - \kappa_2 1)$. Suponhamos que p seja ímpar e $d \equiv a^2 \pmod{p}$ para algum $a \in \mathbb{Z}$. No caso em que $d \equiv 2$ ou $3 \pmod{4}$, temos que $\kappa_p P = (X - \kappa_p a) \cdot (X + \kappa_p a)$, e $\kappa_p a \neq -\kappa_p a$ pois $2a \not\equiv 0 \pmod{p}$. No caso em que $d \equiv 1 \pmod{4}$, temos que $P = X^2 - X - k$, sendo $k \in \mathbb{Z}$ tal que $d = 1 + 4k$. Seja $g \in \mathbb{Z}$ tal que $2g \equiv a + 1 \pmod{p}$; então $d \equiv a^2 \equiv (2g - 1)^2 \pmod{p}$, logo $4k \equiv a^2 - 1 \equiv 4g \cdot (g - 1) \pmod{p}$ e assim $-k \equiv g \cdot (1 - g) \pmod{p}$ e $\kappa_p P = (X - \kappa_p g) \cdot (X - \kappa_p(1 - g))$. Além disto, temos que $\kappa_p g \neq \kappa_p(1 - g)$, pois $2 \cdot g - 1 \equiv a \not\equiv 0 \pmod{p}$. Em todos os casos, $\kappa_p P$ é separável e redutível em $\mathbb{F}_p[X]$. O resto resulta de (13.1). $\square$

Do fato de que os números primos inertes em L são exatamente os que não são nem ramificados nem decompostos em L resulta imediatamente o seguinte:

(15.3) COROLÁRIO. Seja $P = P_{d|\mathbb{Q}}$. Para todo número primo p , as seguintes condições são equivalentes:

- (i) p é inerte em L .
- (ii) O polinômio $\kappa_p P$ é irredutível em $\mathbb{F}_p[X]$.
- (iii) p satisfaz uma das seguintes condições:
 - a) $p = 2$ e $d \equiv 5 \pmod{8}$, ou
 - b) p é ímpar e d é não-resto quadrático mod p .

Neste caso, $p \cdot I_L$ é um ideal primo de I_L e $f(p \cdot I_L) = 2$.

Observamos ainda que o fato das condições (iv) de (15.1), (iii) de (15.2) e (iii) de (15.3) determinarem o tipo de decomposição de p em $L = \mathbb{Q}(\sqrt{d})$ pode ser provado sem usar o teorema de Kummer (13.1) (veja Exercício 15.6. ou Samuel [30], §5.4).

Note-se que é fácil verificar, para cada número primo p , qual dessas condições é satisfeita. De fato, para $p = 2$ basta verificar se $d - 1$ é divisível ou não por 4 ou por 8, e para $p \neq 2$ basta verificar se p divide ou não um dos números $d - q$, onde q percorre um sistema de representantes dos quadrados em $\mathbb{F}_p^*$. Por exemplo, no caso em que $d = -15$, o número 2 é decomposto em $L = \mathbb{Q}(\sqrt{-15})$, pois 8 divide $d - 1 = -16$; os únicos números primos ramificados em L são os que dividem -15 , a saber, 3 e 5; o número 7 é inerte em L , pois 7 não divide nem $d - 1 = -16$, nem $d - 2 = -17$, nem $d - 4 = -19$, sendo 1, 2, 4 um sistema de representantes dos quadrados em $\mathbb{F}_7^*$; o número 17 é decomposto em L pois 17 divide $d - 2 = -17$ e $2 \equiv 6^2 \pmod{17}$.

Este método, que permite determinar o tipo de decomposição em L de cada número primo p , embora sendo fácil, se torna trabalhoso quando usado para números primos grandes. Ele pode ser substituído por um método mais prático que usa a "lei de reciprocidade quadrática", devida a Legendre e Gauss, a ser demonstrada no seguinte parágrafo. A maior importância desta lei, porém, consiste em permitir provar a "lei de decomposição", que afirma que o tipo de decomposição de p em $L = \mathbb{Q}(\sqrt{d})$ depende apenas da classe de $p \pmod{m}$ para certo $m \in \mathbb{N}$ (a saber, para $m = |d_L|$). Note-se que isto já foi demonstrado em (2.9) no caso especial em que $d = -1$, e que uma lei de decomposição deste tipo vale também para corpos ciclotômicos, como foi provado em §14.

EXERCÍCIOS

- 15.1. a) Determine a decomposição dos números primos 2, 3, 5, 7, 11 e 13 em $\mathbb{Q}(\sqrt{15})$ e em $\mathbb{Q}(\sqrt{-15})$.
 b) Determine a decomposição do número primo 2 em $\mathbb{Q}(\sqrt{d})$ para todo $d \in \mathcal{D}$ tal que $-6 \leq d \leq 6$ (veja o frontispício deste livro).

15.2. Seja $L = \mathbb{Q}(\sqrt{-5})$. Indique os ideais primos de I_L que estão acima de 2 ou 3 e compare-os com os indicados no Exercício 9.7.

15.3. Seja $k \geq 1$. Um número ímpar $c \in \mathbb{Z}$ será chamado *resto quadrático mod 2^k* quando $c \equiv a^2 \pmod{2^k}$ para algum $a \in \mathbb{Z}$. Prove, para qualquer $c \in \mathbb{Z}$ ímpar, que

- a) c é resto quadrático mod 2.
 b) c será resto quadrático mod 4 se e somente se $c \equiv 1 \pmod{4}$.
 c) c será resto quadrático mod 8 se e somente se $c \equiv 1 \pmod{8}$; neste caso, c é resto quadrático mod 2^k para todo $k \geq 1$.

Prove uma afirmação semelhante em relação a restos quadráticos módulo as potências de um número primo ímpar (veja Ribenboim [28], Chapter 4).

15.4. Seja $L = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathcal{D}$, d ímpar. Prove que:

- a) 2 será ramificado em L se e somente se d não for resto quadrático mod 4.
 b) 2 será inerte em L se e somente se d for resto quadrático mod 4 mas não mod 8.
 c) 2 será decomposto em L se e somente se d for resto quadrático mod 8.

15.5. Sejam $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$ e $d \equiv 1 \pmod{4}$, e p um número primo ímpar. Prove que:

- a) Para todo $\beta \in I_L$ existe um $\beta' \in \mathbb{Z}[\sqrt{d}]$ tal que $\beta - \beta' \in p \cdot I_L$.
 b) $p \cdot \mathbb{Z}[\sqrt{d}] = p \cdot I_L \cap \mathbb{Z}[\sqrt{d}]$.
 c) $\mathbb{Z}[\sqrt{d}]/p \cdot \mathbb{Z}[\sqrt{d}]$ é canonicamente isomorfo a $I_L/p \cdot I_L$.

15.6. Sejam $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$, e p um número primo; suponhamos que se $d \equiv 1 \pmod{4}$ então $p \neq 2$. Prove que:

- a) $I_L/p \cdot I_L$ é isomorfo a $\mathbb{F}_p[X]/(X^2 - \kappa_p d)$ (utilize os Exercícios 15.5. e 1.6.)
 b) p será ramificado em L se e somente se $I_L/p \cdot I_L$ possuir um elemento nilpotente v (isto é, $v \neq 0$ mas $v^k = 0$ para algum $k \in \mathbb{N}$).

- c) p será inerte (respectivamente decomposto) em L se e somente se $I_L/p \cdot I_L$ for um corpo (respectivamente isomorfo ao produto cartesiano de dois corpos).
- d) Utilize a), b) e c) para provar parte de (15.1), (15.2) e (15.3), sem usar o teorema de Kummer (13.1).

§16. Reciprocidade quadrática

Vimos no §15 que, para qualquer corpo quadrático $L = \mathbb{Q}(\sqrt{d})$ (onde $d \in \mathcal{D}$), o tipo de decomposição de cada número primo p em L depende apenas da classe de $d \bmod p$ (respectivamente $\bmod 8$, no caso em que $p = 2$). Este resultado ainda não é satisfatório, uma vez que não fornece uma descrição simples do conjunto dos números primos que são decompostos (respectivamente inertes) em L . Tal descrição será dada pela “lei de decomposição” a ser demonstrada neste parágrafo, a qual afirma que o tipo de decomposição de p depende apenas da classe de p módulo o valor absoluto do discriminante d_L .

A prova desta “lei de decomposição” é baseada na “lei de reciprocidade quadrática” que, para quaisquer números primos ímpares p e q , relaciona a propriedade de p ser resto quadrático $\bmod q$ com a propriedade de q ser resto quadrático $\bmod p$. Tal relacionamento formula-se convenientemente por meio do “símbolo de Legendre”. Das várias provas existentes apresentaremos uma prova elementar da lei de reciprocidade quadrática, estendida, por conveniência, ao símbolo de Jacobi, que é uma generalização do símbolo de Legendre e é útil na prova da lei de decomposição. Uma prova mais elegante da lei de reciprocidade quadrática, usando “somas de Gauss”, será esboçada no Exercício 16.14.

Dados um número primo ímpar p e qualquer $c \in \mathbb{Z}$, não divisível por p , define-se o *símbolo de Legendre* como

$$\left(\frac{c}{p}\right) = \begin{cases} 1 & \text{quando } c \text{ é resto quadrático mod } p \\ -1 & \text{quando } c \text{ é não-resto quadrático mod } p. \end{cases}$$

Ele pode ser calculado através do seguinte “critério de Euler”:

(16.1) *Seja p um número primo ímpar e seja $c \in \mathbb{Z}$ não divisível por p . Então $\left(\frac{c}{p}\right) = c^{(p-1)/2} \bmod p$.*

Demonstração. O grupo multiplicativo $\mathbb{F}_p^*$ do corpo $\mathbb{F}_p$ é cíclico de ordem $p-1$, por (3.1). Seja $w+p \cdot \mathbb{Z}$, com $w \in \mathbb{Z}$, um gerador de $\mathbb{F}_p^*$; então o único subgrupo de $\mathbb{F}_p^*$ de ordem 2 é gerado por $-1+p \cdot \mathbb{Z} = w^{(p-1)/2} + p \cdot \mathbb{Z}$. Existe $j \in \{0, 1, \dots, p-2\}$ tal que $c \equiv w^j \pmod{p}$. Obviamente c será resto quadrático mod p se e somente se j for par; portanto $\left(\frac{c}{p}\right) = (-1)^{j/2}$.

Resulta que $\left(\frac{c}{p}\right) \equiv w^{j \cdot (p-1)/2} \equiv c^{(p-1)/2} \pmod{p}$. $\square$

Aplicando este critério ao número $c = -1$, vemos que -1 será resto quadrático mod p se e somente se $p \equiv 1 \pmod{4}$. Por (15.2), isto ocorrerá se e somente se p for decomposto no corpo dos números de Gauss $\mathbb{Q}(i)$, um resultado que já foi obtido em (2.9). Mais geralmente, este critério pode ser aplicado a qualquer $c \in \mathbb{Z}$ não divisível por p , para decidir se c é resto quadrático mod p ou não; mas o cálculo de $c^{(p-1)/2}$ tornar-se-á trabalhoso quando p for grande. Por exemplo, temos que

$$\begin{aligned} \left(\frac{-15}{7}\right) &\equiv (-15)^3 = -3\,375 = (-482) \cdot 7 - 1 \equiv -1 \pmod{7} \text{ e} \\ \left(\frac{-15}{17}\right) &= (-15)^8 = 2\,562\,890\,625 = \\ &= 150\,758\,272 \cdot 17 + 1 \equiv 1 \pmod{17}; \end{aligned}$$

portanto -15 é resto (respectivamente não-resto) quadrático mod 17 (respectivamente 7), o que, aliás, já foi visto de uma maneira mais direta no final do §15.

Para definir o símbolo de Jacobi, convém introduzir a seguinte noção. Dado um número ímpar positivo m , diremos que os elementos $s_1, \dots, s_{(m-1)/2} \in \mathbb{Z}$ formam um *semi-sistema* mod m quando $s_1, \dots, s_{(m-1)/2}, 0, -s_1, \dots, -s_{(m-1)/2}$ formarem um sistema de representantes de $\mathbb{Z}/m \cdot \mathbb{Z}$, ou seja, quando todo $a \in \mathbb{Z}$ for côngruo mod m a exatamente um destes elementos.

(16.2) Sejam $m \in \mathbb{N}$ ímpar, $c \in \mathbb{Z}$ tal que $\text{MDC}(m, c) = 1$, e suponhamos que $s_1, \dots, s_{(m-1)/2}$ formem um semi-sistema mod m . Então,

- a) existem números $\delta_1, \dots, \delta_{(m-1)/2} \in \{1, -1\}$ e uma permutação π de $\left\{1, \dots, \frac{m-1}{2}\right\}$, univocamente determinados, tais que $c \cdot s_j \equiv s_{\pi(j)} \cdot \delta_j \pmod{m}$ ($j = 1, \dots, \frac{m-1}{2}$);

b) o produto $\prod_{j=1}^{(m-1)/2} \delta_j$ independe da escolha do semi-sistema.

Demonstração. a) Como $c + m \cdot \mathbb{Z} \in U(\mathbb{Z}/m \cdot \mathbb{Z})$, existem uma aplicação

π de $\left\{1, \dots, \frac{m-1}{2}\right\}$ em si mesmo e $\delta_1, \dots, \delta_{(m-1)/2} \in \{1, -1\}$

tais que $c \cdot s_j \equiv s_{\pi j} \cdot \delta_j \pmod{m}$ ($j = 1, \dots, \frac{m-1}{2}$). Sejam $j, k \in \left\{1, \dots, \frac{m-1}{2}\right\}$

tais que $\pi j = \pi k$; então $c \cdot s_j \cdot \delta_k \equiv s_{\pi j} \cdot \delta_j \cdot \delta_k \equiv s_{\pi k} \cdot \delta_k \cdot \delta_j \equiv c \cdot s_k \cdot \delta_j \pmod{m}$; logo $s_j \cdot \delta_k \equiv s_k \cdot \delta_j \pmod{m}$, e assim $s_j = s_k$. Resulta que π é injetiva e, portanto, uma permutação.

b) Seja $t_1, \dots, t_{(m-1)/2}$ um outro semi-sistema mod m ; sem perda de generalidade podemos supor que $t_j \equiv s_j \cdot \tau_j \pmod{m}$, onde $\tau_j \in \{1, -1\}$ ($j = 1, \dots, \frac{m-1}{2}$). Então $c \cdot t_j \equiv c \cdot s_j \cdot \tau_j \equiv s_{\pi j} \cdot \delta_j \cdot \tau_j \equiv t_{\pi j} \cdot e_j \pmod{m}$,

com $e_j = \tau_{\pi j}^{-1} \cdot \delta_j \cdot \tau_j \in \{1, -1\}$ ($j = 1, \dots, \frac{m-1}{2}$); logo

$$\prod_{j=1}^{(m-1)/2} e_j = \prod_{j=1}^{(m-1)/2} \delta_j. \quad \square$$

O produto indicado no item b) de (16.2) é denotado por $\left(\frac{c}{m}\right)$ e chamado o *símbolo de Jacobi*; obviamente $\left(\frac{c}{m}\right) = 1$ quando $m = 1$ ou $c = 1$.

A coincidência desta notação com a do símbolo de Legendre, no caso em que m é um número primo ímpar, é justificada pelo seguinte:

(16.3) **TEOREMA.** Para qualquer número primo ímpar p e qualquer $c \in \mathbb{Z}$ que não é divisível por p , os símbolos $\left(\frac{c}{p}\right)$ de Jacobi e de Legendre coincidem.

Demonstração. Formando o produto das congruências indicadas no item a) de (16.2), obtemos que

$$c^{(p-1)/2} \cdot \prod_{j=1}^{(p-1)/2} s_j \equiv \prod_{j=1}^{(p-1)/2} s_{\pi j} \cdot \prod_{j=1}^{(p-1)/2} \delta_j \pmod{p}.$$

Como $s_1, \dots, s_{(p-1)/2}$ não são divisíveis por p , concluímos que $c^{(p-1)/2} \equiv \prod_{j=1}^{(p-1)/2} \delta_j \pmod{p}$. Por (16.1), $c^{(p-1)/2}$ é congruo mod p ao símbolo de Legendre $\left(\frac{c}{p}\right)$, o qual, portanto, é congruo mod p , e mesmo igual, ao símbolo de Jacobi $\left(\frac{c}{p}\right)$. $\square$

Utilizando o *semi-sistema natural* mod m , a saber, $1, 2, \dots, \frac{m-1}{2}$, obtemos uma interpretação mais intuitiva do símbolo de Jacobi. Obviamente $\mathbb{Z}/m \cdot \mathbb{Z} = P_m \cup N_m \cup \{m \cdot \mathbb{Z}\}$ (reunião disjunta), sendo

$$P_m = \left\{1 + m \cdot \mathbb{Z}, \dots, \frac{m-1}{2} + m \cdot \mathbb{Z}\right\}$$

(respectivamente $N_m = \left\{-1 + m \cdot \mathbb{Z}, \dots, -\frac{m-1}{2} + m \cdot \mathbb{Z}\right\}$) o conjunto das “classes positivas” (respectivamente “negativas”) mod m . Para cada $c \in \mathbb{Z}$ com $\text{MDC}(m, c) = 1$, a multiplicação por c fornece uma permutação em $P_m \cup N_m$ mas, em geral, não fornece permutações em P_m e N_m ; em particular, o conjunto $c \cdot P_m = \left\{c \cdot j + m \cdot \mathbb{Z} \mid j = 1, \dots, \frac{m-1}{2}\right\}$ geralmente não está contido em P_m .

(16.4) Sejam $m \in \mathbb{N}$ ímpar e $c \in \mathbb{Z}$ tais que $\text{MDC}(m, c) = 1$. Então $\left(\frac{c}{m}\right) = (-1)^v$, onde v é o número de elementos de $c \cdot P_m \cap N_m$.

Demonstração. Com as notações de (16.2) aplicadas ao semi-sistema natural mod m , teremos que $c \cdot j + m \cdot \mathbb{Z} \in N_m$ se e somente se

$\delta_j = -1$, qualquer que seja $j \in \left\{1, \dots, \frac{m-1}{2}\right\}$; portanto $\left(\frac{c}{m}\right) = (-1)^v$,

onde v é o número de elementos do conjunto $\left\{j \mid j = 1, \dots, \frac{m-1}{2}; \delta_j = -1\right\}$.

Pela aplicação $j \mapsto c \cdot j + m \cdot \mathbb{Z}$, este conjunto está em correspondência biunívoca com $c \cdot P_m \cap N_m$. $\square$

Para determinar $\left(\frac{c}{m}\right)$, basta então calcular os menores restos absolutos de $c, 2c, \dots, \frac{m-1}{2} \cdot c \pmod{m}$. Por exemplo, no caso $m=17$ e $c=-15$

temos que $c \equiv 2$, $2 \cdot c \equiv 4$, $3 \cdot c \equiv 6$, $4 \cdot c \equiv 8$, $5 \cdot c \equiv -7$, $6 \cdot c \equiv -5$, $7 \cdot c \equiv -3$ e $8 \cdot c \equiv -1 \pmod{17}$; portanto $c \cdot P_{17} \cap N_{17}$ consiste de quatro elementos, logo $\left(\frac{-15}{17}\right) = (-1)^4 = 1$.

O símbolo de Jacobi tem as seguintes propriedades:

(16.5) Sejam $m \in \mathbb{N}$ ímpar e $c, c' \in \mathbb{Z}$ tais que $\text{MDC}(m, c) = \text{MDC}(m, c') = 1$. Então,

$$\text{a) } c \equiv c' \pmod{m} \text{ implica } \left(\frac{c}{m}\right) = \left(\frac{c'}{m}\right).$$

$$\text{b) } \left(\frac{c \cdot c'}{m}\right) = \left(\frac{c}{m}\right) \cdot \left(\frac{c'}{m}\right).$$

Sejam $m, n \in \mathbb{N}$ ímpares e $c \in \mathbb{Z}$ tais que $\text{MDC}(m, c) = \text{MDC}(n, c) = 1$. Então,

$$\text{c) } \left(\frac{c}{m \cdot n}\right) = \left(\frac{c}{m}\right) \cdot \left(\frac{c}{n}\right).$$

Demonstração. Utilizaremos as notações de (16.2) em relação ao semi-sistema natural $1, \dots, \frac{m-1}{2} \pmod{m}$, isto é, $c \cdot j \equiv \pi j \cdot \delta_j$

$$\pmod{m} \text{ e } c' \cdot j \equiv \pi' j \cdot \delta'_j \pmod{m} \left(j = 1, \dots, \frac{m-1}{2} \right).$$

a) De $c \equiv c' \pmod{m}$ decorre $\pi j \cdot \delta_j \equiv \pi' j \cdot \delta'_j \pmod{m}$, logo $\pi_j = \pi'_j$ e $\delta_j = \delta'_j$ ($j = 1, \dots, \frac{m-1}{2}$); portanto $\left(\frac{c}{m}\right) = \left(\frac{c'}{m}\right)$.

b) Temos que $c \cdot c' \cdot j \equiv c \cdot \pi' j \cdot \delta'_j \equiv \pi(\pi' j) \cdot \delta_{\pi' j} \cdot \delta'_j \pmod{m}$

$$\begin{aligned} \left(j = 1, \dots, \frac{m-1}{2} \right); \text{ logo } \left(\frac{c \cdot c'}{m}\right) &= \prod_{j=1}^{(m-1)/2} \delta_{\pi' j} \cdot \delta'_j = \\ &= \prod_{j=1}^{(m-1)/2} \delta_j \cdot \prod_{j=1}^{(m-1)/2} \delta'_j = \left(\frac{c}{m}\right) \cdot \left(\frac{c'}{m}\right). \end{aligned}$$

c) Seja $1, \dots, \frac{n-1}{2}$ o semi-sistema natural mod n . Por (16.2) existem

$\varepsilon_1, \dots, \varepsilon_{(n-1)/2} \in \{1, -1\}$ e uma permutação ρ de $\left\{1, \dots, \frac{n-1}{2}\right\}$ tais que

$$c \cdot k \equiv \rho k \cdot \varepsilon_k \pmod{n} \left(k = 1, \dots, \frac{n-1}{2} \right). \text{ Os } \frac{m \cdot n - 1}{2} = \frac{m-1}{2} + \frac{n-1}{2} \cdot m$$

elementos $j \cdot n \in k + g \cdot n \left(j = 1, \dots, \frac{m-1}{2}; k = 1, \dots, \frac{n-1}{2}; g = 0, \dots, m-1 \right)$

formam um semi-sistema mod $m \cdot n$, uma vez que eles, juntamente com os seus negativos e o zero, são incôngruos mod $m \cdot n$ dois a dois, como se verifica facilmente. Para qualquer $j \in \left\{ 1, \dots, \frac{m-1}{2} \right\}$ temos que $c \cdot (j \cdot n) \equiv$

$\equiv \pi j \cdot n \cdot \delta_j \text{ mod } m \cdot n$. Para quaisquer $k \in \left\{ 1, \dots, \frac{n-1}{2} \right\}$ e $g \in \{0, \dots, m-1\}$

existe $u \in \mathbb{Z}$ tal que $c \cdot (k + g \cdot n) = (\rho k + u \cdot n) \cdot e_k$ e $u \equiv g' \text{ mod } m$ para um certo $g' \in \{0, \dots, m-1\}$; portanto, $c \cdot (k + g \cdot n) \equiv (\rho k + g' \cdot n) \cdot e_k \text{ mod } m \cdot n$. Resulta que

$$\left(\frac{c}{m \cdot n} \right) = \prod_{j=1}^{(m-1)/2} \delta_j \cdot \prod_{k=1}^{(n-1)/2} e_k^m = \prod_{j=1}^{(m-1)/2} \delta_j \cdot \prod_{k=1}^{(n-1)/2} e_k = \left(\frac{c}{m} \right) \cdot \left(\frac{c}{n} \right). \quad \square$$

Note-se que o semi-sistema mod $m \cdot n$ construído nesta demonstração não é o natural, o que justifica o uso de (16.2 b), em lugar da fórmula mais intuitiva (16.4), para a definição do símbolo de Jacobi.

A propriedade mais importante do símbolo de Jacobi é a seguinte "lei de reciprocidade quadrática".

(16.6) TEOREMA. Sejam $m, n \in \mathbb{N}$ ímpares tais que $\text{MDC}(m, n) = 1$. Então

$$\left(\frac{n}{m} \right) \cdot \left(\frac{m}{n} \right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}.$$

Demonstração. Consideremos o conjunto $\mathcal{R} = \{(j, k) \mid j = 1, \dots, \frac{m-1}{2}; k = 1, \dots, \frac{n-1}{2}\}$ e os subconjuntos $\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \mathcal{R}_4$ dos

pares $(j, k) \in \mathcal{R}$ tais que $n \cdot j - m \cdot k \leq -\frac{m}{2}$, $-\frac{m}{2} < n \cdot j - m \cdot k < 0$,

$0 < n \cdot j - m \cdot k < \frac{n}{2}$ e $\frac{n}{2} \leq n \cdot j - m \cdot k$, respectivamente. Como

$\text{MDC}(m, n) = 1$, temos que $n \cdot j - m \cdot k \neq 0$; portanto $\mathcal{R} = \mathcal{R}_1 \dot{\cup} \mathcal{R}_2 \dot{\cup} \mathcal{R}_3 \dot{\cup} \mathcal{R}_4$ (reunião disjunta).

A aplicação de $\mathcal{R}$ em $\mathcal{R}$, definida por $(j, k) \mapsto \left(\frac{m+1}{2} - j, \frac{n+1}{2} - k \right)$,

induz obviamente uma bijeção de $\mathcal{R}_1$ sobre $\mathcal{R}_4$; portanto, $\mathcal{R}_1$ e $\mathcal{R}_4$ têm o mesmo número de elementos, digamos, g .

Afirmamos que a aplicação de $\mathcal{R}$ em $\mathbb{Z}/m \cdot \mathbb{Z}$, definida por $(j, k) \mapsto n \cdot j + m \cdot k$, induz uma bijeção de $\mathcal{R}_2$ sobre $n \cdot P_m \cap N_m$. De fato, para qualquer $(j, k) \in \mathcal{R}_2$ existe $j' \in \left\{1, \dots, \frac{m-1}{2}\right\}$ tal que $n \cdot j \equiv -j' \pmod{m}$; logo $n \cdot j + m \cdot k \in n \cdot P_m \cap N_m$. Por outro lado, toda classe pertencente a $n \cdot P_m \cap N_m$ é da forma $n \cdot j + m \cdot k = -j' + m \cdot k$, com $j, j' \in \left\{1, \dots, \frac{m-1}{2}\right\}$

univocamente determinados, logo existe $k \in \mathbb{Z}$ tal que $-\frac{m}{2} < n \cdot j - m \cdot k < 0$.

Obviamente $k > 0$ e $m \cdot k < n \cdot j + \frac{m}{2} < n \cdot \frac{m}{2} + \frac{m}{2} = m \cdot \frac{n+1}{2}$; logo $k < \frac{n+1}{2}$, isto é, $k \in \left\{1, \dots, \frac{n-1}{2}\right\}$, e assim $(j, k) \in \mathcal{R}_2$; portanto, a aplicação indicada é sobrejetiva. Ela é também injetiva, pois de $(j_1, k_1), (j_2, k_2) \in \mathcal{R}_2$ e $n \cdot j_1 + m \cdot k_1 = n \cdot j_2 + m \cdot k_2$ decorre que $j_1 = j_2$ e $k_1 = k_2$.

Como $\mathcal{R}_3 = \left\{(j, k) \in \mathcal{R} \mid -\frac{n}{2} < m \cdot k - n \cdot j < 0\right\}$, mostra-se analogamente que a aplicação de $\mathcal{R}$ em $\mathbb{Z}/n \cdot \mathbb{Z}$, definida por $(j, k) \mapsto m \cdot k + n \cdot j$, induz uma bijeção de $\mathcal{R}_3$ sobre $m \cdot P_n \cap N_n$.

Usando (16.4), concluímos que $\left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) = (-1)^{g_2 + g_3}$, onde g_2 (respectivamente g_3) é o número de elementos de $\mathcal{R}_2$ (respectivamente $\mathcal{R}_3$). A igualdade afirmada resulta então de $\frac{m-1}{2} \cdot \frac{n-1}{2} = g_2 + g_3 + 2g \equiv g_2 + g_3 \pmod{2}$. $\square$

A lei de reciprocidade quadrática pode ser formulada também de outras maneiras. Multiplicando a igualdade indicada em (16.6) por $\left(\frac{m}{n}\right)$, obtemos a igualdade

$$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \cdot \left(\frac{m}{n}\right),$$

e, analisando os expoentes, obtemos o seguinte:

(16.7) COROLÁRIO. Sejam $m, n \in \mathbb{N}$ ímpares tais que $\text{MDC}(m, n) = 1$.
Então,

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \text{ se e somente se } m \equiv 1 \pmod{4} \text{ ou } n \equiv 1 \pmod{4};$$

$$\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) \text{ se e somente se } m \equiv n \equiv 3 \pmod{4}.$$

Para números arbitrários $c \in \mathbb{Z}$ tais que $\text{MDC}(m, c) = 1$, o símbolo de Jacobi $\left(\frac{c}{m}\right)$ pode ser reduzido, por (16.5b), aos símbolos $\left(\frac{-1}{m}\right)$, $\left(\frac{2}{m}\right)$ e $\left(\frac{n}{m}\right)$, onde n é positivo e ímpar. Para os dois primeiros valem as seguintes "fórmulas complementares":

(16.8) TEOREMA. Para qualquer número $m \in \mathbb{N}$ ímpar temos que

$$\text{a) } \left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}$$

$$\text{b) } \left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$$

Demonstração. a) Resulta de (16.4), uma vez que $-1 \cdot P_m = N_m$ tem $\frac{m-1}{2}$ elementos.

b) No caso em que $m \equiv 1 \pmod{4}$, teremos que $2 \cdot j + m \cdot \mathbb{Z} \in P_m$ se e somente se $j \in \left\{1, \dots, \frac{m-1}{4}\right\}$; portanto, cada um dos conjuntos $2 \cdot P_m \cap P_m$ e $2 \cdot P_m \cap N_m$ tem $\frac{m-1}{4}$ elementos. No caso em que $m \equiv 3 \pmod{4}$, tere-

mos que $2 \cdot j + m \cdot \mathbb{Z} \in P_m$ se e somente se $j \in \left\{1, \dots, \frac{m-3}{4}\right\}$; portanto $2 \cdot P_m \cap P_m$ tem $\frac{m-3}{4}$ elementos, e assim $2 \cdot P_m \cap N_m$ tem $\frac{m+1}{4}$ elementos. Concluímos de (16.4) que $\left(\frac{2}{m}\right) = (-1)^{(m-1)/4} = (-1)^{\frac{m-1}{4} \cdot \frac{m+1}{2}}$

no caso em que $m \equiv 1 \pmod{4}$, e $\left(\frac{2}{m}\right) = (-1)^{(m+1)/4} = (-1)^{\frac{m+1}{4} \cdot \frac{m-1}{2}}$

no caso em que $m \equiv 3 \pmod{4}$; portanto, $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$ em ambos os casos. $\square$

Mais tarde utilizaremos a seguinte versão da lei de reciprocidade, estendida a números c negativos.

(16.9) COROLÁRIO. *Sejam $m \in \mathbb{N}$ e $c \in \mathbb{Z}$ números ímpares tais que $\text{MDC}(m, c) = 1$. Então*

$$\left(\frac{c}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{c-1}{2}} \left(\frac{m}{|c|}\right).$$

Demonstração. Podemos-nos restringir ao caso em que $c < 0$, digamos $c = -n$, com $n \in \mathbb{N}$; então temos que

$$\left(\frac{c}{m}\right) = (-1)^{\frac{m-1}{2}} \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \left(1 + \frac{n-1}{2}\right)} \left(\frac{m}{n}\right),$$

por (16.5b), (16.8a) e (16.6). De $1 + \frac{n-1}{2} = \frac{1-n}{2} \equiv \frac{c-1}{2} \pmod{2}$ resulta a igualdade afirmada. $\square$

Usando as fórmulas indicadas em (16.5), (16.6), (16.8) e (16.9), é fácil calcular o símbolo de Jacobi $\left(\frac{c}{m}\right)$ para quaisquer $m \in \mathbb{N}$ ímpar e $c \in \mathbb{Z}$ tais que $\text{MDC}(m, c) = 1$. Por exemplo, usando (16.5) e (16.8 a), obtemos que

$$\left(\frac{1309}{325}\right) = \left(\frac{1309}{5}\right)^2 \cdot \left(\frac{1309}{13}\right) = \left(\frac{-4}{13}\right) = \left(\frac{2}{13}\right)^2 \cdot \left(\frac{-1}{13}\right) = (-1)^6 = 1.$$

Usando (16.8 b) e (16.9), obtemos que

$$\left(\frac{-6}{19}\right) = \left(\frac{2}{19}\right) \cdot \left(\frac{-3}{19}\right) = (-1)^{45} \cdot (-1)^{-18} \cdot \left(\frac{19}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

A seguir, voltaremos ao estudo dos restos quadráticos módulo um número primo ímpar p , usando os resultados obtidos para o símbolo de Jacobi $\left(\frac{c}{p}\right)$ e o fato de este coincidir com o símbolo de Legendre.

Substituindo m por p em (16.4), obtemos o “critério de Gauss” que permite decidir, a partir da paridade do número de elementos de $c \cdot P_p \cap N_p$, se c é resto quadrático mod p ou não. Fazendo a mesma substituição no Corolário (16.7), obtemos a lei de reciprocidade quadrática na versão dada por Gauss:

(16.10) COROLÁRIO. Sejam p, q números primos ímpares distintos.

- a) No caso em que $p \equiv 1 \pmod{4}$ ou $q \equiv 1 \pmod{4}$, p será resto quadrático mod q se e somente se q for resto quadrático mod p .
- b) No caso em que $p \equiv q \equiv 3 \pmod{4}$, p será resto quadrático mod q se e somente se q não for resto quadrático mod p .

Finalmente, das "fórmulas complementares" (16.8) resulta:

(16.11) COROLÁRIO. Seja p um número primo ímpar. Então,

- a) -1 será resto quadrático mod p se e somente se $p \equiv 1 \pmod{4}$.
- b) 2 será resto quadrático mod p se e somente se $p \equiv 1$ ou $-1 \pmod{8}$.

Mostraremos a seguir que, para números primos ímpares q em lugar de 2, vale uma afirmação análoga à de (16.11 b). Para prová-la, utilizaremos o seguinte fato:

(16.12) Sejam q um número primo ímpar e $c \in \mathbb{Z}$ um resto quadrático mod q tal que $c \equiv 1 \pmod{4}$. Então, existe um número ímpar $a \in \{1, 3, \dots, q-2\}$ tal que $c \equiv a^2 \pmod{4q}$.

Demonstração. Temos que $c \equiv a^2 \pmod{q}$ para algum $a \in \{1, 2, \dots, q-2, q-1\}$, logo também $c \equiv (q-a)^2 \pmod{q}$. Como a e $q-a$ têm paridades diferentes e $q-a \in \{1, 2, \dots, q-2, q-1\}$, podemos supor que a seja ímpar; portanto $a^2 \equiv 1 \pmod{4}$. Como $c \equiv 1 \pmod{4}$, concluímos que $c - a^2$ é divisível por $4q$. $\square$

Os números primos ímpares q que são restos quadráticos mod p podem ser caracterizados da seguinte maneira.

(16.13) TEOREMA. Sejam p, q números primos ímpares distintos. As seguintes condições são equivalentes:

- (i) q é resto quadrático mod p .
- (ii) Existe um número ímpar $a \in \{1, 3, \dots, q-2\}$ tal que $p \equiv a^2$ ou $\equiv -a^2 \pmod{4q}$.

Demonstração. (i) $\Rightarrow$ (ii): Seja $c = (-1)^{\frac{p-1}{2}} \cdot p$; então, temos que $c \equiv 1 \pmod{4}$, e de (16.9) resulta que $\left(\frac{c}{q}\right) = \left(\frac{q}{p}\right)$. Portanto, (i)

implica que c é resto quadrático mod q . Por (16.12) existe $a \in \{1, 3, \dots, q-2\}$ tal que $c \equiv a^2 \pmod{4q}$; portanto $p \equiv a^2$ ou $\equiv -a^2 \pmod{4q}$.

(ii) $\Rightarrow$ (i): No caso em que $p \equiv a^2 \pmod{4q}$ para algum $a \in \{1, 3, \dots, q-2\}$ temos que $p \equiv a^2 \pmod{q}$ e $p \equiv a^2 \equiv 1 \pmod{4}$; portanto, $\left(\frac{p}{q}\right) = 1$ e $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, por (16.10). No caso em que $p \equiv -a^2 \pmod{4q}$ para algum $a \in \{1, 3, \dots, q-2\}$ temos que $-p \equiv a^2 \pmod{q}$ e $-p \equiv a^2 \equiv 1 \pmod{4}$; logo $\left(\frac{-p}{q}\right) = 1$ e $\left(\frac{-p}{q}\right) = \left(\frac{q}{p}\right)$, por (16.9). Em ambos os casos, q é resto quadrático mod p . $\square$

Provaremos ainda a seguinte afirmação sobre o símbolo de Jacobi, a qual será utilizada, com $k=3$, na demonstração do teorema (16.15).

(16.14) *Seja $m \in \mathbb{N}$ um número ímpar que não é um quadrado e seja $k \in \mathbb{N}$. Então existe $c \in \mathbb{Z}$ tal que $c \equiv 1 \pmod{2^k}$, $\text{MDC}(m, c) = 1$ e $\left(\frac{c}{m}\right) = -1$.*

Demonstração. Seja $m = p_1^{r_1} \cdot \dots \cdot p_s^{r_s}$ a fatoração de m em números primos $p_1, \dots, p_s$, necessariamente ímpares; como m não é um quadrado, podemos supor que r_1 é ímpar. Os números $1 + j \cdot 2^k$ ($j = 0, \dots, p_1 - 1$) são incôngruos mod p_1 , dois a dois, uma vez que $2 + p_1 \cdot \mathbb{Z} \in \mathbb{F}_{p_1}^*$, e, portanto, formam um sistema de representantes de $\mathbb{F}_{p_1}$. Entre estes números, existem $\frac{p_1-1}{2} \geq 1$ que representam não-quadrados em $\mathbb{F}_{p_1}^*$; portanto existe $b \in \{1 + j \cdot 2^k \mid j = 0, \dots, p_1 - 1\}$ tal que $\left(\frac{b}{p_1}\right) = -1$. Por (6.5), existe $c \in \mathbb{Z}$ tal que $c \equiv b \pmod{2^k \cdot p_1}$ e $c \equiv 1 \pmod{p_i}$ ($i = 2, \dots, s$); logo $c \equiv b \equiv 1 \pmod{2^k}$, $\text{MDC}(p_1, c) = \text{MDC}(p_1, b) = 1$ e $\text{MDC}(p_i, c) = 1$ ($i = 2, \dots, s$), e assim $\text{MDC}(m, c) = 1$. De (16.5a) resulta que

$$\left(\frac{c}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1 \text{ e } \left(\frac{c}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1 \text{ (} i = 2, \dots, s \text{);}$$

logo

$$\left(\frac{c}{m}\right) = \prod_{i=1}^s \left(\frac{c}{p_i}\right)^{r_i} = -1, \text{ por (16.5c). } \square$$

Como já foi anunciado, a lei de reciprocidade quadrática permite provar a lei de decomposição, que afirma que o tipo de decomposição em $L = \mathbb{Q}(\sqrt{d})$ de cada número primo p que não dividir o discriminante

d_L , dependerá somente da classe de $p \bmod |d_L|$. Na verdade, demonstraremos uma afirmação mais forte, a saber, a existência de um homomorfismo $\bar{\chi}_L$ do grupo $U(\mathbb{Z}/d_L \cdot \mathbb{Z})$ sobre o grupo multiplicativo $\{1, -1\}$ com a seguinte propriedade: Um número primo qualquer p será decomposto (respectivamente inerte) em L se e somente se $\bar{\chi}_L(p + d_L \cdot \mathbb{Z}) = 1$ (respectivamente -1).

Tal homomorfismo $\bar{\chi}_L$ será obtido a partir da aplicação χ_L de $S_L = \{c \in \mathbb{Z} \mid \text{MDC}(d_L, c) = 1\}$ em $\{1, -1\}$, definida da seguinte maneira:

$$\chi_L c = \begin{cases} \left(\frac{c}{|d|} \right) & \text{no caso em que } d \equiv 1 \pmod{4} \\ (-1)^{(c-1)/2} \cdot \left(\frac{c}{|d|} \right) & \text{no caso em que } d \equiv 3 \pmod{4} \\ (-1)^{\frac{c^2-1}{8} + \frac{c-1}{2} \cdot \frac{d'-1}{2}} \cdot \left(\frac{c}{|d'|} \right) & \text{no caso em que} \\ & d \equiv 2 \pmod{4}, \text{ sendo } d = 2 \cdot d', d' \text{ ímpar.} \end{cases}$$

Note-se que, nos casos $d \equiv 3$ ou $2 \pmod{4}$, S_L consiste apenas de números ímpares, uma vez que 2 divide $d_L = 4 \cdot d$.

(16.15) TEOREMA. Seja $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$.

- a) Se $b, c \in S_L$ tais que $b \equiv c \pmod{|d_L|}$ então $\chi_L b = \chi_L c$.
- b) χ_L é um homomorfismo multiplicativo de S_L sobre $\{1, -1\}$.
- c) Um número primo qualquer $p \in S_L$ será decomposto (respectivamente inerte) em L se e somente se $\chi_L p = 1$ (respectivamente -1).

Demonstração. a) No caso em que $d \equiv 3 \pmod{4}$, a congruência $b \equiv c \pmod{|d_L|}$ implica que $b \equiv c \pmod{|d|}$ e $b \equiv c \pmod{4}$; logo $\frac{b-1}{2} \equiv \frac{c-1}{2}$

$\pmod{2}$. No caso em que $d \equiv 2 \pmod{4}$, $d' = \frac{d}{2}$, a congruência $b \equiv c \pmod{|d_L|}$

implica que $b \equiv c \pmod{|d'|}$ e $b \equiv c \pmod{8}$; portanto $\frac{b-1}{2} \equiv \frac{c-1}{2} \pmod{2}$ e

$\frac{b^2-1}{8} \equiv \frac{c^2-1}{8} \pmod{2}$. A afirmação resulta então de (16.5a) e da definição de χ_L .

b) De (16.5b) e do fato que $\frac{b \cdot c - 1}{2} \equiv \frac{b-1}{2} + \frac{c-1}{2} \pmod{2}$ e $\frac{(b \cdot c)^2 - 1}{8} \equiv \frac{b^2 - 1}{8} + \frac{c^2 - 1}{8} \pmod{2}$, para quaisquer $b, c \in \mathbb{Z}$ ímpares, resulta que χ_L é um homomorfismo. Ele é sobrejetivo, pois por (16.14) existe $c \in S_L$ tal que $c \equiv 1 \pmod{8}$ e $\left(\frac{c}{|d''|}\right) = -1$, onde $d'' = d \left(\text{respectivamente } \frac{d}{2}\right)$ no caso em que $d \equiv 1$ ou 3 (respectivamente $\equiv 2$) $\pmod{4}$; portanto, $\chi_L c = \left(\frac{c}{|d''|}\right) = -1$, pela definição de χ_L .

c) Suponhamos que $2 \in S_L$; então d_L é ímpar, logo $d \equiv 1 \pmod{4}$, logo $\chi_L 2 = \left(\frac{2}{|d|}\right) = (-1)^{(d^2-1)/8}$, por (16.8). Concluimos que $\chi_L 2 = 1$ (respectivamente $= -1$) se e somente se $d \equiv 1$ (respectivamente $\equiv 5$) $\pmod{8}$. Seja $p \in S_L$ um número primo ímpar. No caso em que $d \equiv 1$ ou $3 \pmod{4}$ temos que $\left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{d-1}{2}} \cdot \left(\frac{p}{|d|}\right)$, por (16.9), e no caso em que $d \equiv 2 \pmod{4}$ temos que

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{d'}{p}\right) = (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{d'-1}{2}} \cdot \left(\frac{p}{|d'|}\right),$$

por (16.5b), (16.8b) e (16.9); portanto, temos que $\left(\frac{d}{p}\right) = \chi_L p$ em ambos os casos. A afirmação c) resulta então de (15.2) e (15.3). $\square$

Como consequência imediata obtemos o seguinte:

(16.16) COROLÁRIO. O homomorfismo χ_L induz um homomorfismo $\bar{\chi}_L$ do grupo $U(\mathbb{Z}/d_L \cdot \mathbb{Z})$ sobre o grupo multiplicativo $\{1, -1\}$ com a seguinte propriedade:

Um número primo qualquer p que não dividir d_L será decomposto (respectivamente inerte) em L se e somente se $\bar{\chi}_L(p + d_L \cdot \mathbb{Z}) = 1$ (respectivamente -1).

Obviamente, o núcleo de $\bar{\chi}_L$ é um subgrupo V_L de $U(\mathbb{Z}/d_L \cdot \mathbb{Z})$ de índice 2 e, portanto, tem ordem $\frac{1}{2} \cdot \varphi(|d_L|)$, e $\bar{\chi}_L$ é o único homomorfismo de $U(\mathbb{Z}/d_L \cdot \mathbb{Z})$ sobre $\{1, -1\}$ com núcleo V_L . Por isto, a afirmação principal de (16.16) pode ser reformulada em termos de V_L :

(16.17) COROLÁRIO. Um número primo qualquer p que não dividir d_L será decomposto (respectivamente inerte) em L se e somente se $p + d_L \cdot \mathbb{Z} \in V_L$ (respectivamente $\in U(\mathbb{Z}/d_L \cdot \mathbb{Z}) \setminus V_L$).

Note-se que, em geral, V_L não é o único subgrupo de $U(\mathbb{Z}/d_L \cdot \mathbb{Z})$ de índice 2.

O homomorfismo χ_L é chamado o *caráter quadrático* de L e é usualmente estendido a um homomorfismo do semigrupo multiplicativo $\mathbb{Z}$ sobre o semigrupo multiplicativo $\{1, -1, 0\}$, definindo-se $\chi_L c = 0$ para qualquer $c \in \mathbb{Z}S_L$. Analogamente, estende-se $\bar{\chi}_L$ a um homomorfismo do semigrupo multiplicativo $\mathbb{Z}/d_L \cdot \mathbb{Z}$ sobre o semigrupo $\{1, -1, 0\}$. Obtemos assim o seguinte

(16.18) COROLÁRIO. Para qualquer número primo p teremos que

$$\chi_{Lp} = \begin{cases} 1 & \text{se e somente se } p \text{ for decomposto em } L; \\ -1 & \text{se e somente se } p \text{ for inerte em } L; \\ 0 & \text{se e somente se } p \text{ for ramificado em } L. \end{cases}$$

Obviamente, neste corolário, χ_{Lp} pode ser substituído por $\bar{\chi}_L(p + d_L \cdot \mathbb{Z})$.

Observamos ainda que, devido ao teorema de Dirichlet sobre progressões aritméticas, toda classe $\alpha \in U(\mathbb{Z}/d_L \cdot \mathbb{Z})$ contém uma infinidade de números primos. Portanto, existe uma infinidade de números primos decompostos e uma infinidade de números primos inertes em L .

Finalmente, gostaríamos de chamar a atenção para a semelhança existente entre a lei de decomposição para corpos quadráticos e para corpos ciclotômicos. Para isto, observamos primeiro que a afirmação de (16.15c) pode ser reformulada da seguinte maneira:

“Para qualquer número primo $p \in S_L$, a ordem de χ_{Lp} (no grupo $\{(1, -1)\}$) é igual ao grau de inércia $f(\mathfrak{P})$, para todo ideal primo $\mathfrak{P}$ de I_L que está acima de p .”

No caso do m -ésimo corpo ciclotômico $L = L_m$ (onde $m > 1$ é ímpar ou divisível por 4), o homomorfismo canônico de $\mathbb{Z}$ sobre $\mathbb{Z}/m \cdot \mathbb{Z}$ induz um homomorfismo multiplicativo ψ_L do semigrupo

$$S_L = \{c \in \mathbb{Z} \mid \text{MDC}(m, c) = 1\}$$

sobre $U(\mathbb{Z}/m \cdot \mathbb{Z})$ o qual, por (14.4), possui uma propriedade análoga. Observando-se que m e $\text{disc}(\phi_m)$ têm os mesmos divisores primos (veja

(14.2)), a analogia torna-se ainda mais completa quando se usa os fatos (mencionados, mas não demonstrados, nos §3-4) que $d_L = \text{disc}(\phi_m)$ e $m \mid d_L$, pois destes fatos resulta que $S_L = \{c \in \mathbb{Z} \mid \text{MDC}(d_L, c) = 1\}$, e que $\psi_L p$ depende apenas da classe de $p \bmod \mid d_L \mid$.

Observemos ainda que no caso em que L é um corpo quadrático (respectivamente o m -ésimo corpo ciclotômico), o grupo $\{1, -1\}$ (respectivamente $U(\mathbb{Z}/m \cdot \mathbb{Z})$) é canonicamente isomorfo a, e portanto pode ser identificado com, o grupo de Galois $\text{Aut}(L \mid \mathbb{Q})$. Assim o homomorfismo acima indicado χ_L (respectivamente ψ_L) pode ser considerado como caso especial do homomorfismo da “lei de reciprocidade generalizada”, a qual vale para qualquer extensão abeliana finita L de qualquer corpo de números algébricos K . Trata-se de um homomorfismo $\theta_{L \mid K}$ do grupo $\mathcal{F}_{L \mid K}$ de ideais fracionários de I_K , gerado pelos ideais primos que não dividem o ideal discriminante $\mathfrak{b}_{I_L \mid I_K}$, sobre o grupo abeliano $\text{Aut}(L \mid K)$, que tem a seguinte propriedade: Para qualquer ideal primo $\mathfrak{p} \in \mathcal{F}_{L \mid K}$ (necessariamente não-ramificado em L), a ordem de $\theta_{L \mid K} \mathfrak{p}$ é igual ao grau de inércia $f(\mathfrak{p} \mid \mathfrak{p})$, para todo ideal primo $\mathfrak{p}$ de I_L acima de $\mathfrak{p}$ (veja Artin [2] ou Voloch [36]).

EXERCÍCIOS

- 16.1. Sejam $n \in \mathbb{N}$, $a_1, \dots, a_n$ um sistema de representantes de $\mathbb{Z}/n \cdot \mathbb{Z}$, $b \in \mathbb{Z}$ tal que $\text{MDC}(n, b) = 1$ e $c \in \mathbb{Z}$. Prove que $c + b \cdot a_j$ ($j = 1, \dots, n$) é um sistema de representantes de $\mathbb{Z}/n \cdot \mathbb{Z}$.
- 16.2. a) Seja $m \geq 3$ tal que $U(\mathbb{Z}/m \cdot \mathbb{Z})$ seja cíclico. Prove que $U(\mathbb{Z}/m \cdot \mathbb{Z})$ possui $\frac{\varphi(m)}{2}$ quadrados e $\frac{\varphi(m)}{2}$ não-quadrados.
 b) Determine os quadrados nos grupos $U(\mathbb{Z}/2^k \cdot \mathbb{Z})$, para $k \geq 2$, e no grupo $U(\mathbb{Z}/12 \cdot \mathbb{Z})$.
- 16.3. Utilize os seguintes métodos para decidir se -186 é um resto quadrático $\bmod p = 29$:
 a) Indique um sistema de representantes dos quadrados em $\mathbb{F}_p^*$ e verifique se -186 é congruo $\bmod p$ a um desses representantes.
 b) Aplique o critério de Euler.
 c) Aplique o critério de Gauss.
 d) Calcule $\left(\frac{-186}{29}\right)$, usando (16.5), (16.6) e (16.8).

- 16.4. Mostre que 1979 é inerte em $\mathbb{Q}(\sqrt{1987})$ e decomposto em $\mathbb{Q}(\sqrt{-1987})$.
- 16.5. Sejam p, q números primos distintos, $p \neq 2$, e $L = \mathbb{Q}(\sqrt{q})$. Prove:
- No caso em que $q = 2$, p será decomposto em L se e somente se $p \equiv 1$ ou $\equiv -1 \pmod{8}$.
 - No caso em que $q \equiv 1$ (respectivamente 3) $\pmod{4}$, p será decomposto em L se e somente se $p \equiv a^2 \pmod{q}$ (respectivamente $\equiv a^2$ ou $\equiv -a^2 \pmod{4 \cdot q}$) para algum $a \in \{1, 3, \dots, q-2\}$.
- 16.6. Seja $L = \mathbb{Q}(\sqrt{-q})$ onde q é um número primo. Caracterize os números primos p que são decompostos em L , através das suas classes $\pmod{q}$ ou $\pmod{4 \cdot q}$.
- 16.7. Indique números primos $p_j \equiv 2^j \pmod{11}$ ($j = 0, 1, \dots, 9$) e prove que p_1, p_3, p_5, p_7, p_9 (respectivamente p_0, p_2, p_4, p_6, p_8) são inertes (respectivamente decompostos) em $\mathbb{Q}(\sqrt{-11})$.
- 16.8. Seja m um número natural ímpar que não é um quadrado. Prove que existem números primos ímpares p, p' que não dividem m e tais que $\left(\frac{m}{p}\right) = \left(\frac{-m}{p'}\right) = -1$.
(Sugestão: Use (16.14), (16.9) e (16.5 c)).
- 16.9. Seja $m \in \mathbb{Z} \setminus \{0\}$. Prove que m será um quadrado em $\mathbb{Z}$ se e somente se for um resto quadrático $\pmod{p}$ para todo número primo p que não dividir m . (Veja LeVeque [24], Chapter 5; ou Ribenboim [28], Chapter 4; ou Viswanathan [35], Cap. VI).
- 16.10. Para cada um dos seguintes corpos quadráticos $L = \mathbb{Q}(\sqrt{d})$, onde $d \in \{-7, -6, -5, -3, -2, -1, 2, 3, 5, 6, 7\}$,
- determine o subgrupo V_L de $U(\mathbb{Z}/d_L \cdot \mathbb{Z})$;
 - indique um sistema de representantes de $U(\mathbb{Z}/d_L \cdot \mathbb{Z})$ que consista de números primos. Quais destes números primos são decompostos (respectivamente inertes) em L ?
- 16.11. Seja p um número primo e $c \in \mathbb{Z}$ tal que p não divide c . Prove que se existirem $m, n \in \mathbb{N}$ tais que $p = m^2 + a \cdot n^2$ então $-c$ será um resto quadrático $\pmod{p}$.
- 16.12. Indique números $m, n \in \mathbb{N}$, m ímpar e $\text{MDC}(m, n) = 1$, tais que $\left(\frac{n}{m}\right) = 1$ e $n \not\equiv a^2 \pmod{m}$ para qualquer $a \in \mathbb{N}$.

- 16.13. Prove a lei de reciprocidade quadrática e as fórmulas complementares para o símbolo de Jacobi, a partir da sua validade para o símbolo de Legendre.
- 16.14. Sejam p e q números primos ímpares distintos, $\bar{1}$ (respectivamente $\tilde{1}$) a unidade do corpo $\mathbb{F}_p$ (respectivamente $\mathbb{F}_q$) e ζ uma raiz primitiva p -ésima da unidade numa extensão de $\mathbb{F}_q$. Para qualquer $\bar{c} \in \mathbb{F}_p$ denotamos por $c \in \mathbb{Z}$ um representante de $\bar{c}$. Prove que
- para qualquer $\bar{c} \in \mathbb{F}_p^*$, a “soma de Gauss” $\tau(\bar{c}) = \sum_{\bar{x} \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \cdot \zeta^{c \cdot x}$ independe da escolha dos representantes c e x ;
 - para qualquer $\bar{c} \in \mathbb{F}_p^*$ temos que $\tau(\bar{c}) = \left(\frac{c}{p}\right) \cdot \tau(\bar{1})$;
 - $\tau(\bar{1})^2 = (-1)^{(p-1)/2} \cdot p \cdot \tilde{1}$ e $\tau(\bar{1})^{q-1} = \left(\frac{q}{p}\right) \cdot \tilde{1}$.
 - Usando o critério de Euler (16.1), conclua que

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right).$$

(Veja Samuel [30], §5.5, ou Ribenboim [28], Chapter 4.)

CAPÍTULO VI

O MÉTODO GEOMÉTRICO

O método geométrico é utilizado, na teoria dos números algébricos, principalmente para duas finalidades, a saber:

- 1) para o estudo do número de classes h_L ,
- 2) para o estudo do grupo dos invertíveis $U(I_L)$,

sendo L um corpo de números algébricos.

Quando se tratar de provar apenas a finitude de h_L , o método geométrico será dispensável, uma vez que, em lugar da “cota de Minkowski” obtida geometricamente, pode ser usada uma outra cota, calculada facilmente através do “princípio de gavetas”, como foi exposto no §10. A cota de Minkowski, entretanto, é importante para se obter uma boa estimativa para o discriminante d_L e, em certos casos, é útil para se calcular h_L (veja §10).

Neste capítulo, introduzimos o método geométrico a ser usado na demonstração do teorema de invertíveis de Dirichlet (“unit theorem”), que afirma que o grupo dos invertíveis $U(I_L)$ é finitamente gerado de posto $s + t - 1$, onde s (respectivamente t) é o número das imersões reais (respectivamente dos pares conjugados de imersões complexas) de L .

Primeiramente introduziremos no §17 as noções básicas da “geometria dos números”, a saber, as noções de “rede” e “rede completa” no $\mathbb{R}^n$, e demonstraremos o teorema de Minkowski.

No §18 mostraremos que as imersões reais e complexas de L dão origem à “imersão canônica” de L num $\mathbb{R}$ -espaço $\mathbb{L}$ isomorfo a $\mathbb{R}^n$, a qual leva qualquer base de L sobre $\mathbb{Q}$ numa base de rede completa de $\mathbb{L}$. Mais importante ainda é a “representação logarítmica” do grupo multiplicativo L^* no $\mathbb{R}$ -espaço $\mathbb{R}^{s+t}$. O teorema de invertíveis de Dirichlet resultará do fato desta representação levar $U(I_L)$ numa rede completa de uma certa hipersuperfície H de $\mathbb{R}^{s+t}$.

Finalmente, no §19 estudaremos em mais detalhes, para corpos quadráticos reais $L = \mathbb{Q}(\sqrt{d})$, os invertíveis de I_L e, mais geralmente, de qualquer “ordem” S de L . Mostraremos que este estudo está relacionado com a resolubilidade de certas equações diofantinas e, em particular, da “equação de Pell” $X^2 - d \cdot Y^2 = 1$.

§17. Redes no $\mathbb{R}^n$

Seja $\mathbb{L}$ um $\mathbb{R}$ -espaço de dimensão n , isto é, isomorfo ao $\mathbb{R}$ -espaço $\mathbb{R}^n = \underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_n$. Distinguímos em $\mathbb{L}$ uma base $e_1, \dots, e_n$ (por exem-

plo, $e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$ no caso em que $\mathbb{L} = \mathbb{R}^n$), em relação à qual definimos, para vetores $x = \xi_1 \cdot e_1 + \dots + \xi_n \cdot e_n$ e $y = \eta_1 \cdot e_1 + \dots + \eta_n \cdot e_n$, o *produto escalar* $(x, y) = \xi_1 \cdot \eta_1 + \dots + \xi_n \cdot \eta_n$, bem como o *comprimento* $\|x\| = \sqrt{(x, x)} = \sqrt{\xi_1^2 + \dots + \xi_n^2}$ do vetor $x \in \mathbb{L}$. Denotamos por B_ρ a *bola de raio* ρ ao redor de 0, isto é, $B_\rho = \{x \in \mathbb{L} \mid \|x\| \leq \rho\}$.

Dados $z_1, \dots, z_m \in \mathbb{L}$, consideramos os conjuntos

$$M = \mathbb{Z} \cdot z_1 + \dots + \mathbb{Z} \cdot z_m = \left\{ \sum_{i=1}^m a_i \cdot z_i \mid a_1, \dots, a_m \in \mathbb{Z} \right\} \quad \text{e}$$

$$T_z = \left\{ \sum_{i=1}^m \rho_i \cdot z_i \mid 0 \leq \rho_i < 1 \ (i = 1, \dots, m) \right\}.$$

Diremos que M é uma *rede de $\mathbb{L}$* quando $z_1, \dots, z_m$ forem linearmente independentes sobre $\mathbb{R}$; neste caso, chamamos $z_1, \dots, z_m$ uma *base de rede* associada a M , e T_z a *malha fundamental* associada a esta base. Obviamente, neste caso temos que $m \leq n$. Se $m = n$, então M e $z_1, \dots, z_n$ serão chamados uma *rede completa* e uma *base de rede completa*, respectivamente.

Diremos que um subconjunto C de $\mathbb{L}$ é *limitado*, se $C \subseteq B_\rho$ para algum $\rho > 0$. Diremos que um subconjunto D de $\mathbb{L}$ é *discreto*, se $D \cap B_\rho$ for finito para todo $\rho > 0$; neste caso, $D \cap C$ é finito, qualquer que seja o subconjunto limitado C de $\mathbb{L}$.

Para saber se um subconjunto M de $\mathbb{L}$ é uma rede, não é necessário conhecer uma base desta rede. De fato:

(17.1) *Um subconjunto M de $\mathbb{L}$ será uma rede de $\mathbb{L}$ se e somente se for um grupo, em relação à adição, e for discreto.*

Demonstração. Suponhamos primeiramente que M seja uma rede de $\mathbb{L}$.

Então, obviamente, M é um grupo aditivo. Suponhamos que $v_1, \dots, v_m$ formem uma base da rede M ; então $m \leq n$, e existem $v_{m+1}, \dots, v_n \in \mathbb{L}$ tais que $v_1, \dots, v_n$ são linearmente independentes sobre $\mathbb{R}$ e, portanto, formam uma base de uma rede completa M' que contém M . Para mostrar

que M é discreto, basta provar que M' o é. Se $w_1, \dots, w_n$ formarem a base dual de $v_1, \dots, v_n$, isto é, $(v_i, w_j) = \delta_{ij}$ ($i, j = 1, \dots, n$); então para todo $z = a_1 \cdot v_1 + \dots + a_n \cdot v_n \in M'$ teremos que $(z, w_j) = a_j$ ($j = 1, \dots, n$). Para todo $\rho > 0$ e todo $z \in M' \cap B_\rho$ temos que $|a_j| = |(z, w_j)| \leq \|z\| \cdot \|w_j\| \leq \rho \cdot \|w_j\|$ ($j = 1, \dots, n$); logo $M' \cap B$ é finito; portanto, M' é discreto.

Por outro lado, seja M um grupo, em relação à adição, e discreto. Suponhamos que $u_1, \dots, u_m$ formem um sistema maximal de elementos de M linearmente independentes sobre $\mathbb{R}$; então $u_1, \dots, u_m$ formam uma base da rede $M_0 = \mathbb{Z} \cdot u_1 + \dots + \mathbb{Z} \cdot u_m$. Sendo T_u a malha fundamental associada a esta base, temos que $(M \cap T_u) + M_0 \subseteq M$, e vale mesmo a igualdade, pois todo $x \in M$ é linearmente dependente (sobre $\mathbb{R}$) de $u_1, \dots, u_m$; logo

$$x = \sum_{i=1}^m a_i \cdot u_i + \sum_{i=1}^m \rho_i \cdot u_i \text{ com } a_i \in \mathbb{Z} \text{ e } 0 \leq \rho_i < 1 \text{ (} i = 1, \dots, m \text{), e assim}$$

$$\sum_{i=1}^m \rho_i \cdot u_i = x - \sum_{i=1}^m a_i \cdot u_i \in M \cap T_u. \text{ Concluímos que a restrição a } M \cap T_u$$

do homomorfismo canônico sobre o grupo quociente M/M_0 é sobrejetivo. Como M é discreto e T_u é limitado, temos que $M \cap T_u$ é finito; logo M/M_0 também o é. Denotando por g a ordem de M/M_0 , temos que $M \subseteq g^{-1} \cdot M_0 = \mathbb{Z} \cdot u'_1 + \dots + \mathbb{Z} \cdot u'_m$, onde $u'_i = g^{-1} \cdot u_i$ ($i = 1, \dots, m$). De (5.1) resulta que M é um $\mathbb{Z}$ -módulo livre, de um posto $k \leq m$, logo possui uma base $v_1, \dots, v_k$. Das inclusões $M_0 \subseteq M \subseteq g^{-1} \cdot M_0$ resulta que os $\mathbb{R}$ -espaços gerados por estes $\mathbb{Z}$ -módulos coincidem, isto é, $\mathbb{R} \cdot u_1 + \dots + \mathbb{R} \cdot u_m = \mathbb{R} \cdot v_1 + \dots + \mathbb{R} \cdot v_k$, donde concluímos que $k = m$ e que $v_1, \dots, v_k$ são linearmente independentes sobre $\mathbb{R}$. Portanto M é uma rede de $\mathbb{L}$. $\square$

Dada uma rede M , consideramos, além da malha fundamental T_u , também as outras malhas $z + T_u$ ($z \in M$), associadas a uma base $v_1, \dots, v_m$ da rede M . Mostraremos que todo conjunto limitado intersecta apenas um número finito destas malhas.

(17.2) *Seja T_u a malha fundamental associada à base $v_1, \dots, v_m$ da rede M , e seja C um subconjunto limitado de $\mathbb{L}$. Então $C \cap (z + T_u) = \emptyset$ para quase todos os $z \in M$.*

Demonstração. Para todo $t = \sum_{i=1}^m \rho_i \cdot v_i \in T_u$ temos que

$$\|t\| \leq \sum_{i=1}^m \|\rho_i v_i\| = \sum_{i=1}^m |\rho_i| \cdot \|v_i\| \leq \tau,$$

onde $\tau = \sum_{i=1}^m \|v_i\|$. Supondo, sem perda de generalidade, que $C = B_\rho$ para algum $\rho > 0$, consideramos $z \in M$ tal que $B_\rho \cap (z + T) \neq \emptyset$; digamos $z + t = x \in B_\rho$ para algum $t \in T$; então $\|z\| = \|x - t\| \leq \|x\| + \|t\| \leq \rho + \tau$, logo $z \in B_{\rho+\tau}$. Como M é discreto, por (17.1), o conjunto $M \cap B_{\rho+\tau}$ é finito, donde resulta a afirmação. $\square$

Quanto às redes completas, é intuitivamente claro que a reunião de todas as malhas associadas a uma base de rede completa cobre o espaço todo $\mathbb{L}$. Além de provar isto, mostraremos a seguir que as redes completas podem ser caracterizadas por uma propriedade mais fraca, a saber, pela existência de um conjunto limitado C tal que $\bigcup_{z \in M} (z + C) = \mathbb{L}$.

(17.3) TEOREMA. *Seja M uma rede em $\mathbb{L}$. As seguintes condições são equivalentes:*

- (i) M é uma rede completa de $\mathbb{L}$;
- (ii) Existe um subconjunto limitado C de $\mathbb{L}$ tal que $\mathbb{L} = \bigcup_{z \in M} (z + C)$.

Neste caso temos, em particular, que $\mathbb{L} = \bigcup_{z \in M} (z + T)$ (reunião disjunta), sendo T a malha fundamental associada a uma base de M .

Demonstração. (i) $\Rightarrow$ (ii): Para todo $x \in \mathbb{L}$ temos que $x = \sum_{i=1}^n a_i \cdot v_i + \sum_{i=1}^n \rho_i \cdot v_i$ com $a_i \in \mathbb{Z}$ e $0 \leq \rho_i < 1$ ($i = 1, \dots, n$), logo $\mathbb{L} = \bigcup_{z \in M} (z + T_w)$.

A reunião é disjunta, pois de

$$\sum_{i=1}^n a_i \cdot v_i + \sum_{i=1}^n \rho_i \cdot v_i = \sum_{i=1}^n a'_i \cdot v_i + \sum_{i=1}^n \rho'_i \cdot v_i$$

resulta que $a_i + \rho_i = a'_i + \rho'_i$ ($i = 1, \dots, n$) e, portanto, que $a_i = a'_i$, $\rho_i = \rho'_i$ ($i = 1, \dots, n$).

(ii) $\Rightarrow$ (i): Suponhamos que M não seja completa. Dada uma base $u_1, \dots, u_m$ de M , com $m < n$, ela pode ser completada até uma base $u_1, \dots, u_n$ do $\mathbb{R}$ -espaço $\mathbb{L}$. Se $w_1, \dots, w_n$ formarem a base dual de $v_1, \dots, v_m$ então $(z, w_n) = 0$ para todo $z \in M$. Seja $\rho > 0$ tal que $C \subseteq B_\rho$, e seja $y = \rho' \cdot w_n$ para algum $\rho' > \rho$. De (ii) resulta que $y = z + c$, com $z \in M$ e $c \in C$. Como $(z, y) = 0$, concluímos que

$$\|y\|^2 = (z + c, y) = (z, y) + (c, y) \leq \|c\| \cdot \|y\| \leq \rho \cdot \|y\|;$$

logo $\|y\| \leq \rho$, em contradição com $\|y\| = \|\rho' \cdot w_n\| = \rho'$. $\square$

Para prosseguirmos no estudo de redes completas em L , precisamos da noção de *volume em L* . O volume em $\mathbb{R}^n$ é bem conhecido (veja por exemplo Lima [25], Cap. VI, §3) e pode ser facilmente transferido para o $\mathbb{R}$ -espaço L através do isomorfismo natural entre $\mathbb{R}^n$ e L , definido por meio da base distinguida $e_1, \dots, e_n$. Na verdade, é possível se restringir a subconjuntos C de L que são reuniões finitas de paralelepípedos, usando assim apenas as seguintes propriedades do volume:

- a) $\text{vol}(T_v) = |\det(\alpha_{ij})|$, sendo $v_i = \sum_{j=1}^n \alpha_{ij} \cdot e_j$ ($i = 1, \dots, n$; $\alpha_{ij} \in \mathbb{R}$);
- b) $\text{vol}(x + C) = \text{vol}(C)$ para qualquer $x \in L$;
- c) $\text{vol}(\gamma \cdot C) = \gamma^n \cdot \text{vol}(C)$ para qualquer $\gamma \in \mathbb{R}$, $\gamma > 0$;
- d) se $C \cap C' = \emptyset$ então $\text{vol}(C \cup C') = \text{vol}(C) + \text{vol}(C')$;

(veja Greub [11], Chapter X, §3), não havendo necessidade do uso do integral, o qual, entretanto, é indispensável para definir o volume de conjuntos mais gerais (como, por exemplo, o do conjunto C , indicado no Exercício 17.8.).

De a) resulta imediatamente:

(17.4) $v_1, \dots, v_n \in L$ formarão uma base de rede completa em L se e somente se $\text{vol}(T_v) \neq 0$.

Usando a multiplicatividade do determinante, concluímos de (17.4):

(17.5) Seja $w_i = \sum_{j=1}^n \omega_{ij} \cdot v_j$ ($i = 1, \dots, n$), com $\omega_{ij} \in \mathbb{R}$. Então

$$\text{vol}(T_w) = |\det(\omega_{ij})| \cdot \text{vol}(T_v).$$

Obviamente, $w_1, \dots, w_n$ e $v_1, \dots, v_n$ formarão bases da mesma rede completa se e somente se $\omega_{ij} \in \mathbb{Z}$ ($i, j = 1, \dots, n$) e $\det(\omega_{ij}) \in \{1, -1\}$. Por isto, resulta de (17.5) o seguinte:

(17.6) Para todas as bases $v_1, \dots, v_n$ de uma rede completa M , os volumes $\text{vol}(T_v)$ coincidem.

Este volume será denotado por $\text{vol}(M)$. Observamos que é igual ao volume $\text{vol}(z + T_v)$ de todas as malhas associadas a $v_1, \dots, v_n$ ($z \in M$).

É óbvio que os conjuntos $z + C$ ($z \in M$), obtidos de C por deslocamento ao longo de uma rede M , serão disjuntos, dois a dois, somente quando C for suficientemente "pequeno". Mais precisamente, demonstraremos o seguinte:

(17.7) TEOREMA. Seja $C \subseteq \mathbb{L}$ tal que $\text{vol}(C)$ seja definido e seja M uma rede completa de $\mathbb{L}$. Se os conjuntos $z + C$ ($z \in M$) forem disjuntos dois a dois, então $\text{vol}(C) \leq \text{vol}(M)$.

Demonstração. Seja T a malha fundamental associada a uma base de M . Por (17.3) temos que $L = \bigcup_{z \in M} z + T$, logo $C = \bigcup_{z \in M} (C \cap (z + T))$, sendo ambas as reuniões disjuntas. Por (17.2) existem $z_1, \dots, z_r \in M$ tais que $C \cap (z + T) = \emptyset$ para todos os $z \in M \setminus \{z_1, \dots, z_r\}$; logo $C = \bigcup_{i=1}^r (C \cap (z_i + T))$ (reunião disjunta). Como, por hipótese, $-z_i + C$ ($i = 1, \dots, r$) são disjuntos dois a dois, a reunião $\bigcup_{i=1}^r ((-z_i + C) \cap T)$ também é disjunta. Finalmente $C \cap (z_i + T) = ((-z_i + C) \cap T) + z_i$ ($i = 1, \dots, r$); logo

$$\begin{aligned} \text{vol}(C) &= \sum_{i=1}^r \text{vol}(C \cap (z_i + T)) = \sum_{i=1}^r \text{vol}((-z_i + C) \cap T) = \\ &= \text{vol}\left(\bigcup_{i=1}^r (-z_i + C) \cap T\right) \leq \text{vol}(T) = \text{vol}(M). \quad \square \end{aligned}$$

Um subconjunto C de $\mathbb{L}$ será chamado *simétrico* se, para qualquer $c \in C$, tivermos que $-c \in C$. Um subconjunto C de $\mathbb{L}$ será chamado *convexo* se, para quaisquer $c, c' \in C$, o conjunto $\{\rho \cdot c + (1 - \rho) \cdot c' \mid 0 \leq \rho \leq 1\}$ estiver contido em C ; note que este conjunto consiste dos pontos situados entre c e c' , na reta que liga estes dois pontos.

Para conjuntos simétricos e convexas demonstramos o seguinte teorema de Minkowski sobre "pontos de rede":

(17.8) COROLÁRIO. Seja C um subconjunto simétrico e convexo de $\mathbb{L}$ tal que $\text{vol}(C) > 2^n \cdot \text{vol}(M)$, então $C \cap (M \setminus \{0\}) \neq \emptyset$.

Se $\text{vol}(C) > 2^n \cdot \text{vol}(M)$ então $C \cap (M \setminus \{0\}) \neq \emptyset$.

Demonstração. Como $\text{vol}\left(\frac{1}{2} \cdot C\right) = 2^{-n} \cdot \text{vol}(C) > \text{vol}(M)$, concluímos de

(17.7) que os conjuntos $\frac{1}{2} \cdot C + z$ ($z \in M$) não são disjuntos dois a dois, isto é, existem $z_1, z_2 \in M$, $z_1 \neq z_2$, e $c_1, c_2 \in C$ tais que $\frac{1}{2} \cdot c_1 + z_1 = \frac{1}{2} \cdot c_2 + z_2$. Como C é simétrico e convexo, temos que

$$-c_1 \in C \text{ e } z_1 - z_2 = \frac{1}{2}c_2 + \left(1 - \frac{1}{2}\right)(-c_1) \in C \cap (M \setminus \{0\}). \quad \square$$

O teorema de Minkowski, aplicado a um certo subconjunto simétrico e convexo do $\mathbb{R}$ -espaço $\mathbb{L} = \underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_s \times \underbrace{\mathbb{C} \times \dots \times \mathbb{C}}_t$, será usado no

§18, na demonstração do teorema de invertíveis de Dirichlet. Outras aplicações do teorema de Minkowski encontram-se nos Exercícios 17.6. e 17.9.

EXERCÍCIOS

17.1. Indique elementos $u_1, \dots, u_n \in \mathbb{L}$ que sejam linearmente independentes sobre $\mathbb{Z}$, mas linearmente dependentes sobre $\mathbb{R}$.

17.2. Seja M uma rede de $\mathbb{L}$. Prove:

- a) Toda base do $\mathbb{Z}$ -módulo M é uma base da rede M .
- b) Todo submódulo M' do $\mathbb{Z}$ -módulo M é uma rede de $\mathbb{L}$.

17.3. Suponhamos que $v_1, \dots, v_m$ formem uma base de uma rede M de $\mathbb{L}$;

e seja $w_i = \sum_{j=1}^m a_{ij} \cdot v_j$ ($i = 1, \dots, m$) com $a_{ij} \in \mathbb{Z}$. Prove:

- a) $w_1, \dots, w_m$ formam uma base de uma rede M' em L se e somente se $\det(a_{ij}) \neq 0$.
- b) $w_1, \dots, w_m$ formam uma base da rede M se e somente se $\det(a_{ij}) = \pm 1$.

17.4. Seja $\mathbb{T}^n$ o toro n -dimensional, isto é, o produto cartesiano de n cópias do grupo multiplicativo $\{\alpha \in \mathbb{C} \mid |\alpha| = 1\}$, e suponhamos que $v_1, \dots, v_n$ formem uma base de uma rede completa M de $\mathbb{L}$. Prove:

a) A aplicação Φ definida por

$$\Phi(\rho_1 \cdot v_1 + \dots + \rho_n \cdot v_n) = (\exp(2\pi i \cdot \rho_1), \dots, \exp(2\pi i \cdot \rho_n))$$

$(\rho_1, \dots, \rho_n \in \mathbb{R})$ é um homomorfismo do grupo aditivo de $\mathbb{R}^n$ sobre $\mathbb{T}^n$, com núcleo M .

b) Φ induz uma bijeção de $z + T_v$ sobre $\mathbb{T}^n$, qualquer que seja $z \in M$.

17.5. Seja M uma rede completa de $\mathbb{R}^2$ tal que $M \subseteq \mathbb{Z}^2$. Prove que $\text{vol}(M) = \#(T_v \cap \mathbb{Z}^2)$, sendo T_v a malha fundamental associada a qualquer base v_1, v_2 de M . Generalize esta afirmação para $\mathbb{R}^n$, qualquer que seja $n \geq 2$.

17.6. Utilize o teorema de Minkowski (17.8) para provar:

- a) o "teorema de dois quadrados", isto é, a implicação (iii) $\Rightarrow$ (i) de (2.10).
- b) o "teorema de quatro quadrados", que afirma que todo inteiro positivo é soma de quatro quadrados de números naturais. (Veja Stewart-Tall [33], 7.2 e 7.3).

17.7. Prove que a afirmação do teorema de Minkowski (17.8) continua válida para qualquer subconjunto simétrico e convexo C que é compacto e satisfaz $\text{vol}(C) \geq 2^n \cdot \text{vol}(M)$ (veja Samuel [30], §4.1).

17.8. Sejam $s, t \in \mathbb{N}$ e $n = s + 2t$. Prove que, para qualquer $\rho > 0$, o subconjunto $C_\rho = \left\{ (\xi_1, \dots, \xi_s, \eta_1, \zeta_1, \dots, \eta_t, \zeta_t) \mid \sum_{j=1}^s |\xi_j| + 2 \cdot \sum_{j=1}^t \sqrt{\eta_j^2 + \zeta_j^2} \leq \rho \right\}$ de $\mathbb{R}^n$ é convexo, simétrico e compacto e calcule o seu volume (veja Samuel [30], Chapter 4, Appendix).

17.9. Utilize o teorema de Minkowski e o Exercício 17.8. para provar que, na afirmação de (10.1), a cota ρ pode ser substituída pela cota de Minkowski $\mu_L = \left(\frac{4}{\pi}\right)^t \cdot \frac{n!}{n^n} \cdot \sqrt{|d_L|}$. (Veja Samuel [30], §4.3, ou Stewart-Tall [33], 10.2).

§18. Representações geométricas de números algébricos

Recordamos que, dada uma extensão L de $\mathbb{Q}$ de grau n , existem exatamente n isomorfismos σ de L em $\mathbb{C}$. Chamaremos σ uma *imersão real* (respectivamente *complexa*) de L quando $\sigma L \subseteq \mathbb{R}$ (respectivamente $\not\subseteq \mathbb{R}$). As imersões complexas ocorrem em pares complexo-conjugados; de fato, se σ for uma imersão complexa de L , então o mesmo acontecerá com a aplicação $\bar{\sigma} : L \rightarrow \mathbb{C}$ que associa a cada $\alpha \in L$ o complexo-conjugado de $\sigma\alpha$, e teremos que $\bar{\sigma} \neq \sigma = \bar{\bar{\sigma}}$. Denotaremos por $\sigma_1, \dots, \sigma_s$ as imersões reais e por $\sigma_{s+1}, \bar{\sigma}_{s+1}, \dots, \sigma_{s+t}, \bar{\sigma}_{s+t}$ as imersões complexas de L ; obviamente $0 \leq s \leq n$, $0 \leq t \leq \frac{n}{2}$ e $s + 2t = n$.

Observamos que, no caso em que L está contido em $\mathbb{C}$, a aplicação idêntica i de L em $\mathbb{C}$ é uma das imersões de L ; podemos supor que $i = \sigma_1$ (respectivamente $= \sigma_{s+1}$) quando $L \subseteq \mathbb{R}$ (respectivamente $\not\subseteq \mathbb{R}$).

As imersões reais e complexas de L podem ser obtidas através do polinômio minimal $P_{\alpha|\mathbb{Q}}$ de qualquer elemento primitivo α de $L|\mathbb{Q}$. De fato, sendo $P_{\alpha|\mathbb{Q}} = (X - \alpha_1) \cdot \dots \cdot (X - \alpha_s) \cdot Q_1 \cdot \dots \cdot Q_t$ a sua fatoração em $\mathbb{R}[X]$, onde $Q_1, \dots, Q_t$ são polinômios irreduzíveis de grau 2, as imersões reais de L são determinadas por

$$\sigma_j \alpha = \alpha_j, (j = 1, \dots, s),$$

enquanto que os pares de imersões complexas são determinados por

$$\sigma_{s+j} \alpha = \beta_j, \quad \bar{\sigma}_{s+j} \alpha = \bar{\beta}_j \quad (j = 1, \dots, t),$$

onde $\beta_j, \bar{\beta}_j \in \mathbb{C} \setminus \mathbb{R}$ são as duas raízes de Q_j .

No caso particular em que $L = \mathbb{Q}(\alpha)$ é um corpo quadrático ($\alpha^2 = d \in \mathcal{D}$), temos que

$$\begin{aligned} s = 2, t = 0, & \text{ no caso real } (d > 0), \text{ e} \\ s = 0, t = 1, & \text{ no caso imaginário } (d < 0). \end{aligned}$$

No primeiro caso, as duas imersões reais σ_1, σ_2 são determinadas por $\sigma_1 \alpha = \sqrt{d}$, $\sigma_2 \alpha = -\sqrt{d}$; no segundo caso temos que $\sigma \alpha = i \cdot \sqrt{|d|}$, $\bar{\sigma} \alpha = -i \cdot \sqrt{|d|}$. Também para corpos cúbicos L , isto é, corpos L tais que $[L:\mathbb{Q}] = 3$, existem apenas dois casos. De fato, verifica-se facilmente que:

$$\begin{aligned} s = 3, t = 0 & \text{ se e somente se } d_L > 0. \\ s = 1, t = 1 & \text{ se e somente se } d_L < 0. \end{aligned}$$

Sejam $s, t \in \mathbb{N}$ tais que $s + 2t = n \geq 1$. Consideramos o produto cartesiano $\mathbb{L}^{s,t} = \underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_s \times \underbrace{\mathbb{C} \times \dots \times \mathbb{C}}_t$ de s cópias de $\mathbb{R}$ e t cópias de $\mathbb{C}$,

isto é, o conjunto de todas as $(s+t)$ -uplas $(\xi_1, \dots, \xi_s; \omega_1, \dots, \omega_t)$ com $\xi_1, \dots, \xi_s \in \mathbb{R}$ e $\omega_1, \dots, \omega_t \in \mathbb{C}$. Munido das operações componente a componente, $\mathbb{L}^{s,t}$ é um anel e ao mesmo tempo um $\mathbb{R}$ -espaço de dimensão n , tendo como base distinguida a seguinte:

$$\begin{aligned} e_1 &= (1, 0, \dots, 0, \dots, 0), \dots, e_s = (0, \dots, 0, 1, 0, \dots, 0), \\ e_{s+1} &= (0, \dots, 0, 1, 0, \dots, 0), e_{s+2} = (0, \dots, 0, i, 0, \dots, 0), \dots, \\ e_{s+2t-1} &= (0, \dots, 0, 0, \dots, 0, 1), e_{s+2t} = (0, \dots, 0, 0, \dots, 0, i). \end{aligned}$$

Às vezes convém escrever f_j em lugar de e_{s+2j-1} e g_j em lugar de e_{s+2j} ($j = 1, \dots, t$).

As noções introduzidas no §17, como “comprimento”, “bola de raio ρ ” e “volume” serão consideradas em relação a esta base. Por exemplo, na demonstração de (18.11) consideraremos o “cubo n -dimensional”

$$C = \left\{ \sum_{j=1}^n \gamma_j \cdot e_j \mid -\rho \leq \gamma_j \leq \rho \ (j=1, \dots, n) \right\} \text{ em } \mathbb{L}^{s,t},$$

que é o produto cartesiano de s intervalos $[-\rho, \rho]$ em $\mathbb{R}$ e de t quadrados $\{\eta + i \cdot \zeta \mid -\rho \leq \eta \leq \rho, -\rho \leq \zeta \leq \rho\}$ em $\mathbb{C}$ e, portanto, tem o volume $(2\rho)^n$. A este conjunto, que é obviamente simétrico e convexo, será aplicado o teorema de Minkowski.

Seja L uma extensão de $\mathbb{Q}$ de grau n . Consideramos as imersões reais $\sigma_1, \dots, \sigma_s$ de L e, em cada par $\sigma_{s+j}, \bar{\sigma}_{s+j}$ de imersões complexo-conjugadas, escolhemos uma das duas imersões, digamos σ_{s+j} ($j=1, \dots, t$). A aplicação χ de L em $\mathbb{L}^{s,t}$ definida por:

$$\chi\alpha = (\sigma_1\alpha, \dots, \sigma_s\alpha; \sigma_{s+1}\alpha, \dots, \sigma_{s+t}\alpha) \ (\alpha \in L)$$

é chamada a *imersão canônica* de L (embora χ dependa da escolha acima mencionada). Obviamente,

(18.1) χ é um homomorfismo injetivo do corpo L no anel $\mathbb{L}^{s,t}$ e é $\mathbb{Z}$ -linear.

Mostraremos a seguir que a imersão canônica χ de L leva qualquer base $\alpha_1, \dots, \alpha_n$ da extensão $L|\mathbb{Q}$ numa base $v_1, \dots, v_n$ de rede completa de $\mathbb{L}^{s,t}$. Este resultado será obtido provando-se que o volume de T_v é não-nulo; de fato, este volume pode ser calculado por meio do discriminante $\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$.

(18.2) TEOREMA. *Seja $\alpha_1, \dots, \alpha_n$ uma base de $L|\mathbb{Q}$. Então $\chi\alpha_1, \dots, \chi\alpha_n$ formam uma base da rede completa $M_\alpha = \chi(\mathbb{Z} \cdot \alpha_1 + \dots + \mathbb{Z} \cdot \alpha_n)$, e temos que*

$$\text{vol}(M_\alpha) = 2^{-t} \cdot \sqrt{|\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n)|} \neq 0.$$

Demonstração. Por (4.2) e (4.4) temos que $\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = \delta^2$, onde $\delta = \det(\sigma_1\alpha_j, \dots, \sigma_s\alpha_j, \sigma_{s+1}\alpha_j, \bar{\sigma}_{s+1}\alpha_j, \dots, \sigma_{s+t}\alpha_j, \bar{\sigma}_{s+t}\alpha_j)$. Sejam $\sigma_k\alpha_j = \xi_{jk}$ ($k=1, \dots, s$) e $\sigma_{s+k}\alpha_j = \eta_{jk} + i \cdot \zeta_{jk}$ ($k=1, \dots, t$). Através de transformações elementares, a saber, pela adição da $(s+2k)$ -ésima coluna à sua anterior, seguida pela subtração da $(s+2k-1)$ -ésima coluna da sua posterior ($k=1, \dots, t$), obtemos as seguintes igualdades:

$$\begin{aligned}\delta &= \det(\xi_{j_1}, \dots, \xi_{j_s}, \eta_{j_1} + i \cdot \zeta_{j_1}, \eta_{j_1} - i \cdot \zeta_{j_1}, \dots, \eta_{j_t} + i \cdot \zeta_{j_t}, \eta_{j_t} - i \cdot \zeta_{j_t}) = \\ &= 2^t \cdot \det(\xi_{j_1}, \dots, \xi_{j_s}, \eta_{j_1}, \eta_{j_1} - i \cdot \zeta_{j_1}, \dots, \eta_{j_t}, \eta_{j_t} - i \cdot \zeta_{j_t}) = \\ &= 2^t \cdot (-i)^t \cdot \det(\xi_{j_1}, \dots, \xi_{j_s}, \eta_{j_1}, \zeta_{j_1}, \dots, \eta_{j_t}, \zeta_{j_t}).\end{aligned}$$

Por outro lado, como

$$v_j = \chi \alpha_j = \xi_{j_1} \cdot e_1 + \dots + \xi_{j_s} \cdot e_s + \eta_{j_1} \cdot f_1 + \zeta_{j_1} \cdot g_1 + \dots + \eta_{j_t} \cdot f_t + \zeta_{j_t} \cdot g_t$$

($j = 1, \dots, n$), resulta de (17.4) que

$$\begin{aligned}\text{vol}(T_v) &= |\det(\xi_{j_1}, \dots, \xi_{j_s}, \eta_{j_1}, \zeta_{j_1}, \dots, \eta_{j_t}, \zeta_{j_t})| = \\ &= 2^{-t} \cdot |\delta| = 2^{-t} \cdot \sqrt{|\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n)|},\end{aligned}$$

o que é não-nulo devido a (4.4); portanto, $v_1, \dots, v_n$ formam uma base de rede completa, a saber, da rede M_α , e temos que $\text{vol}(M_\alpha) = \text{vol}(T_v)$. $\square$

Aplicamos este teorema aos subanéis S de L que, como $\mathbb{Z}$ -módulos, são livres de posto n . Recordamos que estes coincidem com os subanéis S de I_L tais que $Q(S) = L$ (veja (5.5)) e são chamados as "ordens" de L .

(18.3) **COROLÁRIO.** *Seja S um subanel de I_L tal que $Q(S) = L$. Então, χS é uma rede completa em $\mathbb{L}^{s,t}$ com volume*

$$\text{vol}(\chi S) = 2^{-t} \cdot \sqrt{|\text{disc}_{L|\mathbb{Q}}(\alpha_1, \dots, \alpha_n)|} \neq 0,$$

sendo $\alpha_1, \dots, \alpha_n$ uma base do $\mathbb{Z}$ -módulo S .

Em particular, χI_L é uma rede completa em $\mathbb{L}^{s,t}$, com volume

$$\text{vol}(\chi I_L) = 2^{-t} \cdot \sqrt{|d_L|} \neq 0.$$

Seja $\mathcal{N}$ a aplicação de $\mathbb{L}^{s,t}$ em $\mathbb{R}$ definida por $\mathcal{N}(\xi_1, \dots, \xi_s; \omega_1, \dots, \omega_t) = \xi_1 \cdot \dots \cdot \xi_s \cdot |\omega_1|^2 \cdot \dots \cdot |\omega_t|^2$ ($\xi_1, \dots, \xi_s \in \mathbb{R}$; $\omega_1, \dots, \omega_t \in \mathbb{C}$). Ela chama-se a *norma* de $\mathbb{L}^{s,t}$, devido às seguintes propriedades:

(18.4) $\mathcal{N}$ é um homomorfismo multiplicativo e satisfaz $\mathcal{N} \circ \chi = \mathcal{N}_{L|\mathbb{Q}}$.

Demonstração. Resulta da definição e das igualdades

$$\begin{aligned}\mathcal{N}(\chi \gamma) &= \sigma_1 \gamma \cdot \dots \cdot \sigma_s \gamma \cdot |\sigma_{s+1} \gamma|^2 \cdot \dots \cdot |\sigma_{s+t} \gamma|^2 = \\ &= \sigma_1 \gamma \cdot \dots \cdot \sigma_s \gamma \cdot \sigma_{s+1} \gamma \cdot \bar{\sigma}_{s+1} \gamma \cdot \dots \cdot \sigma_{s+t} \gamma \cdot \bar{\sigma}_{s+t} \gamma = \mathcal{N}_{L|\mathbb{Q}} \gamma,\end{aligned}$$

para qualquer $\gamma \in L$. $\square$

A norma $\mathcal{N}$ será útil para compararmos os volumes de duas redes completas cujas bases se distinguem por um fator $c \in \mathbb{L}^{s,t}$. Isto será feito por meio da seguinte proposição:

(18.5) Seja $c \in \mathbb{L}^{s,t}$.

a) Se $c \cdot e_j = \sum_{k=1}^n \rho_{jk} \cdot e_k$ ($j=1, \dots, n$), com $\rho_{jk} \in \mathbb{R}$, então $\mathcal{N}c = \det(\rho_{jk})$.

b) Sejam $v_1, \dots, v_n \in \mathbb{L}^{s,t}$ e $w_j = c \cdot v_j$ ($j=1, \dots, n$); então

$$\text{vol}(T_w) = |\mathcal{N}c| \cdot \text{vol}(T_v).$$

Demonstração. a) Seja $c = (\xi_1, \dots, \xi_s; \eta_1 + i \cdot \zeta_1, \dots, \eta_t + i \cdot \zeta_t)$, com $\xi_j, \eta_j, \zeta_j \in \mathbb{R}$. Então $c \cdot e_k = \xi_k \cdot e_k$ ($k=1, \dots, s$),

$c \cdot f_h = \eta_h \cdot f_h + \zeta_h \cdot g_h$ e $c \cdot g_h = -\zeta_h \cdot f_h + \eta_h \cdot g_h$ ($h=1, \dots, t$); logo $\det(\rho_{jk}) = \xi_1 \cdot \dots \cdot \xi_s \cdot (\eta_1^2 + \zeta_1^2) \cdot \dots \cdot (\eta_t^2 + \zeta_t^2) = \xi_1 \cdot \dots \cdot \xi_s \cdot |\eta_1 + i \cdot \zeta_1|^2 \cdot \dots \cdot |\eta_t + i \cdot \zeta_t|^2 = \mathcal{N}c$.

b) Seja $v_j = \sum_{h=1}^n e_{jh} \cdot e_h$ ($j=1, \dots, n$), com $e_{jh} \in \mathbb{R}$; então

$$w_j = c \cdot v_j = \sum_{h=1}^n e_{jh} \cdot c \cdot e_h = \sum_{h,k=1}^n e_{jh} \cdot \rho_{hk} \cdot e_k \quad (j=1, \dots, n).$$

Por (17.4), temos que $\text{vol}(T_w) = \left| \det \left(\sum_{h=1}^n e_{jh} \cdot \rho_{hk} \right) \right| = |\det(e_{jk})| \cdot |\det(\rho_{jk})| = \text{vol}(T_v) \cdot |\mathcal{N}c|$. $\square$

Observando que $\mathcal{N}c \neq 0$ se e somente se

$$c \in \underbrace{\mathbb{R}^* \times \dots \times \mathbb{R}^*}_s \times \underbrace{\mathbb{C}^* \times \dots \times \mathbb{C}^*}_t,$$

que é obviamente o grupo dos invertíveis $U(\mathbb{L}^{s,t})$ do anel $\mathbb{L}^{s,t}$, concluímos de (18.5) e (17.4):

(18.6) Seja $c \in \mathbb{L}^{s,t}$ e suponhamos que $v_1, \dots, v_n$ formem uma base da rede completa M de $\mathbb{L}^{s,t}$; então $c \cdot v_1, \dots, c \cdot v_n$ geram o $\mathbb{Z}$ -módulo $c \cdot M = \{c \cdot z \mid z \in M\}$. Além disto, $c \cdot M$ será uma rede completa de $\mathbb{L}^{s,t}$ se e somente se $c \in U(\mathbb{L}^{s,t})$; neste caso,

$$\text{vol}(c \cdot M) = |\mathcal{N}c| \cdot \text{vol}(M).$$

A fim de podermos aplicar a noção de rede para estudar o grupo multiplicativo dos invertíveis de I_L , será necessário transformar a multiplicação em adição, o que será feito através do logaritmo natural. Mais precisamente, definiremos primeiramente homomorfismos $\mu_1, \dots, \mu_{s+t}$ do grupo multiplicativo $U(\mathbb{L}^{s,t})$ no grupo aditivo $\mathbb{R}$ por

$$\mu_j(\xi_1, \dots, \xi_s; \omega_1, \dots, \omega_t) = \begin{cases} \log |\xi_j| & \text{quando } j = 1, \dots, s \\ \log |\omega_{j-s}|^2 & \text{quando } j = s+1, \dots, s+t \end{cases}$$

$(\xi_1, \dots, \xi_s \in \mathbb{R}; \omega_1, \dots, \omega_t \in \mathbb{C})$, bem como um homomorfismo μ de $U(\mathbb{L}^{s,t})$ no grupo aditivo $\mathbb{R}^{s+t} = \underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_{s+t}$ por

$$\mu c = (\mu_1 c, \dots, \mu_{s+t} c) \quad (c \in U(\mathbb{L}^{s,t})).$$

Observemos que $\mu_1, \dots, \mu_{s+t}$ e μ são sobrejetivos.

Compondo estas aplicações com a restrição χ^* de χ a L^* , a qual é obviamente um homomorfismo multiplicativo de L^* em $U(\mathbb{L}^{s,t})$, obtemos os homomorfismos $\lambda_1 = \mu_1 \circ \chi^*, \dots, \lambda_{s+t} = \mu_{s+t} \circ \chi^*$ de L^* no grupo aditivo $\mathbb{R}$ e o homomorfismo $\lambda = \mu \circ \chi^*$ de L^* no grupo aditivo $\mathbb{R}^{s+t}$; este último homomorfismo chama-se a *representação logarítmica* de L^* . Obviamente,

$$\lambda \gamma = (\lambda_1 \gamma, \dots, \lambda_{s+t} \gamma) = (\log |\sigma_1 \gamma|, \dots, \log |\sigma_s \gamma|, \log |\sigma_{s+1} \gamma|^2, \dots, \log |\sigma_{s+t} \gamma|^2).$$

Determinaremos a seguir os núcleos dos homomorfismos μ e λ , bem como a imagem inversa, sob estes homomorfismos, do hiperplano

$$\mathbb{H} = \{(\rho_1, \dots, \rho_{s+t}) \in \mathbb{R}^{s+t} \mid \rho_1 + \dots + \rho_{s+t} = 0\},$$

o qual é obviamente um subespaço, de dimensão $s+t-1$, do $\mathbb{R}$ -espaço $\mathbb{R}^{s+t}$.

$$(18.7) \text{ a) } \text{Ker } \mu = \{(\xi_1, \dots, \xi_s; \omega_1, \dots, \omega_t) \in U(\mathbb{L}^{s,t}) \mid |\xi_1| = \dots = |\xi_s| = |\omega_1| = \dots = |\omega_t| = 1\}.$$

$$\text{b) } \mu^{-1} \mathbb{H} = \{a \in U(\mathbb{L}^{s,t}) \mid \mathcal{N}a \in \{1, -1\}\}.$$

Demonstração. a) $\mu(\xi_1, \dots, \xi_s; \omega_1, \dots, \omega_t) = 0$ se e somente se

$$\log |\xi_1| = \dots = \log |\xi_s| = \log |\omega_1|^2 = \dots = \log |\omega_t|^2 = 0,$$

se e somente se $|\xi_1| = \dots = |\xi_s| = |\omega_1| = \dots = |\omega_t| = 1$.

b) Seja $a = (\xi_1, \dots, \xi_s; \omega_1, \dots, \omega_t)$; então

$$\begin{aligned} \log |\mathcal{N}a| &= \log |\xi_1 \cdot \dots \cdot \xi_s \cdot \omega_1|^2 \cdot \dots \cdot \omega_t|^2 = \log |\xi_1| + \dots + \log |\xi_s| + \\ &+ \log |\omega_1|^2 + \dots + \log |\omega_t|^2 = \mu_1 a + \dots + \mu_{s+t} a. \end{aligned}$$

Portanto, $\mu a \in \mathbb{H}$ se e somente se $\log |\mathcal{N}a| = 0$, se e somente se $\mathcal{N}a \in \{1, -1\}$. $\square$

- (18.8) a) $\text{Ker } \lambda = W(L)$ (grupo das raízes da unidade em L).
 b) $\lambda^{-1}\mathbb{H} = \{\alpha \in L^* \mid \mathcal{N}_{L|\mathbb{Q}}\alpha \in \{1, -1\}\}$.

Demonstração. Seja $\alpha \in L^*$. a) Teremos que $\lambda\alpha = 0$ se e somente se $\chi^*\alpha \in \text{Ker } \mu$, se e somente se

$$|\sigma_1\alpha| = \dots = |\sigma_s\alpha| = |\sigma_{s+1}\alpha| = \dots = |\sigma_{s+t}\alpha| = 1,$$

por (18.7a). Obviamente, isso ocorrerá se e somente se

$$|\sigma_1\alpha| = \dots = |\sigma_s\alpha| = |\sigma_{s+1}\alpha| = |\bar{\sigma}_{s+1}\alpha| = \dots = |\sigma_{s+t}\alpha| = |\bar{\sigma}_{s+t}\alpha| = 1,$$

o que equivale a $\alpha \in W(L)$, por (1.16).

b) $\lambda\alpha \in \mathbb{H}$ se e somente se $\chi^*\alpha \in \mu^{-1}\mathbb{H}$, se e somente se $\mathcal{N}(\chi^*\alpha) \in \{1, -1\}$, por (18.7b). A afirmação resulta então de (18.4). $\square$

Recordamos que, para qualquer subanel S de I_L , temos que $U(S) = \{\alpha \in S \mid \mathcal{N}_{L|\mathbb{Q}}\alpha \in \{1, -1\}\}$ (veja (1.11c)); logo $U(S) \subseteq \lambda^{-1}\mathbb{H}$ por (18.8b), ou seja, $\lambda(U(S)) \subseteq \mathbb{H}$. Mostraremos a seguinte afirmação mais precisa:

(18.9) Para qualquer subanel S de I_L , $\lambda(U(S))$ é uma rede em $\mathbb{H}$.

Demonstração. Como $\lambda(U(S))$ é um grupo aditivo, basta provar, por (17.1), que é um subconjunto discreto de $\mathbb{H}$. Para isto é suficiente mostrar que, para qualquer $\rho > 0$, a interseção de $\lambda(U(S))$ com a bola de raio ρ em $\mathbb{R}^{s+t}$ é finita, ou seja, que λU_ρ é finito, onde

$$U_\rho = \{\alpha \in U(S) \mid \|\lambda\alpha\| \leq \rho\}.$$

Afirmamos primeiramente que χU_ρ é limitado em $\mathbb{L}^{s,t}$. De fato, como $\rho \geq \|\lambda\alpha\| = \sqrt{(\lambda_1\alpha)^2 + \dots + (\lambda_{s+t}\alpha)^2} \geq \lambda_j\alpha = \log|\sigma_j\alpha|$ (respectivamente $= \log|\bar{\sigma}_j\alpha|^2$), para $j = 1, \dots, s$ (respectivamente $j = s+1, \dots, s+t$), temos que $|\sigma_j\alpha| \leq \exp(\rho)$ ($j = 1, \dots, s$) e $|\bar{\sigma}_j\alpha|^2 \leq \exp(\rho)$ ($j = s+1, \dots, s+t$). Seja $\sigma_{s+h}\alpha = \eta_h + i \cdot \zeta_h$ ($h = 1, \dots, t$), com $\eta_h, \zeta_h \in \mathbb{R}$; então

$$\chi\alpha = (\sigma_1\alpha) \cdot e_1 + \dots + (\sigma_s\alpha) \cdot e_s + \eta_1 \cdot f_1 + \zeta_1 \cdot g_1 + \dots + \eta_t \cdot f_t + \zeta_t \cdot g_t,$$

$$\begin{aligned} \text{logo } \|\chi\alpha\| &= \sqrt{(\sigma_1\alpha)^2 + \dots + (\sigma_s\alpha)^2 + \eta_1^2 + \zeta_1^2 + \dots + \eta_t^2 + \zeta_t^2} = \\ &= \sqrt{(\sigma_1\alpha)^2 + \dots + (\sigma_s\alpha)^2 + |\sigma_{s+1}\alpha|^2 + \dots + |\sigma_{s+t}\alpha|^2} \leq \\ &\leq \sqrt{s \cdot \exp(2\rho) + t \cdot \exp(\rho)}; \end{aligned}$$

portanto, χU_ρ é limitado em $\mathbb{L}^{s,t}$. De $U_\rho \subseteq S \subseteq I_L$ resulta que χU_ρ está contido em χI_L , que é discreto por (18.3) e (17.1); portanto, $\chi U_\rho = \chi I_L \cap \chi U_\rho$

é finito. Como χ é injetivo, resulta que U_ρ é finito; portanto, λU_ρ também o é. $\square$

O teorema de invertíveis de Dedekind será obtido como consequência do fato de $\lambda(U(I_L))$ ser mesmo uma rede completa de $\mathbb{H}$, fato este que será demonstrado a seguir, usando-se a seguinte proposição.

(18.10) *Seja C um subconjunto de $\mu^{-1}\mathbb{H}$, limitado em $\mathbb{L}^{s,t}$. Então, o subconjunto μC de $\mathbb{H}$ é limitado em $\mathbb{R}^{s+t}$ (e, portanto, em $\mathbb{H}$).*

Demonstração. Sem perda de generalidade podemos supor que

$$C \subseteq \{(\xi_1, \dots, \xi_s; \omega_1, \dots, \omega_t) \in \mathbb{L}^{s,t} \mid |\xi_j| \leq \rho \ (j = 1, \dots, s), \\ |\omega_k|^2 \leq \rho \ (k = 1, \dots, t)\}$$

para algum $\rho > 1$; então temos que $\mu_j a \leq \log \rho$ ($j = 1, \dots, s+t$) para qualquer $a \in C$. Por outro lado, de $C \subseteq \mu^{-1}\mathbb{H}$ resulta que $\mu_1 a + \dots + \mu_{s+t} a = 0$; logo

$$\mu_j a = -(\mu_1 a + \dots + \mu_{j-1} a + \mu_{j+1} a + \dots + \mu_{s+t} a) \geq -(s+t-1) \cdot \log \rho$$

e, portanto, $|\mu_j a| \leq (s+t) \cdot \log \rho$ ($j = 1, \dots, s+t$). Concluímos que

$$\|\mu a\| = \sqrt{|\mu_1 a|^2 + \dots + |\mu_{s+t} a|^2} \leq (s+t)^2 \cdot \log \rho; \text{ portanto } \mu C \text{ é limitado em } \mathbb{R}^{s+t}. \quad \square$$

(18.11) **TEOREMA.** *Seja S um subanel de I_L tal que $Q(S) = L$. Então, $\lambda(US)$ é uma rede completa em $\mathbb{H}$.*

Demonstração. Basta indicar um subconjunto B de $\mu^{-1}\mathbb{H}$, limitado em $\mathbb{L}^{s,t}$, tal que $\mu^{-1}\mathbb{H} = \bigcup_{s \in U(S)} \chi s \cdot B$. De fato, teremos então que $\mathbb{H} = \mu(\mu^{-1}\mathbb{H}) = \bigcup_{s \in U(S)} (\lambda s + \mu B) = \bigcup_{z \in \lambda(U(S))} (z + \mu B)$, e sendo μB limitado em $\mathbb{H}$, por (18.10), resultará de (17.3) e (18.9) que $\lambda(U(S))$ é uma rede completa em $\mathbb{H}$.

Por (18.3), χS é uma rede completa em $\mathbb{L}^{s,t}$, com volume não-nulo. Para construirmos B , escolhemos $\rho > \sqrt[n]{\text{vol}(\chi S)}$ e consideramos em $\mathbb{L}^{s,t}$ o cubo n -dimensional $C = \left\{ \sum_{j=1}^n \gamma_j \cdot e_j \mid -\rho \leq \gamma_j \leq \rho \ (j = 1, \dots, n) \right\}$, o qual obviamente é limitado, simétrico e convexo e tem o volume $\text{vol}(C) = (2\rho)^n$.

Notamos que, para qualquer $c = \sum_{j=1}^n \gamma_j \cdot e_j \in C$, temos que $|\mathcal{N}c| = |\gamma_1| \cdot \dots \cdot |\gamma_s| \cdot |\gamma_{s+1} + i \cdot \gamma_{s+2}|^2 \cdot \dots \cdot |\gamma_{n-1} + i \cdot \gamma_n|^2 \leq 2^t \cdot \rho^n$. Por (1.17), existe um número finito de elementos não-nulos $\alpha_1, \dots, \alpha_g$ de S tais que todo $\alpha \in S \setminus \{0\}$ com $|\mathcal{N}_{L|\mathbb{Q}}\alpha| \leq 2^t \cdot \rho^n$ seja associado a um deles. Seja $B = \mu^{-1}\mathbb{H} \cap \bigcup_{j=1}^g \chi\alpha_j^{-1} \cdot C$; obviamente B é limitado em $\mathbb{L}^{s,t}$.

Afirmamos que $\bigcup_{\varepsilon \in U(S)} \chi\varepsilon \cdot B = \mu^{-1}\mathbb{H}$. A inclusão $\subseteq$ resulta do fato de, para quaisquer $\varepsilon \in U(S)$ e $b \in B$, termos que $\mathcal{N}(\chi\varepsilon \cdot b) = \mathcal{N}_{L|\mathbb{Q}}\varepsilon \cdot \mathcal{N}b \in \{1, -1\}$ e, portanto, $\chi\varepsilon \cdot b \in \mu^{-1}\mathbb{H}$, devido a (1.11c), (18.4) e (18.7). Para provarmos a inclusão inversa, observamos que, para qualquer $a \in \mu^{-1}\mathbb{H}$, $a \cdot \chi S$ é uma rede completa em $\mathbb{L}^{s,t}$, com volume $\text{vol}(a \cdot \chi S) = |\mathcal{N}a| \cdot \text{vol}(\chi S) = \text{vol}(\chi S)$, devido a (18.6) e (18.7b). De $\text{vol}(C) = (2\rho)^n > 2^n \cdot \text{vol}(a \cdot \chi S)$ concluímos, por (17.8), que $C \cap (a \cdot \chi S \setminus \{0\}) \neq \emptyset$, ou seja, que existe $c = a \cdot \chi\alpha \in C$ com $\alpha \in S \setminus \{0\}$. De $|\mathcal{N}_{L|\mathbb{Q}}\alpha| = |\mathcal{N}a| \cdot |\mathcal{N}_{L|\mathbb{Q}}\alpha| = |\mathcal{N}(a \cdot \chi\alpha)| = |\mathcal{N}c| \leq 2^t \cdot \rho^n$ resulta que existem $j \in \{1, \dots, g\}$ e $\varepsilon \in U(S)$ tais que $\alpha_j = \alpha \cdot \varepsilon$; logo $a = (\chi\alpha_j^{-1}) \cdot c = \chi\varepsilon \cdot (\chi\alpha_j^{-1}) \cdot c$. Finalmente, de $\mathcal{N}((\chi\alpha_j^{-1}) \cdot c) = \mathcal{N}(\chi\varepsilon^{-1} \cdot a) = \mathcal{N}_{L|\mathbb{Q}}\varepsilon^{-1} \cdot \mathcal{N}a \in \{1, -1\}$ concluímos que $(\chi\alpha_j^{-1}) \cdot c \in \mu^{-1}\mathbb{H}$; portanto, $(\chi\alpha_j^{-1}) \cdot c \in B$ e assim $a \in \chi\varepsilon \cdot B$. $\square$

De (18.11) obtemos, como corolário, o seguinte teorema de invertíveis de Dirichlet, válido para qualquer "ordem" S de L .

(18.12) COROLÁRIO. *Seja L uma extensão de $\mathbb{Q}$ de grau n que possua s imersões reais e t pares de imersões complexo-conjugadas, e seja S um subanel de I_L tal que $Q(S) = L$.*

Então, existem $\varepsilon_1, \dots, \varepsilon_{s+t-1} \in U(S)$ tais que $U(S)$ seja produto direto $W(S) \odot (\varepsilon_1) \odot \dots \odot (\varepsilon_{s+t-1})$ do grupo cíclico finito $W(S) = W(L) \cap U(S)$ e dos grupos cíclicos infinitos gerados por $\varepsilon_1, \dots, \varepsilon_{s+t-1}$.

Demonstração. Seja $r = s + t - 1$. Por (18.11), existem $\varepsilon_1, \dots, \varepsilon_r \in U(S)$ tais que $\lambda\varepsilon_1, \dots, \lambda\varepsilon_r$ fornecem uma base da rede completa $\lambda(U(S))$ de $\mathbb{H}$; portanto, para qualquer $\varepsilon \in U(S)$ temos que $\lambda\varepsilon = k_1 \cdot \lambda\varepsilon_1 + \dots + k_r \cdot \lambda\varepsilon_r$, com $k_1, \dots, k_r \in \mathbb{Z}$ apropriados. Seja $\beta = \varepsilon \cdot \varepsilon_1^{-k_1} \cdot \dots \cdot \varepsilon_r^{-k_r}$; então $\beta \in U(S)$ e $\lambda\beta = \lambda\varepsilon - k_1 \cdot \lambda\varepsilon_1 - \dots - k_r \cdot \lambda\varepsilon_r = 0$; logo $\beta \in W(S)$, por (18.8), e, portanto, $\varepsilon = \beta \cdot \varepsilon_1^{k_1} \cdot \dots \cdot \varepsilon_r^{k_r} \in W(S) \cdot (\varepsilon_1) \cdot \dots \cdot (\varepsilon_r)$. Resulta que

$$U(S) = W(S) \cdot (\varepsilon_1) \cdot \dots \cdot (\varepsilon_r).$$

Afirmamos que este produto é direto. De fato, sejam $\beta \in W(S)$ e $k_1, \dots, k_r \in \mathbb{Z}$ tais que $\beta \cdot \varepsilon_1^{k_1} \cdot \dots \cdot \varepsilon_r^{k_r} = 1$; então $\lambda\beta + k_1 \cdot \lambda\varepsilon_1 + \dots + k_r \cdot \lambda\varepsilon_r = 0$ e $\lambda\beta = 0$,

devido a (18.8), e da independência linear de $\lambda\varepsilon_1, \dots, \lambda\varepsilon_r$, resulta que $k_1 = \dots = k_r = 0$ e $\beta = 1$. Finalmente, como $W(L)$ é um grupo finito (por (1.16) ou Exercício 3.2.), o grupo $W(S)$ também o é. $\square$

A afirmação principal do teorema de invertíveis de Dirichlet pode ser resumida da seguinte forma:

(18.13) COROLÁRIO. *Sob as hipóteses de (18.12), o grupo $U(S)$ é um subgrupo finitamente gerado de L^* , de posto $s+t-1$, cujo grupo de torção é cíclico.*

Qualquer $(s+t-1)$ -upla de invertíveis $\varepsilon_1, \dots, \varepsilon_{s+t-1}$ de S que tiver a propriedade indicada em (18.12), será chamada um *sistema de invertíveis fundamentais de S* . No caso em que $S = I_L$, será chamada também um *sistema de invertíveis fundamentais de L* .

Observamos que o caso $s+t-1=0$ ocorrerá se e somente se $L = \mathbb{Q}$ ou se L for um corpo quadrático imaginário. O caso em que L é um corpo quadrático real, no qual $s+t-1=1$, será estudado no §19.

Mencionamos ainda, sem demonstração, que, sendo $\mathcal{V}$ o conjunto das valorizações discretas de L e R_v o anel da valorização v , o teorema de invertíveis de Dirichlet pode ser generalizado para o subanel $J_{\mathcal{W}} = \bigcap_{v \in \mathcal{V} \setminus \mathcal{W}} R_v$ de L , qualquer que seja o subconjunto finito $\mathcal{W}$ de $\mathcal{V}$. De fato, prova-se que $U(J_{\mathcal{W}})$ é um subgrupo finitamente gerado de L de posto $\#\mathcal{W} + s+t-1$, tendo $W(L)$ como grupo de torção (veja Weiss [37], 5.3.10). Em particular, no caso $\mathcal{W} = \emptyset$ obtemos o anel $J_{\emptyset} = I_L$ (veja Exercício 8.11), cujo grupo de invertíveis tem o posto $s+t-1$, de acordo com (18.13). Neste contexto cabe mencionar que o número $s+t$ é igual ao número das valorizações arquimedianas de L , como se prova facilmente.

EXERCÍCIOS

- 18.1. Indique todas as imersões de $\mathbb{Q}(\sqrt[4]{5})$ em $\mathbb{C}$. Quais delas são reais, quais são complexas?
- 18.2. Seja $\zeta \neq 1$ uma raiz quinta da unidade. Determine a rede completa em $\mathbb{L}^{0,2} = \mathbb{C}^2$ com a base $\chi 1, \chi\zeta, \chi\zeta^2, \chi\zeta^3$, sendo χ a imersão canônica de $\mathbb{Q}(\zeta)$.

18.3. Sejam $\zeta \neq 1$ uma raiz terceira da unidade e $L = \mathbb{Q}(\zeta)$. Determine a rede em $\mathbb{L}^{0,1} = \mathbb{C}$ a qual se obtém como imagem, pela imersão canônica χ de L ,

- a) do anel I_L ;
- b) do grupo aditivo gerado por $1 + \zeta$ e $\zeta^2 - 2$;
- c) do grupo aditivo gerado por $-2 \cdot \zeta$ e $3 \cdot \zeta^2 + 3$;

e calcule o volume das malhas destas redes.

18.4. Sejam L e M corpos de números algébricos tais que $L \subseteq M$ e $[M : L] = m$. Prove:

- a) Para cada imersão real σ de L existe $q \in \mathbb{N}$, com $\frac{m}{2} \leq q \leq m$, tal que σ se estenda a $2 \cdot q - m$ imersões reais e $m - q$ pares de imersões complexo-conjugadas de M .
- b) Cada imersão complexa de L estende-se a m imersões complexas de M , não complexo-conjugadas duas a duas.
- c) O número s' das imersões reais de M satisfaz a desigualdade

$$s \cdot m \geq s' \geq \begin{cases} 0 & \text{quando } m \text{ for par,} \\ s & \text{quando } m \text{ for ímpar,} \end{cases}$$

sendo s o número de imersões reais de L .

18.5. Seja $L = \mathbb{Q}(\alpha)$, sendo α uma raiz do polinômio $X^3 - 5$.

- a) Indique a imersão canônica $\chi : L \rightarrow \mathbb{L}^{1,1} = \mathbb{R} \times \mathbb{C}$ de L .
- b) Prove que $\chi(\mathbb{Z}[\alpha])$ é uma rede completa de $\mathbb{L}^{1,1}$; indique uma base desta rede e calcule o volume de suas malhas.
- c) Indique um ponto, diferente de $(0, 0)$, desta rede que esteja dentro do cilindro $\left\{ (\xi, \omega) \in \mathbb{R} \times \mathbb{C} \mid |\xi| < \frac{1}{2}, |\omega| < 4 \right\}$.

18.6. Seja L um corpo de números algébricos. Prove que a imagem, sob a imersão canônica de L , de qualquer ideal $\mathfrak{a}$ não-nulo de I_L , é uma rede completa, e calcule o volume das suas malhas, em termos de d_L e $\mathfrak{N}\mathfrak{a}$.

18.7. Seja $L = \mathbb{Q}(\alpha)$, sendo α uma raiz do polinômio $X^3 - 10 \cdot X + 5$. Prove que existem elementos invertíveis ε, η de $\mathbb{Z}[\alpha]$ tais que $\varepsilon > 1$, $\eta > 1$, $\mathcal{N}_{L/\mathbb{Q}} \eta = 1$ e $\varepsilon^m \neq \eta^n$, quaisquer que sejam $m, n \in \mathbb{N} \setminus \{0\}$.

18.8. Usando as notações de (18.12) e sendo $r = s + t - 1$, $\mathcal{N} = \mathcal{N}_{L|\mathbb{Q}}$, prove que:

- Se $s \neq 0$ então $W(S) = \{1, -1\}$.
- Se n for ímpar, então $W(S) = \{1, -1\}$ e existirá um sistema de invertíveis fundamentais $\varepsilon_1, \dots, \varepsilon_r$ de S tais que $\mathcal{N}\varepsilon_1 = \dots = \mathcal{N}\varepsilon_r = 1$ e $\mathcal{N}((-1)^e \cdot \varepsilon_1^{k_1} \cdot \dots \cdot \varepsilon_r^{k_r}) = (-1)^e$, quaisquer que sejam $e \in \{0, 1\}$ e $k_1, \dots, k_r \in \mathbb{Z}$.
- Se n for par, então existirá um sistema de invertíveis fundamentais $\varepsilon_1, \dots, \varepsilon_r$ de S tais que

$$\mathcal{N}\varepsilon_1 = \dots = \mathcal{N}\varepsilon_{r-1} = 1 \text{ e } \mathcal{N}(\zeta \cdot \varepsilon_1^{k_1} \cdot \dots \cdot \varepsilon_r^{k_r}) = (\mathcal{N}\varepsilon_r)^{k_r},$$

quaisquer que sejam $\zeta \in W(S)$ e $k_1, \dots, k_r \in \mathbb{Z}$.

§19. Invertíveis em corpos quadráticos

Estudaremos neste parágrafo o grupo $U(S)$ dos elementos invertíveis de uma "ordem" S de um corpo quadrático, bem como o seu relacionamento com as soluções da "equação de Pell" $X^2 - k \cdot Y^2 = 1$ e de outras equações diofantinas.

No §2 foi provado que todo corpo quadrático é da forma $L_d = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$ univocamente determinado, e que $1, \delta$ formam uma base para o seu anel dos inteiros I_d , considerado como $\mathbb{Z}$ -módulo, sendo $\delta = \sqrt{d}$ (respectivamente $= \frac{1 + \sqrt{d}}{2}$) no caso em que $d \equiv 2$ ou 3 (respectivamente $\equiv 1 \pmod{4}$). É óbvio que, para qualquer $n \in \mathbb{N} \setminus \{0\}$, $S_{d,n} = \mathbb{Z}[n \cdot \delta]$ é um subanel de I_d , que $1, n \cdot \delta$ formam uma base para o $\mathbb{Z}$ -módulo $S_{d,n}$, e que $S_{d,n} \subseteq S_{d,n'}$ se e somente se n' for um divisor de n ; em particular, temos que $I_d = S_{d,1}$. Recordamos ainda que $\text{disc}_{L_d|\mathbb{Q}}(1, n \cdot \delta) = n^2 \cdot d_{L_d}$ e $(I_d : S_{d,n}) = n$ (veja §4A e (5.7)). O seguinte teorema mostra que todo subanel de I_d , diferente de $\mathbb{Z}$, é igual a um dos anéis $S_{d,n}$.

(19.1) TEOREMA. O conjunto $\mathcal{S}_d$ dos subanéis S de I_d tais que $\mathbb{Z} \neq S$ está em correspondência biunívoca com o conjunto $\mathbb{N} \setminus \{0\}$, dada pelas aplicações

$$n \mapsto S_{d,n} \quad (n \in \mathbb{N} \setminus \{0\}) \quad \text{e} \quad S \mapsto (I_d : S) \quad (S \in \mathcal{S}_d).$$

Demonstração. De $S_{d,n} = S_{d,n'}$ decorre que $n = n'$; portanto a aplicação $n \mapsto S_{d,n}$ é injetiva. Basta mostrar que ela é sobrejetiva. Seja

$S \in \mathcal{S}_d$; então todo elemento de S é da forma $a + b \cdot \delta$, com $a, b \in \mathbb{Z}$, e existe um menor $n \in \mathbb{N} \setminus \{0\}$ tal que $c + n \cdot \delta \in S$ para algum $c \in \mathbb{Z}$; portanto $n \cdot \delta \in S$ e assim $S_{d,n} \subseteq S$. Por outro lado, seja $a + b \cdot \delta \in S$, com $a, b \in \mathbb{Z}$. Existem $q, r \in \mathbb{Z}$ tais que $b = q \cdot n + r$ e $0 \leq r < n$; portanto $a - q \cdot c + r \cdot \delta = (a + b \cdot \delta) - q \cdot (c + n \cdot \delta) \in S$; logo $r = 0$ pela escolha de n , e assim $a + b \cdot \delta \in S_n$. $\square$

Observemos que os $S \in \mathcal{S}_d$ são exatamente as "ordens" de L_d no sentido de (5.5). Notemos ainda que, no caso em que $d \equiv 1 \pmod{4}$, temos que $S_{d,2n} = \mathbb{Z}[n \cdot \sqrt{d}]$ e que às vezes convém usar, neste caso, a base $1, n \cdot \sqrt{d}$ em lugar da base $1, 2n \cdot \delta$.

Recordamos que o grupo dos elementos invertíveis de $S \in \mathcal{S}_d$ é dado por $U(S) = \{\eta \in S \mid |\mathcal{N}\eta| = 1\} = U(I_d) \cap S$, sendo $\mathcal{N} = \mathcal{N}_{L_d|\mathbb{Q}}$ (veja (1.11c)). Às vezes convém separar os invertíveis de norma 1 dos de norma -1 ; por isto definimos $U_e(S) = \{\eta \in S \mid \mathcal{N}\eta = (-1)^e\}$ ($e = 0, 1$), e assim $U(S) = U_0(S) \cup U_1(S)$ (reunião disjunta). Recordamos também que

$$\mathcal{N}(x + y \cdot n \cdot \sqrt{d}) = x^2 - n^2 \cdot d \cdot y^2 \text{ e}$$

$$\mathcal{N}\left(x + y \cdot n \cdot \frac{1 + \sqrt{d}}{2}\right) = x^2 + n \cdot x \cdot y - n^2 \cdot \frac{d-1}{4} \cdot y^2,$$

quaisquer que sejam $x, y \in \mathbb{Q}$. Concluimos que vale a seguinte proposição, quaisquer que sejam $a, b \in \mathbb{Z}$ e $e \in \{0, 1\}$:

(19.2) a) $a + b \cdot n \cdot \sqrt{d} \in U_e(\mathbb{Z}[n \cdot \sqrt{d}])$ se e somente se (a, b) for solução da equação $X^2 - n^2 \cdot d \cdot Y^2 = (-1)^e$.

b) No caso em que $d \equiv 1 \pmod{4}$ teremos que $a + b \cdot n \cdot \delta \in U_e(S_{d,n})$ se e somente se (a, b) for solução da equação

$$X^2 + n \cdot X \cdot Y - n^2 \cdot \frac{d-1}{4} \cdot Y^2 = (-1)^e.$$

Notemos que a afirmação a) se aplica não somente ao caso em que $d \equiv 2$ ou $3 \pmod{4}$, no qual $\mathbb{Z}[n \cdot \sqrt{d}] = S_{d,n}$, mas também ao caso em que $d \equiv 1 \pmod{4}$, no qual $\mathbb{Z}[n \cdot \sqrt{d}] = S_{d,2n}$.

Quando o corpo quadrático L_d for imaginário, isto é, $d < 0$, temos que $U_1(S) = \emptyset$ e $U(S) = W(S)$ (veja (2.7)), em concordância com o teorema de invertíveis de Dirichlet (18.12). Considerando as equações indicadas em

(19.2), obtemos a seguinte generalização do teorema (2.7), que mostra que I_{-1} e I_{-3} são os únicos $S \in \{S_{d,n} \mid d \in \mathcal{D}, n \in \mathbb{N} \setminus \{0\}\}$ tais que o grupo $U(S)$ tenha ordem > 2 .

(19.3) TEOREMA. a) $U(I_{-1}) = U(S_{-1,1}) = \{1, -1, i, -i\}$.

b) $U(I_{-3}) = U(S_{-3,1}) = \{\zeta^j \mid j = 0, \dots, 5\}$ onde $\zeta = \frac{1 + \sqrt{-3}}{2}$.

c) $U(S_{d,n}) = \{1, -1\}$ para qualquer $(d, n) \notin \{(-1, 1), (-3, 1)\}$.

Demonstração. Resulta do fato de as equações indicadas em (19.2) possuírem soluções não-triviais (isto é, diferentes de $(1, 0)$ e $(-1, 0)$) somente nos seguintes casos: Se $d = -1$, $n = 1$, então $X^2 + Y^2 = 1$ terá as soluções não-triviais $(0, 1)$ e $(0, -1)$; se $d = -3$, $n = 1$, então $X^2 + X \cdot Y + Y^2 = 1$ terá as soluções não-triviais $(0, 1)$, $(0, -1)$, $(-1, 1)$ e $(1, -1)$. $\square$

Quando o corpo quadrático L_d for real, isto é, $d > 0$, teremos que $W(S) = \{1, -1\}$ e, pelo teorema de invertíveis de Dirichlet, $U(S) = \{1, -1\} \odot \langle \varepsilon \rangle$, onde ε tem ordem $o(\varepsilon)$ infinita. Obviamente, ε pode ser substituído por qualquer um dos elementos $\varepsilon, -\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}$, e exatamente um deles é maior que 1. Portanto, podemos supor que $\varepsilon > 1$, e este elemento será chamado o *invertível fundamental* de S .

Para calcular ε , convém considerar o conjunto $V(S) = \{\eta \in U(S) \mid \eta > 1\}$. É óbvio que $V(S) = \{\varepsilon^j \mid j \in \mathbb{N} \setminus \{0\}\}$ e, portanto, ε é o menor elemento de $V(S)$.

(9.4) Para quaisquer $d \in \mathcal{D}$ e $n \in \mathbb{N} \setminus \{0\}$ temos que

$$V(S_{d,n}) \subseteq \{a + b \cdot n \cdot \delta \mid a, b \in \mathbb{Z}, a > 0, b > 0\},$$

exceto no caso $(d, n) = (5, 1)$, no qual " $a > 0$ " deve ser substituído por " $a \geq 0$ ".

Demonstração. Sendo σ o único automorfismo não-idêntico de L_d ,

$$\text{temos que } \sigma\sqrt{d} = -\sqrt{d} \text{ e } \sigma\left(\frac{1 + \sqrt{d}}{2}\right) = \frac{1 - \sqrt{d}}{2}, \text{ logo}$$

$\delta - \sigma\delta > 0$. Seja $\eta \in V(S_{d,n})$, digamos, $\eta = a + b \cdot n \cdot \delta$, com $a, b \in \mathbb{Z}$. De $\eta \cdot \sigma\eta = \mathcal{N}\eta \in \{1, -1\}$ resulta que $\sigma\eta \in \{\eta^{-1}, -\eta^{-1}\}$; portanto $|a + b \cdot n \cdot \sigma\delta| = |\sigma\eta| < 1$ e $b \cdot n \cdot (\delta - \sigma\delta) = \eta - \sigma\eta > 0$; logo $b > 0$. Como $\sigma\delta < -1$ (com exceção do caso $d = 5$, no qual $-1 < \sigma\delta = \frac{1 - \sqrt{5}}{2} < 0$),

concluimos da desigualdade $|a + b \cdot n \cdot \sigma\delta| < 1$ que $a > 0$ (com exceção do caso $d = 5$, $n = 1$, no qual $a \geq 0$). $\square$

Distinguindo novamente entre os invertíveis com norma 1 e os com norma -1 , escrevemos $V(S) = V_0(S) \cup V_1(S)$, sendo

$$V_e(S) = V(S) \cap U_e(S) = \{\eta \in S \mid \eta > 1, \mathcal{N}\eta = (-1)^e\} \quad (e = 0, 1).$$

Estes conjuntos podem ser caracterizados da seguinte maneira.

(19.5) TEOREMA. a) No caso em que $d \equiv 2$ ou $3 \pmod{4}$ temos que

$$V_e(S_{d,n}) = \{a + b \cdot n \cdot \sqrt{d} \mid a, b \in \mathbb{N} \setminus \{0\}, a^2 - n^2 \cdot d \cdot b^2 = (-1)^e\} \quad (e = 0, 1).$$

b) No caso em que $d \equiv 1 \pmod{4}$ temos que

$$\begin{aligned} V_e(S_{d,n}) &= \left\{ a + b \cdot n \cdot \delta \mid a \in \mathbb{N}, b \in \mathbb{N} \setminus \{0\}, a^2 + n \cdot a \cdot b - n^2 \cdot \frac{d-1}{4} \cdot b^2 = (-1)^e \right\} = \\ &= \left\{ \frac{a}{2} + \frac{b}{2} \cdot n \cdot \sqrt{d} \mid a, b \in \mathbb{N} \setminus \{0\}, a^2 - n^2 \cdot d \cdot b^2 = (-1)^e \cdot 4 \right\} \quad (e = 0, 1). \end{aligned}$$

Demonstração. A afirmação a) e a primeira igualdade de b) resultam de

(19.2), (19.4) e do fato que $a + b \cdot n \cdot \delta > 1$, quaisquer que sejam $a \in \mathbb{N}$ e $b \in \mathbb{N} \setminus \{0\}$. Para provarmos a segunda igualdade de b), supomos que $d \equiv 1 \pmod{4}$. Seja $\eta \in V_e(S_{d,n})$, digamos, $\eta = a + b \cdot n \cdot \delta$ com $a \in \mathbb{N}$, $b \in \mathbb{N} \setminus \{0\}$. Então temos que $\eta = \frac{a'}{2} + \frac{b}{2} \cdot n \cdot \sqrt{d}$,

onde $a' = 2 \cdot a + b \cdot n \in \mathbb{N} \setminus \{0\}$, e $\frac{a'^2}{4} - n^2 \cdot d \cdot \frac{b^2}{4} = \mathcal{N}\eta = (-1)^e$, ou seja,

$$a'^2 - n^2 \cdot d \cdot b^2 = (-1)^e \cdot 4. \text{ Por outro lado, seja } \eta = \frac{a}{2} + \frac{b}{2} \cdot n \cdot \sqrt{d}$$

tal que $a, b \in \mathbb{N} \setminus \{0\}$ e $a^2 - n^2 \cdot d \cdot b^2 = (-1)^e \cdot 4$; então $a^2 \equiv n^2 \cdot b^2 \pmod{4}$, logo $a = n \cdot b + 2 \cdot a''$ para algum $a'' \in \mathbb{Z}$. Concluimos que $\eta = a'' + b \cdot n \cdot \delta \in S_{d,n}$ e mesmo $\eta \in V_e(S_{d,n})$, uma vez que $\eta > 1$ e

$$\mathcal{N}\eta = \frac{a^2}{4} - n^2 \cdot d \cdot \frac{b^2}{4} = (-1)^e. \quad \square$$

O seguinte corolário será útil para calcular o invertível fundamental.

(19.6) COROLÁRIO. Sejam $\eta_1, \eta_2 \in V(S_{d,n})$, digamos

$$\eta_j = \begin{cases} a_j + b_j \cdot n \cdot \sqrt{d} & \text{quando } d \equiv 2 \text{ ou } 3 \pmod{4} \\ \frac{a_j}{2} + \frac{b_j}{2} \cdot n \cdot \sqrt{d} & \text{quando } d \equiv 1 \pmod{4} \end{cases},$$

onde $a_j, b_j \in \mathbb{N} \setminus \{0\}$ ($j = 1, 2$). Então, $\eta_1 \leq \eta_2$ implica $b_1 \leq b_2$.

Demonstração. Seja $q = 1$ (respectivamente $= 4$) no caso em que $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) mod 4. De (19.5) resulta que $a_j^2 - n^2 \cdot d \cdot b_j^2 \in \{q, -q\}$, logo $a_j^2 + q \geq n^2 \cdot d \cdot b_j^2 \geq a_j^2 - q$ ($j = 1, 2$). Se $b_1 > b_2$, então $a_1^2 + q \geq n^2 \cdot d \cdot b_1^2 \geq n^2 \cdot d \cdot (b_2 + 1)^2 \geq n^2 \cdot d \cdot b_2^2 + 2 \cdot d \geq a_2^2 - q + 2 \cdot d > a_2^2 + q$, uma vez que $d > q$; portanto $a_1 > a_2$ e assim $\eta_1 > \eta_2$. $\square$

Concluimos de (19.6) que, para obter o invertível fundamental $\varepsilon_{d,n}$ de $S_{d,n}$, basta determinar o menor número $b \in \mathbb{N} \setminus \{0\}$ tal que $a^2 - n^2 \cdot d \cdot b^2 \in \{q, -q\}$ para algum $a \in \mathbb{N} \setminus \{0\}$, ou seja, que $n^2 \cdot d \cdot b^2 - q$ ou $n^2 \cdot d \cdot b^2 + q$ seja um quadrado em $\mathbb{N} \setminus \{0\}$. Nos seguintes exemplos será calculado, para alguns valores de $d \in \mathcal{D}$ e $n \in \mathbb{N} \setminus \{0\}$, o par

$$(n^2 \cdot d \cdot b^2 - q, n^2 \cdot d \cdot b^2 + q),$$

sucessivamente para $b = 1, 2, 3, \dots$. O primeiro quadrado ocorrendo num par deste tipo (posto em grifo) fornecerá o número $a \in \mathbb{N} \setminus \{0\}$ tal que

$$\varepsilon_{d,n} = \begin{cases} a + b \cdot n \cdot \sqrt{d} & \text{quando } d \equiv 2 \text{ ou } 3 \pmod{4} \\ \frac{a}{2} + \frac{b}{2} \cdot n \cdot \sqrt{d} & \text{quando } d \equiv 1 \pmod{4}, \end{cases}$$

e teremos que $\mathcal{N}\varepsilon_{d,n} = -1$ (respectivamente $= 1$) se e somente se quadrado ocorrer como o primeiro (respectivamente segundo) elemento deste par.

$d=2$	$b=1$	$b=2$	$b=3$	$b=4$	
$n=1$	(1,3)				$\varepsilon_{2,1} = 1 + \sqrt{2} = \varepsilon_2$
$n=2$	(7,9)				$\varepsilon_{2,2} = 3 + 2 \cdot \sqrt{2} = \varepsilon_2^2$
$n=3$	(17,19)	(71,73)	(161,163)	(287,289)	$\varepsilon_{2,3} = 17 + 12 \cdot \sqrt{2} = \varepsilon_2^4$
$n=4$	(31,33)	(127,129)	(287,289)		$\varepsilon_{2,4} = 17 + 12 \cdot \sqrt{2} = \varepsilon_2^4$
$n=5$	(49,51)				$\varepsilon_{2,5} = 7 + 5 \cdot \sqrt{2} = \varepsilon_2^3$

$$\boxed{d=5} \quad b=1 \quad b=2$$

$$n=1 \quad (1,9)$$

$$\varepsilon_{5,1} = \frac{1}{2} + \frac{1}{2} \cdot \sqrt{5} = \varepsilon_5$$

$$n=2 \quad (16,24)$$

$$\varepsilon_{5,2} = 2 + \sqrt{5} = \varepsilon_5^3$$

$$n=3 \quad (41,49)$$

$$\varepsilon_{5,3} = \frac{7}{2} + \frac{3}{2} \cdot \sqrt{5} = \varepsilon_5^4$$

$$n=4 \quad (76,84) \quad (316,324)$$

$$\varepsilon_{5,4} = 9 + 4 \cdot \sqrt{5} = \varepsilon_5^6$$

$$\boxed{d=17} \quad b=1 \quad b=2$$

$$n=1 \quad (13,21) \quad (64,72)$$

$$\varepsilon_{17,1} = 4 + \sqrt{17} = \varepsilon_{17}$$

$$n=2 \quad (64,72)$$

$$\varepsilon_{17,2} = 4 + \sqrt{17} = \varepsilon_{17}$$

$$\boxed{d=94} \quad b=1 \quad b=2$$

$$n=1 \quad (93,95) \quad (375,377)$$

$$b=221064$$

$$(4593713457023, 4593713457025)$$

$$\varepsilon_{94,1} = 2143295 + 221064 \cdot \sqrt{94} = \varepsilon_{94}$$

Uma tabela do invertível fundamental $\varepsilon_d = \varepsilon_{d,1}$ dos anéis $I_d = S_{d,1}$ para $d \in \mathcal{D}$, $2 \leq d \leq 101$, encontra-se em Borevich-Shafarevich [6], Table 1. Note-se que, a partir de ε_d , é fácil calcular $\varepsilon_{d,n}$ para qualquer $n > 1$. De fato, da igualdade $V(S_{d,n}) = V(I_d) \cap S_{d,n}$ resulta que $\varepsilon_{d,n}$ é a primeira entre as potências $\varepsilon_d^1, \varepsilon_d^2, \varepsilon_d^3, \dots$ que pertence a $S_{d,n}$, isto é, que é da forma $a + b \cdot \delta$ com $n \mid b$.

Vimos nos exemplos acima indicados que o invertível fundamental ε_d de I_d pode ter norma 1 ou -1 . Devido à multiplicatividade da norma, no primeiro caso todas as suas potências, e no segundo caso apenas as suas potências pares, têm norma 1. Este resultado estende-se, de maneira óbvia, aos elementos invertíveis arbitrários:

(19.7) a) Se o invertível fundamental ε de S tiver norma 1, então

$$V_0(S) = \{\varepsilon^j \mid j \in \mathbb{N} \setminus \{0\}\} = V(S), \quad V_1(S) = \phi,$$

$$U_0(S) = \{\pm \varepsilon^j \mid j \in \mathbb{Z}\} = U(S), \quad U_1(S) = \phi.$$

b) Se o invertível fundamental ε de S tiver norma -1 , então

$$V_0(S) = \{\varepsilon^{2j} \mid j \in \mathbb{N} \setminus \{0\}\}, \quad V_1(S) = \{\varepsilon^{2j+1} \mid j \in \mathbb{N}\}$$

$$U_0(S) = \{\pm \varepsilon^{2j} \mid j \in \mathbb{Z}\}, \quad U_1(S) = \{\pm \varepsilon^{2j+1} \mid j \in \mathbb{Z}\}.$$

Observamos ainda que se o invertível fundamental de I_d tiver norma 1, então o mesmo ocorrerá com o invertível fundamental de qualquer $S \in \mathcal{S}_d$.

No que se segue, os resultados sobre os elementos invertíveis serão utilizados para tratar o problema de determinar as soluções, de números inteiros, de certas equações diofantinas, isto é, equações do tipo $F(X, Y, \dots) = 0$ sendo F um polinômio com coeficientes em $\mathbb{Z}$.

Consideraremos primeiro, para qualquer $k \in \mathbb{Z}$ que não for um quadrado em $\mathbb{Z}$, a "equação de Pell" $X^2 - k \cdot Y^2 = 1$. Mostraremos que as suas soluções (inteiras) correspondem biunivocamente aos elementos invertíveis de $\mathbb{Z}[\sqrt{k}]$ com norma 1. Observamos inicialmente que $k = n^2 \cdot d$ para $d \in \mathcal{D}$ e $n \in \mathbb{N} \setminus \{0\}$ univocamente determinados; portanto

$$\mathbb{Z}[\sqrt{k}] = \mathbb{Z}[n \cdot \sqrt{d}] = S_{d, n} \text{ (respectivamente } = S_{d, 2n})$$

no caso em que $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) mod 4 e, portanto, é um subanel de I_d .

Para visualizar tal correspondência, convém introduzir em $\mathbb{Z} \times \mathbb{Z}$ a multiplicação; definida por

$$(a, b) \cdot_k (a', b') = (a \cdot a' + b \cdot b' \cdot k, a \cdot b' + a' \cdot b) \quad (a, b, a', b' \in \mathbb{Z}).$$

Munido desta multiplicação, além da adição componente a componente, o conjunto $\mathbb{Z} \times \mathbb{Z}$ torna-se um anel $\mathfrak{R}_k$ isomorfo a $\mathbb{Z}[\sqrt{k}] = \mathbb{Z}[n \cdot \sqrt{d}]$; de fato, a aplicação definida por

$$(a, b) \mapsto a + b \cdot \sqrt{k} = a + b \cdot n \cdot \sqrt{d} \quad (a, b \in \mathbb{Z})$$

é um isomorfismo θ_k de $\mathfrak{R}_k$ sobre $\mathbb{Z}[\sqrt{k}]$.

Denotaremos por $\mathfrak{U}_k$ (respectivamente $\mathfrak{U}_{e, k}$) a imagem inversa de $U(\mathbb{Z}[\sqrt{k}])$ (respectivamente de $U_e(\mathbb{Z}[\sqrt{k}])$, onde $e \in \{0, 1\}$), pelo isomorfismo θ_k . A primeira afirmação de (19.2) pode então ser reformulada da seguinte maneira.

(19.8) TEOREMA. $\mathfrak{U}_{e, k}$ é o conjunto das soluções da equação

$$X^2 - k \cdot Y^2 = (-1)^e \quad (e = 0, 1).$$

No caso em que $k < 0$, obtemos imediatamente de (19.3):

- (19.9) TEOREMA. a) $\mathcal{U}_{0, -1} = \mathcal{U}_{-1} = \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$.
 b) $\mathcal{U}_{0, k} = \mathcal{U}_k = \{(1, 0), (-1, 0)\}$ quando $k < -1$.
 c) $\mathcal{U}_{1, k} = \phi$ para qualquer $k < 0$.

Em outras palavras, quando k for negativo, a equação de Pell possuirá apenas as duas (e, no caso $k = -1$, as quatro) soluções triviais, enquanto que a equação $X^2 - k \cdot Y^2 = -1$ não possuirá nenhuma solução.

No caso em que $k > 0$, denotaremos por $e_k = (v_k, w_k)$ a imagem inversa, sob θ_k , do invertível fundamental do anel $\mathbb{Z}[\sqrt{k}]$ e recordamos que este é igual a $e_{d, n}$ (respectivamente $e_{d, 2n}$) no caso em que $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) mod 4. O seguinte teorema é uma consequência imediata de (19.7).

- (19.10) TEOREMA. a) Se o invertível fundamental de $\mathbb{Z}[\sqrt{k}]$ tiver norma 1, então $\mathcal{U}_{0, k} = \mathcal{U}_k = \{\pm e^j \mid j \in \mathbb{Z}\}$ e $\mathcal{U}_{1, k} = \phi$. Isto ocorrerá, em particular, quando $\mathcal{N}e_d = 1$.

- b) Se o invertível fundamental de $\mathbb{Z}[\sqrt{k}]$ tiver norma -1 , então $\mathcal{U}_{0, k} = \{\pm e^{2j} \mid j \in \mathbb{Z}\}$ e $\mathcal{U}_{1, k} = \{\pm e^{2j+1} \mid j \in \mathbb{Z}\}$.

É claro que as potências de e são entendidas no sentido da multiplicação; e é fácil calculá-las sucessivamente; por exemplo,

$$e_k^2 = (v_k^2 + w_k^2 \cdot k, 2 \cdot v_k \cdot w_k), \quad e_k^3 = (v_k^3 + 3 \cdot v_k \cdot w_k^2, 3 \cdot v_k^2 \cdot w_k + w_k^3 \cdot k),$$

..., além disto, $e_k^{-1} = (v_k, -w_k)$ (respectivamente $= (-v_k, w_k)$).

no caso em que o invertível fundamental de $\mathbb{Z}[\sqrt{k}]$ tiver norma 1 (respectivamente -1).

Os resultados assim obtidos sobre as soluções da equação de Pell serão reformulados no seguinte corolário.

- (19.11) COROLÁRIO. Para todo $k > 0$ que não for quadrado em $\mathbb{Z}$, a equação $X^2 - k \cdot Y^2 = 1$ terá uma infinidade de soluções. A equação $X^2 - k \cdot Y^2 = -1$ não terá nenhuma solução (terá, respectivamente, uma infinidade de soluções) quando o invertível fundamental de $\mathbb{Z}[\sqrt{k}]$ tiver norma 1 (respectivamente -1).

Consideremos ainda a equação $X^2 - k \cdot Y^2 = c$ para qualquer $c \in \mathbb{Z} \setminus \{0\}$. Seja $\mathcal{I}_k(c)$ a imagem inversa do conjunto $\{y \in \mathbb{Z}[\sqrt{k}] \mid \mathcal{N}y = c\}$ pelo isomorfismo θ_k ; em particular, $\mathcal{I}_k(1) = \mathcal{U}_{0, k}$ e $\mathcal{I}_k(-1) = \mathcal{U}_{1, k}$. Verifica-se facilmente que, em analogia a (19.8), vale o seguinte:

(19.12) TEOREMA. $\mathfrak{I}_k(c)$ é o conjunto das soluções da equação

$$X^2 - k \cdot Y^2 = c.$$

Da multiplicatividade da norma concluímos que se $t \in \mathfrak{I}_k(c)$, então para todo $e \in \mathcal{U}_{0,k}$ (respectivamente $\in \mathcal{U}_{1,k}$) temos que $e \cdot t \in \mathfrak{I}_k(c)$ (respectivamente $\in \mathfrak{I}_k(-c)$). Diremos que $t, t' \in \mathfrak{I}_k(c)$ são *associados* quando se distinguem por um $\mathcal{U}_{0,k}$ -fator $e \in \mathcal{U}_{0,k}$. Recordamos que

$$\{\gamma \in \mathbb{Z}[\sqrt{k}] \mid |\mathcal{N}\gamma| = c\}$$

é reunião de um número finito $m \geq 0$ de classes

$$U(\mathbb{Z}[\sqrt{k}]) \cdot \alpha_1, \dots, U(\mathbb{Z}[\sqrt{k}]) \cdot \alpha_m \text{ (veja 1.17)}.$$

Deste fato resulta imediatamente o seguinte:

(19.13) TEOREMA. $\mathfrak{I}_k(c)$ é reunião de um número finito $n \geq 0$ de classes

$$\mathcal{U}_{0,k} \cdot t_1, \dots, \mathcal{U}_{0,k} \cdot t_n.$$

Usando (19.9) e (19.10) concluímos:

(19.14) COROLÁRIO. a) No caso em que $k < 0$, a equação $X^2 - k \cdot Y^2 = c$ possui no máximo um número finito de soluções.

b) No caso em que $k > 0$, a equação $X^2 - k \cdot Y^2 = c$ não possui nenhuma solução ou possui uma infinidade de soluções, mas apenas um número finito de soluções não-associadas, duas a duas.

c) Se $k > 0$ e o invertível fundamental de $\mathbb{Z}[\sqrt{k}]$ tiver norma -1 , a existência de soluções da equação $X^2 - k \cdot Y^2 = c$ implica a existência de soluções da equação $X^2 - k \cdot Y^2 = -c$.

Mencionamos ainda que estes resultados podem ser estendidos às equações diofantinas que se obtêm de uma equação do tipo $X^2 - k \cdot Y^2 = c$ através de uma transformação das indeterminadas X, Y . Por exemplo, considerando a transformação $X \mapsto X + Y^j$, para algum $j \in \mathbb{N}$, é óbvio que (a, b) será uma solução de $X^2 - k \cdot Y^2 = c$ se e somente se $(a - b^j, b)$ for uma solução de $X^2 + 2 \cdot X \cdot Y^j + Y^{2j} - k \cdot Y^2 = c$.

Finalmente, queremos mencionar que a correspondência entre as soluções inteiras da equação $X^2 - k \cdot Y^2 = c$ e os elementos $\gamma \in \mathbb{Z}[\sqrt{k}]$ tais que $\mathcal{N}\gamma = c$ é um caso especial da teoria das "formas decompostas" (veja Borevich-Shafarevich [6], Chapter 2). De fato, sejam L um corpo de nú-

meros algébricos, $\alpha \in I_L$ um elemento primitivo e $\sigma_1, \dots, \sigma_n$ os isomorfismos de L em $\mathbb{C}$; então $F(X_1, \dots, X_n) = \prod_{j=1}^n \left(\sum_{h=1}^n \sigma_j \alpha^{h-1} \cdot X_h \right)$ é uma forma (isto é, um polinômio homogêneo) de grau n com coeficientes em $\mathbb{Z}$, e as soluções da equação diofantina $F(X_1, \dots, X_n) = c$ correspondem aos elementos $\gamma \in \mathbb{Z}[\alpha]$ tais que $\mathcal{N}_{L|\mathbb{Q}} \gamma = c$. Para determinar esses elementos, os sistemas de invertíveis fundamentais de $\mathbb{Z}[\alpha]$ representam um papel importante.

EXERCÍCIOS

19.1. Usando as notações de (19.6), prove que $\eta_1 < \eta_2$ implica $b_1 < b_2$, com exceção do caso em que

$$d = 5, n = 1, \eta_1 = \frac{1}{2} + \frac{1}{2} \cdot \sqrt{5} \text{ e } \eta_2 = \frac{3}{2} + \frac{1}{2} \cdot \sqrt{5}.$$

19.2. Seja $d \in \mathcal{D}$, $d > 0$. Prove que todo elemento invertível $\eta > 1$ de I_d , com exceção de $\frac{3 + \sqrt{5}}{2}$ no caso $d = 5$, é o invertível fundamental de algum $S \in \mathcal{S}_d$.

19.3. Seja $d \in \mathcal{D}$, $d > 0$. Prove que:

- a) Se $d \equiv 3 \pmod{4}$, então o invertível fundamental de $I_d = \mathbb{Z}[\sqrt{d}]$ tem norma 1.
- b) Se $d \equiv 1 \pmod{8}$, então o invertível fundamental de I_d coincide com o invertível fundamental de $S_{d,2} = \mathbb{Z}[\sqrt{d}]$.

19.4. Seja $d \in \mathcal{D}$, $d > 0$, $d \equiv 1 \pmod{4}$, e seja $\eta = \frac{a}{2} + \frac{b}{2} \cdot \sqrt{d} \in U(I_d)$, com $a, b \in \mathbb{Z}$. Prove que:

- a) $2 \mid a$ se e somente se $2 \mid b$, se e somente se $\eta \in \mathbb{Z}[\sqrt{d}]$, se e somente se $\eta \in U(\mathbb{Z}[\sqrt{d}])$.
- b) Se $\eta \notin \mathbb{Z}[\sqrt{d}]$, então $\eta^2 \notin \mathbb{Z}[\sqrt{d}]$ e $\eta^3 \in \mathbb{Z}[\sqrt{d}]$.

19.5. a) Prove que os números $b^2 \cdot 3 - 1$, $b^2 \cdot 11 - 1$, $b^2 \cdot 6 - 1$ e $b^2 \cdot 21 - 4$ não são quadrados em $\mathbb{Z}$, qualquer que seja $b \in \mathbb{Z}$.

b) Usando o fato de $170 + 39 \cdot \sqrt{19}$ ser o invertível fundamental de $\mathbb{Z}[\sqrt{19}]$, prove que $b^2 \cdot 19 - 1$ (respectivamente $b^2 \cdot 19 + 1$) não é quadrado em $\mathbb{Z}$, qualquer que seja $b \in \mathbb{Z}$ (respectivamente $b \in \mathbb{Z}$ tal que $|b| < 39$).

19.6. Sejam $d \in \mathcal{D}$, $d > 0$, $d \equiv 1 \pmod{4}$, $n \in \mathbb{N} \setminus \{0\}$ e $e \in \{0, 1\}$.

a) Determine as soluções $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ da equação

$$X^2 + n \cdot X \cdot Y - n^2 \cdot \frac{d-1}{4} \cdot Y^2 = (-1)^e$$

(respectivamente $X^2 + n^2 \cdot d \cdot Y^2 = (-1)^e \cdot 4$),

relacionando-as com os elementos invertíveis de $S_{d,n}$.

b) Formule e demonstre um teorema, análogo ao Corolário (19.14), sobre as soluções das equações

$$X^2 + n \cdot X \cdot Y - n^2 \cdot \frac{d-1}{4} \cdot Y^2 = c \quad \text{e} \quad X^2 - n^2 \cdot d \cdot Y^2 = 4 \cdot c$$

($c \in \mathbb{Z}$).

19.7. Determine as soluções $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ da equação

$$2 \cdot X^2 - 8 \cdot X \cdot Y + 7 \cdot Y^2 = (-1)^e \quad (e = 0, 1).$$

(Sugestão: Aplique a transformação $X \mapsto 3 \cdot X + 5 \cdot Y$, $Y \mapsto X + 2 \cdot Y$.)

19.8. Considere as equações diofantinas $X^2 - 6 \cdot Y^2 = c$, para todo

$$c \in \{-7, -5, -2, -1, 1, 2, 5, 7\}.$$

a) Quais destas equações possuem uma solução $(a, b) \in \mathbb{Z} \times \mathbb{Z}$?

b) Nos casos em que tal solução existe, indique um método de calcular uma infinidade de soluções.

19.9. Seja $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$, $d \equiv 2$ ou $3 \pmod{4}$, tal que I_L seja fatorial. Prove que, para qualquer número primo p , as seguintes condições são equivalentes:

(i) p é ramificado ou decomposto em I_L .

(ii) Pelo menos uma das equações $X^2 - d \cdot Y^2 = p$, $X^2 - d \cdot Y^2 = -p$ tem uma solução inteira.

EXTENSÕES GALOISIANAS

Neste capítulo, os resultados de §12 serão reforçados e complementados para extensões finitas galoisianas $L|K$.

Mostraremos primeiramente que, dado um domínio de Dedekind R com $K = Q(R)$, os ideais primos $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ de $S = I_L(R)$, acima de um ideal primo $\mathfrak{p}$ de R , são K -conjugados dois a dois. Neste fato baseia-se a definição de certos subgrupos do grupo de Galois $G = \text{Aut}(L|K)$, a saber, do grupo de decomposição G^Z (§20), do grupo de inércia G^I e de uma cadeia de grupos de ramificação $G^T = G_0^V \supseteq G_1^V \supseteq G_2^V \supseteq \dots$ (§21). Os corpos associados a estes grupos, pela teoria de Galois, formam uma cadeia $K \subseteq K^Z \subseteq K^I = K_0^V \subseteq K_1^V \subseteq K_2^V \subseteq \dots \subseteq L$, cujos graus relativos refletem o comportamento de decomposição, inércia e ramificação de $\mathfrak{p}$ sobre p .

§20. Grupo e corpo de decomposição

Sejam R um domínio de Dedekind, L uma extensão finita galoisiana de $K = Q(R)$, e $S = I_L(R)$. Para podermos provar que todos os ideais primos de S , acima de um ideal primo não-nulo $\mathfrak{p}$ de R , são K -conjugados, necessitaremos do seguinte lema, que é válido para anéis R arbitrários.

(20.1) *Sejam $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideais primos e $\mathfrak{a}$ um ideal qualquer de R . Se $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_r$, então $\mathfrak{a} \subseteq \mathfrak{p}_j$ para algum $j \in \{1, \dots, r\}$.*

Demonstração. Sem perda de generalidade podemos supor que, para quaisquer $i, j \in \{1, \dots, r\}$, $i \neq j$, temos que $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$. digamos $c_{j,i} \in \mathfrak{p}_i \setminus \mathfrak{p}_j$. Se para todo $j \in \{1, \dots, r\}$ existir um elemento $a_j \in \mathfrak{a} \setminus \mathfrak{p}_j$, então $b_j = c_{j,1} \cdot \dots \cdot c_{j,j-1} \cdot a_j \cdot c_{j,j+1} \cdot \dots \cdot c_{j,r} \in \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_{j-1} \cap \mathfrak{a} \cap \mathfrak{p}_{j+1} \cap \dots \cap \mathfrak{p}_r$, mas $b_j \notin \mathfrak{p}_j$; logo $b_1 + \dots + b_r \in \mathfrak{a} \setminus (\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_r)$. $\square$

(20.2) TEOREMA. Sejam R um domínio de Dedekind, $S = I_L(R)$, sendo L uma extensão finita galoisiana, e $G = \text{Aut}(L|K)$. Então:

a) $\sigma S = S$ para qualquer $\sigma \in G$.

Sejam $\mathfrak{p}$ um ideal primo não-nulo de R e $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ os ideais primos distintos de S , acima de $\mathfrak{p}$; então:

b) Todo $\sigma \in G$ induz um $R/\mathfrak{p}$ -isomorfismo de $S/\mathfrak{P}_j$ sobre $S/\sigma\mathfrak{P}_j$ ($j = 1, \dots, r$);

c) $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\} = \{\sigma\mathfrak{P}_1 | \sigma \in G\}$;

d) $e(\mathfrak{P}_1 | \mathfrak{p}) = \dots = e(\mathfrak{P}_r | \mathfrak{p})$ e $f(\mathfrak{P}_1 | \mathfrak{p}) = \dots = f(\mathfrak{P}_r | \mathfrak{p})$;

e) $e(\mathfrak{P}_j | \mathfrak{p}) \cdot f(\mathfrak{P}_j | \mathfrak{p}) \cdot r = [L : K]$ ($j = 1, \dots, r$).

Demonstração. a) Dado $\alpha \in S$, existe um polinômio mônico $F \in R[X]$ tal que $F(\alpha) = 0$. Para todo $\sigma \in G$ temos que $F(\sigma\alpha) = 0$, logo $\sigma\alpha \in S$. Concluímos que $\sigma S \subseteq S$, e vale mesmo a igualdade, pois $\sigma^{-1}S \subseteq S$ e assim $S = \sigma(\sigma^{-1}S) \subseteq \sigma S$.

b) Resulta do fato de, para quaisquer $\sigma \in G$ e $j \in \{1, \dots, r\}$, a composição de σ_S (= restrição de σ a S) com o homomorfismo canônico de S sobre $S/\sigma\mathfrak{P}_j$ ter núcleo $\mathfrak{P}_j$ e estender o homomorfismo canônico de R sobre $R/\mathfrak{p}$.

c) Para todo $\sigma \in G$ temos que $\sigma\mathfrak{P}_1 \cap R = \sigma(\mathfrak{P}_1 \cap R) = \mathfrak{p}$, logo $\sigma\mathfrak{P}_1 \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$. Suponhamos que exista $j \in \{1, \dots, r\}$ tal que $\mathfrak{P}_j \notin \{\sigma\mathfrak{P}_1 | \sigma \in G\}$; então $\mathfrak{P}_j \not\subseteq \sigma\mathfrak{P}_1$ para todo $\sigma \in G$, uma vez que $\mathfrak{P}_j$ é um ideal maximal de S . De (20.1) concluímos que $\mathfrak{P}_j \not\subseteq \bigcup_{\sigma \in G} \sigma\mathfrak{P}_1$, digamos

$\alpha \in \mathfrak{P}_j \setminus \bigcup_{\sigma \in G} \sigma\mathfrak{P}_1$. De a) resulta que $\prod_{\sigma \in G} \sigma\alpha = \mathcal{N}_{L|K}\alpha \in \mathfrak{P}_j \cap R = \mathfrak{p} \subseteq \mathfrak{P}_1$;

logo existe $\sigma \in G$ tal que $\sigma\alpha \in \mathfrak{P}_1$ e assim $\alpha \in \sigma^{-1}\mathfrak{P}_1$, em contradição com a escolha de α .

d) Para todo $\sigma \in G$ e $k \in \mathbb{N}$, $(\sigma\mathfrak{P}_1)^k$ dividirá o ideal $\mathfrak{p} \cdot S$ se e somente se $\mathfrak{P}_1^k$ dividir $\mathfrak{p} \cdot S$; portanto $e(\sigma\mathfrak{P}_1 | \mathfrak{p}) = e(\mathfrak{P}_1 | \mathfrak{p})$. De b) concluímos que $f(\sigma\mathfrak{P}_1 | \mathfrak{p}) = f(\mathfrak{P}_1 | \mathfrak{p})$. A afirmação d) resulta então de c).

e) Resulta de c), d) e (12.3). $\square$

A seguir, fixamos um ideal primo $\mathfrak{P}$ de S , acima de $\mathfrak{p}$. Escreveremos $e(\mathfrak{P}|K)$, $f(\mathfrak{P}|K)$ (ou simplesmente e , f) em lugar de $e(\mathfrak{P}|\mathfrak{p})$, $f(\mathfrak{P}|\mathfrak{p})$, e denotaremos por $r(\mathfrak{P}|K)$ (ou simplesmente r) o número de ideais primos que estiverem acima de $\mathfrak{p}$. Com estas notações, a igualdade fundamental (20.2e) escreve-se na seguinte forma:

$$e(\mathfrak{P}|K) \cdot f(\mathfrak{P}|K) \cdot r(\mathfrak{P}|K) = [L : K] \quad (\text{ou simplesmente } e \cdot f \cdot r = [L : K]).$$

Note-se que $e(\mathfrak{P}|K)$, $f(\mathfrak{P}|K)$ e $r(\mathfrak{P}|K)$ dependem apenas de $\mathfrak{p} = \mathfrak{P} \cap R$, isto é, coincidem para todo $\mathfrak{P}$ que está acima de $\mathfrak{p}$.

Além disto, denotamos por $\mathcal{K}$ (respectivamente $\mathcal{L}$) o corpo de restos $R/\mathfrak{p}$ (respectivamente $S/\mathfrak{P}$), e por κ (respectivamente λ) o homomorfismo canônico de R sobre $\mathcal{K}$ (respectivamente, de S sobre $\mathcal{L}$). Obviamente, $\mathcal{L}|\mathcal{K}$ é uma extensão finita de grau f . Mostramos:

(20.3) a) $\mathcal{L}|\mathcal{K}$ é uma extensão normal,

b) Para qualquer $\alpha \in S$, todas as raízes de $P_{\lambda\alpha|\mathcal{K}}$ (polinômio minimal de $\lambda\alpha$ sobre $\mathcal{K}$) estão em $\{\lambda(\sigma\alpha) \mid \sigma \in G\}$.

Demonstração. Para qualquer $\alpha \in S$ temos que $\prod_{\sigma \in G} (X - \sigma\alpha) = F_{\alpha, L|K} \in R[X]$, por (1.10). Como $\sigma\alpha \in S$ para todo $\sigma \in G$ e $\lambda\alpha$ é raiz de $\kappa F_{\alpha, L|K} = \prod_{\sigma \in G} (X - \lambda(\sigma\alpha))$, este polinômio é um múltiplo, em $\mathcal{K}[X]$, do polinômio $P_{\lambda\alpha|\mathcal{K}}$, o qual, portanto, se fatora em $\mathcal{L}[X]$ em polinômios lineares. Resulta que $\mathcal{L}|\mathcal{K}$ é normal e vale a afirmação b). $\square$

Deve-se mencionar que nem sempre $\mathcal{L}|\mathcal{K}$ é galoisiana, pois a separabilidade de $L|K$ não implica a de $\mathcal{L}|\mathcal{K}$ (veja Exercício 20.1.), a não ser que $\mathcal{K}$ seja um corpo perfeito.

Os ideais primos conjugados $\sigma\mathfrak{P}$ ($\sigma \in G$) serão distintos dois a dois se e somente se $\mathfrak{p}$ for totalmente decomposto em L , isto é, $r = [L:K]$, o que ocorrerá se e somente se $e = f = 1$. No caso geral, consideramos o subgrupo

$$G^Z(\mathfrak{P}|K) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

de G , que é chamado o *grupo de decomposição de $\mathfrak{P}$ sobre K* . Escreveremos G^Z em lugar de $G^Z(\mathfrak{P}|K)$, reservando a notação detalhada $G^Z(\mathfrak{P}''|K')$ para o caso de uma subextensão normal $L'|K'$, sendo $\mathfrak{P}'' = \mathfrak{P} \cap S''$ e $S'' = S \cap K''$.

Os grupos de decomposição dos ideais primos de S que estão acima de $\mathfrak{p}$ são subgrupos de G , conjugados dois a dois; de fato:

$$(20.4) \quad G^Z(\sigma\mathfrak{P}|K) = \sigma \circ G^Z \circ \sigma^{-1}, \text{ qualquer que seja } \sigma \in G.$$

Demonstração. Para quaisquer $\sigma \in G$ e $\rho \in G^Z$ temos que $(\sigma \circ \rho \circ \sigma^{-1})(\sigma\mathfrak{P}) = \sigma\mathfrak{P}$, logo $\sigma \circ G^Z \circ \sigma^{-1} \subseteq G^Z(\sigma\mathfrak{P}|K)$. A inclusão inversa resulta de $\sigma^{-1} \circ G^Z(\sigma\mathfrak{P}|K) \circ \sigma \subseteq G^Z(\sigma^{-1}(\sigma\mathfrak{P})|K) = G^Z$. $\square$

Convém considerar o grupo de decomposição de $\mathfrak{P}$ sobre corpos intermediários. A seguinte afirmação é óbvia.

(20.5) Se $K \subseteq K' \subseteq L$ então $G^Z(\mathfrak{P} | K') = G^Z \cap \text{Aut}(L | K')$.

Seja L' um corpo entre K e L tal que $L' | K$ seja normal (e, portanto, finita galoisiana). Denotaremos por θ o homomorfismo canônico de G sobre $G' = \text{Aut}(L | K)$, com núcleo $\text{Aut}(L | L')$, dado pela restrição $\sigma \mapsto \sigma|_{L'}$ ($\sigma \in G$). A seguinte proposição mostra que $G^Z(\mathfrak{P}' | K)$ é canonicamente isomorfo a $G^Z/G^Z(\mathfrak{P} | L')$, onde $\mathfrak{P}' = \mathfrak{P} \cap L'$, $S' = S \cap L'$.

(20.6) A restrição de θ ao subgrupo G^Z de G é um homomorfismo sobrejetivo $\theta^Z : G^Z \rightarrow G^Z(\mathfrak{P}' | K)$ com núcleo $G^Z(\mathfrak{P} | L)$.

Demonstração. Para todo $\sigma \in G^Z$ temos que $(\theta\sigma)\mathfrak{P}' = \sigma\mathfrak{P} \cap \sigma L' = \mathfrak{P}'$, logo $\theta\sigma \in G^Z(\mathfrak{P}' | K)$. Por outro lado, todo $\sigma' \in G^Z(\mathfrak{P}' | K)$ é a restrição a L' de algum $\sigma \in G$, e temos que $\sigma\mathfrak{P} \cap L' = \sigma'\mathfrak{P}' = \mathfrak{P}$; portanto $\mathfrak{P} = \rho(\sigma\mathfrak{P})$ para algum $\rho \in \text{Aut}(L | L')$. Concluimos que $\rho \circ \sigma \in G^Z$ e $\theta^Z(\rho \circ \sigma) = \theta\rho \circ \theta\sigma = \theta\sigma = \sigma'$. Resulta que θ^Z é sobrejetivo. O núcleo $\text{Aut}(L | L') \cap G^Z$ de θ^Z é igual a $G^Z(\mathfrak{P} | L)$, por (20.5). $\square$

O grupo de decomposição G^Z está relacionado com os números e , f e r da seguinte maneira. Seja $G/G^Z = \{\sigma \circ G^Z \mid \sigma \in G\}$ o conjunto das classes laterais à esquerda de G^Z em G ; então:

(20.7) a) A aplicação $\sigma \mapsto \sigma\mathfrak{P}$ ($\sigma \in G$) induz uma bijeção de G/G^Z sobre $\{\sigma\mathfrak{P} \mid \sigma \in G\}$.

b) r é igual ao índice $(G : G^Z)$.

c) $e \cdot f$ é igual à ordem de G^Z .

Demonstração. a) resulta do fato de $\sigma\mathfrak{P} = \rho\mathfrak{P}$ se e somente se $\sigma \circ G^Z = \rho \circ G^Z$, quaisquer que sejam $\sigma, \rho \in G$.

b) resulta de a).

c) resulta de b) e da igualdade fundamental. $\square$

Em particular, resulta de (20.7) que

- (20.8) $r = 1$ se e somente se $G^Z = G$;
 $r = [L : K]$ se e somente se G^Z for o grupo trivial.

Pela teoria de Galois, ao subgrupo G^Z de G é associado um corpo $K^Z(\mathfrak{P} | K)$ entre K e L , chamado o *corpo de decomposição de $\mathfrak{P}$ sobre K* . Escreveremos K^Z em lugar de $K^Z(\mathfrak{P} | K)$, reservando a notação detalhada $K^Z(\mathfrak{P}' | K')$ para o caso de uma subextensão normal $L' | K'$, sendo $\mathfrak{P}' = \mathfrak{P} \cap S'$, $S' = S \cap K'$. Obviamente,

- (20.9) $L | K^Z$ é uma extensão finita galoisiana com $\text{Aut}(L | K^Z) = G^Z$.

De (20.4), (20.5) e (20.6) resulta facilmente, pela teoria de Galois:

- (20.10) a) $K^Z(\sigma\mathfrak{P} | K) = \sigma K^Z$, qualquer que seja $\sigma \in G$.
 b) Se $K \subseteq K' \subseteq L$ então $K^Z(\mathfrak{P} | K') = K^Z \cdot K'$.
 c) Se $K \subseteq L' \subseteq L$ e $L' | K$ for normal, então $K^Z(\mathfrak{P}' | K) = K^Z \cap L'$ (onde $\mathfrak{P}' = \mathfrak{P} \cap S'$, $S' = S \cap L'$).

O corpo de decomposição pode ser caracterizado como o menor corpo K' entre K e L tal que $\mathfrak{P}$ seja o único ideal primo de S , acima de $\mathfrak{P} \cap R'$, onde $R' = S \cap K'$. Em outras palavras:

- (20.11) TEOREMA. Seja $K \subseteq K' \subseteq L$. Então, teremos que $K^Z \subseteq K'$ se e somente se $r(\mathfrak{P} | K') = 1$.

Demonstração. $r(\mathfrak{P} | K') = 1$ se e somente se $G^Z(\mathfrak{P} | K') = \text{Aut}(L | K')$, por (20.8). De (20.5) concluimos que isto ocorrerá se e somente se $\text{Aut}(L | K') \subseteq G^Z$, o que equivale a $K^Z \subseteq K'$, por (20.9). $\square$

Terminaremos este parágrafo calculando o grau das extensões $K^Z | K$ e $L | K^Z$ e os respectivos índices de ramificação e graus de inércia. Denotaremos por R^Z o anel $S \cap K^Z$, por $\mathfrak{p}^Z$ o ideal primo $\mathfrak{P} \cap R^Z$ de R^Z e por $\mathcal{K}^Z$ o corpo de restos $R^Z/\mathfrak{p}^Z$, o qual pode ser considerado como corpo entre $\mathcal{K}$ e $\mathcal{L}$.

- (20.12) COROLÁRIO. a) $[L : K^Z] = e \cdot f$, $[K^Z : K] = r$.
 b) $e(\mathfrak{p}^Z | K) = f(\mathfrak{p}^Z | K) = 1$, $\mathcal{K}^Z = \mathcal{K}$.
 c) $r(\mathfrak{P} | K^Z) = 1$, $e(\mathfrak{P} | K^Z) = e$, $f(\mathfrak{P} | K^Z) = f$.

Demonstração. a) resulta de (20.7) e (20.9).

b-c) De (20.11) resulta que $r(\mathfrak{P}|K^Z)=1$, logo $e(\mathfrak{P}|K^Z) \cdot f(\mathfrak{P}|K^Z) = [L:K^Z]$, pela igualdade fundamental. Por outro lado, temos que $[L:K^Z] = e \cdot f$, por a), e $e = e(\mathfrak{P}|K^Z) \cdot e(\mathfrak{p}^Z|K)$, $f = f(\mathfrak{P}|K^Z) \cdot f(\mathfrak{p}^Z|K)$, pela multiplicatividade do índice de ramificação e do grau de inércia (veja Exercício 12.5); portanto valem as igualdades indicadas em b) e c). $\square$

Notemos ainda que $r(\mathfrak{p}^Z|K) = r$ quando $K^Z|K$ for normal (veja Exercício 20.3).

EXERCÍCIOS

20.1. Sejam K_0 um corpo imperfeito e $R = K_0[t]$, sendo t transcendente sobre K_0 . Indique uma extensão finita galoisiana L de $K = K_0(t)$ tal que $S = I_L(R)$ possua um ideal primo $\mathfrak{P}$, acima de $\mathfrak{p} = t \cdot R$, cujo corpo de restos $\mathscr{L} = S/\mathfrak{P}$ seja inseparável sobre $\mathscr{K} = R/\mathfrak{p}$.

20.2. Prove que K^Z é o maior corpo K' entre K e L tal que $e(\mathfrak{p}'|K) = f(\mathfrak{p}'|K) = 1$, sendo $\mathfrak{p}' = \mathfrak{P} \cap R'$, $R' = S \cap K'$.

20.3. a) Prove que as seguintes condições são equivalentes:

(i) $r(\mathfrak{p}^Z|K) = r$;

(ii) $e(\mathfrak{p}'|K) = f(\mathfrak{p}'|K) = 1$ para todo ideal primo $\mathfrak{p}'$ de R^Z que está acima de $\mathfrak{p}$.

(iii) $e(\mathfrak{P}'|K^Z) = e$ e $f(\mathfrak{P}'|K^Z) = f$ para todo ideal primo $\mathfrak{P}'$ de S que está acima de $\mathfrak{p}$.

b) Prove que as condições indicadas em a) serão satisfeitas quando $K^Z|K$ for normal.

20.4. Dado um corpo quadrático (respectivamente ciclotômico) L , caracterize os números primos p tais que $K^Z(\mathfrak{P}|\mathbb{Q}) = L$, sendo $\mathfrak{P}$ um ideal primo de I_L , acima de $p \cdot \mathbb{Z}$.

20.5. Sejam K_1, K_2 corpos entre K e L tais que $L = K_1 \cdot K_2$. Prove que se o ideal primo $\mathfrak{p}$ de R for totalmente decomposto em K_1 e em K_2 , então será totalmente decomposto em L .

§21. Grupos e corpos de inércia e de ramificação

Usando as notações introduzidas no §20, recordamos que todo $\sigma \in G$ induz um $\mathcal{K}$ -isomorfismo $\bar{\sigma}$ de $\mathcal{L} = S/\mathfrak{P}$ sobre $S/\sigma\mathfrak{P}$ (veja (20.2 b)). Em particular, se $\sigma \in G^Z$ então $\bar{\sigma}$ será o $\mathcal{K}$ -automorfismo determinado por $\bar{\sigma} \circ \lambda = \lambda \circ \sigma_S$. Por (20.3), a extensão $\mathcal{L}|\mathcal{K}$ é normal e tem grau f . Por razões de simplificação, faremos a hipótese de $\mathcal{L}|\mathcal{K}$ ser separável⁽¹⁾; então será finita galoisiana, e seu grupo de Galois $\text{Aut}(\mathcal{L}|\mathcal{K})$ será denotado por $\mathcal{G}$.

Será chamado o grupo de inércia de $\mathfrak{P}$ sobre K , e denotado por $G^T(\mathfrak{P}|K)$, o conjunto

$$\{\sigma \in G^Z \mid \sigma\alpha - \alpha \in \mathfrak{P} \text{ para todo } \alpha \in S\}.$$

Escreveremos G^T em lugar de $G^T(\mathfrak{P}|K)$, reservando a notação detalhada $G^T(\mathfrak{P}''|K')$ para o caso de uma subextensão normal $L'|K'$, sendo $\mathfrak{P}'' = \mathfrak{P} \cap S''$ e $S'' = S \cap K''$. O fato de G^T ser realmente um subgrupo de G^Z resultará do seguinte:

- (21.1) TEOREMA. a) A aplicação $\sigma \mapsto \bar{\sigma}$ ($\sigma \in G^Z$) é um homomorfismo sobrejetivo $\Phi: G^Z \rightarrow \mathcal{G}$ com núcleo G^T .
b) G^T é um subgrupo normal de G^Z .

Demonstração. a) A aplicação indicada é um homomorfismo, pois $\overline{\sigma \circ \rho} \circ \lambda = \lambda \circ \sigma_S \circ \rho_S = \bar{\sigma} \circ \lambda \circ \rho_S = \bar{\sigma} \circ \bar{\rho} \circ \lambda$, quaisquer que sejam $\sigma, \rho \in G^Z$. Teremos que $\sigma \in G^T$ se e somente se $\lambda(\sigma\alpha) = \lambda\alpha$ para qualquer $\alpha \in S$, o que ocorrerá se e somente se $\bar{\sigma}$ for a aplicação idêntica de $\mathcal{L}$; portanto, G^T é o núcleo do homomorfismo Φ . Para mostrar que este é sobrejetivo, escolhemos um elemento primitivo de $\mathcal{L}|\mathcal{K}$, digamos $\lambda\beta$, onde $\beta \in S$. Seja $\hat{\sigma} \in \mathcal{G}$; então $\hat{\sigma}(\lambda\beta)$ é uma raiz de $P_{\lambda\beta|K}$. Aplicando (20.3 b) à extensão $L|K^Z$ e observando que $\mathcal{K}^Z = \mathcal{K}$, por (20.12 b), concluímos que $\hat{\sigma}(\lambda\beta) = \lambda(\sigma\beta)$ para algum $\sigma \in \text{Aut}(L|K^Z) = G^Z$ e, portanto, $\hat{\sigma}(\lambda\beta) = (\Phi\sigma)(\lambda\beta)$. Concluímos que os $\mathcal{K}$ -automorfismos $\hat{\sigma}$ e $\Phi\sigma$ coincidem no elemento primitivo $\lambda\beta$; portanto eles são iguais.

b) é uma consequência imediata de a). $\square$

Os grupos de inércia dos ideais primos de S que estão acima de $\mathfrak{p}$ são subgrupos de G conjugados dois a dois; de fato:

⁽¹⁾ Esta hipótese será supérflua quando $\mathcal{K}$ for um corpo perfeito, por exemplo, um corpo de característica zero ou um corpo finito. Em particular, ela será supérflua quando K for um corpo de números algébricos.

(21.2) $G^T(\sigma\mathfrak{P} | K) = \sigma \circ G^T \circ \sigma^{-1}$, qualquer que seja $\sigma \in G$.

Demonstração. Quaisquer que sejam $\sigma \in G$, $\rho \in G^T$ e $\alpha \in S$, temos que $(\sigma \circ \rho \circ \sigma^{-1})(\sigma\alpha) = \sigma\rho\alpha = \sigma(\rho\alpha) \in \sigma\mathfrak{P}$; portanto $\sigma \circ G^T \circ \sigma^{-1} \subseteq G^T(\sigma\mathfrak{P} | K)$. A inclusão inversa resulta de

$$\sigma^{-1} \circ G^T(\sigma\mathfrak{P} | K) \circ \sigma \subseteq G^T(\sigma^{-1}(\sigma\mathfrak{P}) | K) = G^T. \quad \square$$

Seja K' um corpo entre K e L . Recordamos que

$$G^Z(\mathfrak{P} | K') = G^Z \cap \text{Aut}(L | K'),$$

por (20.5), e denotamos por $\mathcal{H}$ o grupo de Galois $\text{Aut}(\mathcal{L} | \mathcal{K}')$, onde $\mathcal{K}' = R'/\mathfrak{p}'$, $\mathfrak{p}' = \mathfrak{P} \cap R'$ e $R' = S \cap K'$. Seja $\Phi' : G^Z(\mathfrak{P} | K') \rightarrow \mathcal{H}$ o homomorfismo definido em (21.1) em relação à extensão $L | K'$. Da própria definição resulta imediatamente:

(21.3) O homomorfismo $\Phi' : G^Z(\mathfrak{P} | K') \rightarrow \mathcal{H}$ é igual à restrição do homomorfismo $\Phi : G^Z \rightarrow \mathcal{G}$ e tem como núcleo o grupo $G^T(\mathfrak{P} | K') = G^T \cap \text{Aut}(L | K')$.

Pela teoria de Galois, ao subgrupo G^T de G é associado um corpo $K^T(\mathfrak{P} | K)$ entre K^Z e L , chamado o corpo de inércia de $\mathfrak{P}$ sobre K . Escreveremos K^T em lugar de $K^T(\mathfrak{P} | K)$, reservando a notação detalhada para o caso de subextensões normais. Obtemos de (21.1) o seguinte:

(21.4) COROLÁRIO. a) $L | K^T$ é uma extensão finita galoisiana com $\text{Aut}(L | K^T) = G^T$.

b) $K^T | K^Z$ é uma extensão finita galoisiana, e o homomorfismo $\Phi : G^Z \rightarrow \mathcal{G}$ induz um isomorfismo de $\text{Aut}(K^T | K^Z)$ sobre $\mathcal{G}$.

Demonstração. a) é óbvio.

b) De (21.1 b) resulta que $K^T | K^Z$ é uma extensão normal e, portanto, finita galoisiana. O homomorfismo canônico θ^{ZT} de $\text{Aut}(L | K^Z) = G^Z$ sobre $\text{Aut}(K^T | K^Z)$ tem núcleo $\text{Aut}(L | K^T) = G^T$; logo o homomorfismo Φ indicado em (21.1) induz um isomorfismo $\bar{\Phi}$ de $\text{Aut}(K^T | K^Z)$ sobre $\mathcal{G}$, isto é, $\bar{\Phi} \circ \theta^{ZT} = \Phi$. $\square$

Analogamente ao corpo de decomposição, o corpo de inércia pode ser caracterizado por uma propriedade de “ser o menor”. De fato, usando as notações acima introduzidas, provamos o seguinte

(21.5) TEOREMA. Seja $K^Z \subseteq K' \subseteq L$. Então, teremos que $K^T \subseteq K'$ se e somente se $f(\mathfrak{P} | K') = 1$, ou seja, $\mathcal{K}' = \mathcal{L}$.

Demonstração. $G^Z(\mathfrak{P} | K') = \text{Aut}(L | K')$ por (20.5) e (20.9), e $G^T(\mathfrak{P} | K') = \text{Aut}(L | K^T) \cap \text{Aut}(L | K')$ por (21.3) e (21.4 a). Teremos que $f(\mathfrak{P} | K') = 1$ se e somente se $\mathcal{K}' = \mathcal{L}$, se e somente se $\mathcal{H}$ for o grupo trivial, o que ocorrerá se e somente se $G^T(\mathfrak{P} | K') = G^Z(\mathfrak{P} | K')$, por (21.1). Esta igualdade será válida se e somente se $\text{Aut}(L | K^T) \supseteq \text{Aut}(L | K')$, se e somente se $K^T \subseteq K'$. $\square$

Definindo R^T , $\mathfrak{p}^T$ e $\mathcal{K}^T$ analogamente às definições de R^Z , $\mathfrak{p}^Z$ e $\mathcal{K}^Z$, obtemos as seguintes igualdades para o grau das extensões $K^T | K^Z$ e $L | K^T$ e para os respectivos índices de ramificação e graus de inércia.

(21.6) COROLÁRIO. a) $[L : K^T] = e$, $[K^T : K^Z] = f$.
 b) $r(\mathfrak{p}^T | K^Z) = 1$, $e(\mathfrak{p}^T | K^Z) = 1$, $f(\mathfrak{p}^T | K^Z) = f$.
 c) $r(\mathfrak{P} | K^T) = 1$, $e(\mathfrak{P} | K^T) = e$, $f(\mathfrak{P} | K^T) = 1$, $\mathcal{K}^T = \mathcal{L}$.

Demonstração. a) resulta de (20.12 a), (21.4 b) e do fato de $\mathcal{G}$ ter ordem $[\mathcal{L} : \mathcal{K}] = f$.

b-c) De (20.12) resulta que $r(\mathfrak{p}^T | K^Z) = r(\mathfrak{P} | K^T) = 1$, e de (21.5) resulta que $f(\mathfrak{P} | K^T) = 1$; logo $e(\mathfrak{P} | K^T) = [L : K^T]$ pela igualdade fundamental. As outras igualdades resultam de $[L : K^T] = e$ e da multiplicatividade do índice de ramificação e do grau de inércia. $\square$

A situação descrita em (20.12) e (21.6) pode ser visualizada no seguinte quadro, mostrando que a decomposição, inércia e ramificação de $\mathfrak{P}$ ocorrem sucessivamente na passagem de K a K^Z , de K^Z a K^T e de K^T a L , respectivamente. Em particular, $\mathfrak{p}^Z$ é totalmente inerte em K^T e $\mathfrak{p}^T$ é totalmente ramificado em L .

grupo de Galois	corpo	ideal primo	índice de ramificação	grau de inércia
G^T	L	$\mathfrak{P}$	e	1
$\mathcal{G} \cong G^Z/G^T$	K^T	$\mathfrak{p}^T$	1	f
	K^Z	$\mathfrak{p}^Z$	1	1
	K	$\mathfrak{p}$	1	1

Utilizaremos (21.6) para demonstrar, para o grupo de inércia, uma afirmação análoga a (20.6). Seja L um corpo entre K e L , tal que $L|K$ seja normal; sejam S' , $\mathfrak{P}'$ e θ^Z como definidos no §20, $\mathcal{L}' = S'/\mathfrak{P}'$, $\mathcal{G}' = \text{Aut}(\mathcal{L}'|\mathcal{K})$, $\bar{\theta}$ o homomorfismo canônico de $\mathcal{G}$ sobre $\mathcal{G}'$, e $\Phi: G^Z \rightarrow \mathcal{G}$ (respectivamente $\bar{\Phi}: G^Z(\mathfrak{P}'|K) \rightarrow \mathcal{G}'$) o homomorfismo definido em (21.1) em relação à extensão $L|K$ (respectivamente $L|K$).

(21.7) a) $\bar{\Phi} \circ \theta^Z = \bar{\theta} \circ \Phi$.

b) A restrição de θ^Z ao subgrupo G^T de G^Z é um homomorfismo sobrejetivo $\theta^T: G^T \rightarrow G^T(\mathfrak{P}'|K)$ com núcleo $G^T(\mathfrak{P}|L)$.

Demonstração. a) Quaisquer que sejam $\sigma \in G^Z$ e $\alpha \in S'$, temos que $(\bar{\Phi}(\theta^Z \sigma))(\lambda' \alpha) = (\lambda'(\theta^Z \sigma))\alpha = \lambda(\sigma \alpha) = (\Phi \sigma)(\lambda \alpha) = (\bar{\theta} \circ \Phi \sigma)(\lambda' \alpha)$, sendo λ (respectivamente λ') o homomorfismo canônico de S sobre $\mathcal{L}$ (respectivamente de S' sobre $\mathcal{L}'$).

b) Qualquer que seja $\sigma \in G^T$, $\bar{\Phi}(\theta^Z \sigma) = \bar{\theta}(\Phi \sigma)$ é a aplicação idêntica de $\mathcal{L}'$, logo $\theta^Z \sigma \in G^T(\mathfrak{P}'|K)$; portanto, θ^Z induz um homomorfismo $\theta^T: G^T \rightarrow G^T(\mathfrak{P}'|K)$, cujo núcleo é igual a

$$G^Z(\mathfrak{P}|L) \cap G^T = G^Z \cap \text{Aut}(L|L) \cap G^T = G^T(\mathfrak{P}|L),$$

por (20.5) e (21.3). De (21.4 a) e (21.6 a) resulta que a ordem do grupo G^T (respectivamente $G^T(\mathfrak{P}|L)$, $G^T(\mathfrak{P}'|K)$) é igual a $e = e(\mathfrak{P}|K)$ (respectivamente $e(\mathfrak{P}|L)$, $e(\mathfrak{P}'|K)$). Da multiplicatividade do índice de ramificação concluimos que a ordem de G^T é igual ao produto das ordens de $G^T(\mathfrak{P}|L)$ e de $G^T(\mathfrak{P}'|K)$; portanto, θ^T é sobrejetivo. $\square$

Finalmente, de (21.2), (21.3) e (21.7) obtemos a seguinte proposição análoga a (20.10):

(21.8) a) $K^T(\sigma \mathfrak{P}|K) = \sigma K^T$, qualquer que seja $\sigma \in G$.

b) Se $K \subseteq K' \subseteq L$ então $K^T(\mathfrak{P}|K') = K^T \cap K'$.

c) Se $K \subseteq L \subseteq L$ e $L|K$ for normal, então $K^T(\mathfrak{P}'|K) = K^T \cap L$ (onde $\mathfrak{P}' = \mathfrak{P} \cap S'$, $S' = S \cap L$).

No que se segue, estudaremos mais detalhadamente a ramificação total de p^T em L através dos grupos de ramificação.

Para todo $i \in \mathbb{N}$, será chamado o i -ésimo grupo de ramificação de $\mathfrak{P}$ sobre K , e denotado por $G_i^Y(\mathfrak{P}|K)$ (ou simplesmente G_i^Y quando não houver ambigüidade), o conjunto

$$\{\sigma \in G^Z \mid \sigma \alpha - \alpha \in \mathfrak{P}^{i+1} \text{ para todo } \alpha \in S\}.$$

O fato de G_i^Y ser um subgrupo de G^Z resulta do seguinte:

(21.9) G_i^V é um subgrupo normal de G^Z , para todo $i \in \mathbb{N}$.

Demonstração. Todo $\sigma \in G^Z$ satisfaz obviamente $\sigma \mathfrak{P}^{i+1} = \mathfrak{P}^{i+1}$ e, portanto, induz um automorfismo $\bar{\sigma}_i$ do anel $S/\mathfrak{P}^{i+1}$, determinado por $\bar{\sigma}_i \circ \lambda_i = \lambda_i \circ \sigma_S$, sendo λ_i o homomorfismo canônico de S sobre $S/\mathfrak{P}^{i+1}$. A aplicação $\sigma \mapsto \bar{\sigma}_i$ ($\sigma \in G^Z$) é obviamente um homomorfismo com núcleo G_i^V ; portanto G_i^V é um subgrupo normal de G^Z . $\square$

Pela definição, G_0^V coincide com o grupo de inércia G^T , e temos que $G_0^V \supseteq G_1^V \supseteq G_2^V \supseteq \dots$. Nesta cadeia, somente um número finito de grupos são não-triviais; de fato:

(21.10) Existe $s \in \mathbb{N}$ tal que G_s^V seja o grupo trivial.

Demonstração. Como G_0^V é finito, a cadeia indicada é estacionária, digamos $G_s^V = G_{s+1}^V = \dots$ para algum $s \in \mathbb{N}$, logo $G_s^V = \bigcap_{i \in \mathbb{N}} G_i^V$.

Este é o grupo trivial, pois se $\sigma \in G_i^V$ para todo $i \in \mathbb{N}$, então $\sigma\alpha - \alpha \in \bigcap_{i \in \mathbb{N}} \mathfrak{P}^{i+1} = (0)$, logo $\sigma\alpha = \alpha$, qualquer que seja $\alpha \in S$. $\square$

É óbvio que vale, analogamente aos grupos de decomposição e de inércia, o seguinte:

(21.11) Se $K \subseteq K' \subseteq L$ então $G_i^V(\mathfrak{P} | K') = G_i^V \cap \text{Aut}(L | K')$ ($i \in \mathbb{N}$).

Para estudar os grupos de ramificação, necessitaremos do método de localização, isto é, da substituição dos anéis R e S pelos anéis de frações R_M e S_M , onde $M = R \setminus \mathfrak{p}$. Os grupos de decomposição, de inércia e de ramificação ficarão inalterados quando se substituir $\mathfrak{P}^i$ por $(\mathfrak{P} \cdot S_M)^i = \mathfrak{P}^i \cdot S_M$ ($i \in \mathbb{N}$); de fato:

(21.12) a) $G^Z = \{\sigma \in G \mid \sigma(\mathfrak{P} \cdot S_M) = \mathfrak{P} \cdot S_M\}$.
b) $G_i^V = \{\sigma \in G^Z \mid \sigma\alpha - \alpha \in (\mathfrak{P} \cdot S_M)^{i+1} \text{ para todo } \alpha \in S_M\}$ ($i \in \mathbb{N}$).

Demonstração. a) Como $\mathfrak{P} \cdot S_M = \{\gamma \cdot m^{-1} \mid \gamma \in \mathfrak{P}, m \in M\}$, por (11.1), $\sigma\mathfrak{P} = \mathfrak{P}$ implica que $\sigma(\mathfrak{P} \cdot S_M) = \mathfrak{P} \cdot S_M$; portanto vale a inclusão $\subseteq$. A inclusão inversa resulta de $\sigma S = S$ e $\mathfrak{P} \cdot S_M \cap S = \mathfrak{P}$ (veja (11.2)).

b) Quaisquer que sejam $\sigma \in G_i^V$, $\alpha \in S$ e $m \in M$, temos que $\sigma(\alpha \cdot m^{-1}) = \sigma\alpha \cdot m^{-1} = (\sigma\alpha - \alpha) \cdot m^{-1} \in \mathfrak{P}^{i+1} \cdot S_M = (\mathfrak{P} \cdot S_M)^{i+1}$; portanto vale a inclusão $\subseteq$. A inclusão inversa resulta de $\sigma S = S$ e $\mathfrak{P}^{i+1} \cdot S_M \cap S = \mathfrak{P}^{i+1}$ (veja (11.8 c)). $\square$

Fazendo a hipótese de $\mathfrak{p}$ ser totalmente ramificado em L , podemos dar aos grupos de ramificação uma forma mais simples. Esta hipótese implica, por (12.4), que $\mathfrak{P} \cdot S_M$ é o único ideal primo não-nulo do anel S_M o qual, portanto, é um domínio principal (veja (11.8a) e (8.17)); em particular, $\mathfrak{P} \cdot S_M$ é um ideal principal de S_M .

(21.13) Se $\mathfrak{p}$ for totalmente ramificado em L , então $G = G^Z = G^T$ e

$$G_i^V = \{\sigma \in G \mid \sigma\pi - \pi \in (\mathfrak{P} \cdot S_M)^{i+1}\} \quad (i \in \mathbb{N}),$$

qualquer que seja o gerador π do ideal $\mathfrak{P} \cdot S_M$.

Demonstração. Pela hipótese temos que $r=f=1$; logo $K=K^Z=K^T$ e assim $G=G^Z=G^T$. Na igualdade afirmada para G_i^V a inclusão $\subseteq$ resulta de (21.12b). Por outro lado, seja $\sigma \in G$ tal que $\sigma\pi - \pi \in (\mathfrak{P} \cdot S_M)^{i+1}$. Qualquer $\alpha \in S_M$ é da forma $\alpha = \sum_{i=0}^{n-1} a_i \cdot \pi^i$ com $a_0, \dots, a_{n-1} \in R_M$, por (13.8 b);

logo

$$\sigma\alpha - \alpha = \sum_{i=0}^{n-1} a_i \cdot (\sigma\pi^i - \pi^i) = \sum_{i=0}^{n-1} a_i \cdot (\sigma\pi - \pi) \cdot \sum_{j=0}^i (\sigma\pi)^{i-j} \cdot \pi^j \in (\mathfrak{P} \cdot S_M)^{i+1};$$

portanto vale a inclusão inversa. $\square$

Numa certa analogia com o homomorfismo Φ de G^Z , indicado em (21.1), indicaremos para cada $i \in \mathbb{N}$ um homomorfismo ψ_i de G_i^V , com núcleo G_{i+1}^V . Como preliminar mostraremos que, em qualquer anel R que possuir apenas um ideal maximal $\mathfrak{m}$, as potências de $\mathfrak{m}$ fornecerão uma cadeia de subgrupos do grupo dos invertíveis $U(R)$.

(21.14) Seja R um domínio que possua apenas um ideal maximal $\mathfrak{m}$. Então:

a) Para todo $i \geq 1$, $U_i = \{1 + a \mid a \in \mathfrak{m}^i\}$ é um subgrupo do grupo $U_0 = U(R)$ dos invertíveis de R , e temos que $U_0 \supseteq U_1 \supseteq U_2 \dots$.

b) U_0/U_1 é canonicamente isomorfo ao grupo multiplicativo do corpo $R/\mathfrak{m}$.

c) Para todo $i \geq 1$, U_i/U_{i+1} é canonicamente isomorfo ao grupo aditivo do $R/\mathfrak{m}$ -espaço $\mathfrak{m}^i/\mathfrak{m}^{i+1}$.

d) Se R for um domínio de Dedekind então, para todo $i \geq 1$, o grupo aditivo de $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ será isomorfo ao grupo aditivo do corpo $R/\mathfrak{m}$.

Demonstração. a) Seja $i \geq 1$. Para todo $a \in \mathfrak{m}^i$ temos que $1+a \in R \setminus \mathfrak{m} = U(R)$; portanto $U_i \subseteq U(R)$. Se $a, b \in \mathfrak{m}^i$ então $(1+a) \cdot (1+b) = 1+c$, onde $c = a+b+a \cdot b \in \mathfrak{m}^i$, e $(1+a)^{-1} = 1+d$, onde $d = -a \cdot (1+a)^{-1} \in \mathfrak{m}^i$; portanto, U_i é um subgrupo de $U(R)$. O resto é óbvio.

b) A aplicação $a \mapsto a + \mathfrak{m}$ ($a \in R$) induz obviamente um homomorfismo $U_0 \rightarrow (R/\mathfrak{m})^*$ com núcleo U_1 . Ele é sobrejetivo, uma vez que $R \setminus \mathfrak{m} = U_0$.

c) Seja $i \geq 1$. Se $a, b \in \mathfrak{m}^i$ então $(1+a) \cdot (1+b) \cdot (1+a+b)^{-1} = 1+a \cdot b \cdot (1+a+b)^{-1} \in U_{i+1}$. Portanto, a aplicação $a \mapsto (1+a) \cdot U_{i+1}$ ($a \in \mathfrak{m}^i$) é um homomorfismo do grupo aditivo $\mathfrak{m}^i$ sobre o grupo U_i/U_{i+1} , com núcleo $\mathfrak{m}^{i+1}$, e este induz um isomorfismo do grupo aditivo $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ sobre U_i/U_{i+1} . Obviamente, $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ pode ser considerado como $R/\mathfrak{m}$ -espaço (veja §9).

d) Por (9.2), $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ é um $R/\mathfrak{m}$ -espaço de dimensão 1. Portanto, seu grupo aditivo é isomorfo ao grupo aditivo de $R/\mathfrak{m}$. $\square$

Mostraremos a existência de um homomorfismo canônico ψ_i de G_i^V , para cada $i \in \mathbb{N}$, primeiramente sob a hipótese de $\mathfrak{p}$ ser totalmente ramificado em L . Recordamos que esta hipótese implica que $\mathfrak{P} \cdot S_M$ é um ideal principal e é o único ideal maximal de S_M .

(21.15) TEOREMA. Suponhamos que $\mathfrak{p}$ seja totalmente ramificado em L . Sejam $M = R \setminus \mathfrak{p}$, $U_0 = U(S_M)$, $U_i = \{1 + \alpha \mid \alpha \in (\mathfrak{P} \cdot S_M)^i\}$ ($i \geq 1$) e π um gerador do ideal $\mathfrak{P} \cdot S_M$.

Para todo $i \in \mathbb{N}$, a aplicação $\sigma \mapsto \frac{\sigma\pi}{\pi} \cdot U_{i+1}$ ($\sigma \in G_i^V$) independe da escolha de π e é um homomorfismo $\psi_i: G_i^V \rightarrow U_i/U_{i+1}$ com núcleo G_{i+1}^V .

Demonstração. Seja $\sigma \in G_i^V$. Por (21.12) temos que $\sigma\alpha - \alpha \in (\mathfrak{P} \cdot S_M)^{i+1}$ para

todo $\alpha \in S_M$. Portanto $\frac{\sigma\pi}{\pi} - 1 \in (\mathfrak{P} \cdot S_M)^{i+1}$ e assim $\frac{\sigma\pi}{\pi} \in U_{i+1}$

para todo $\pi \in U_0$, e $\frac{\sigma\pi}{\pi} - 1 \in (\mathfrak{P} \cdot S_M)^i$; logo $\frac{\sigma\pi}{\pi} \in U_i$. Se $\sigma, \tau \in G_i^V$, então

$\varepsilon = \frac{\tau\pi}{\pi} \in U_i \subseteq U_0$; logo $\frac{\sigma\varepsilon}{\varepsilon} \in U_{i+1}$ e $\frac{(\sigma \circ \tau)\pi}{\pi} = \frac{\sigma\pi}{\pi} \cdot \frac{\tau\pi}{\pi} \cdot \frac{\sigma\varepsilon}{\varepsilon}$; portanto, a

aplicação indicada é um homomorfismo de G_i^V em U_i/U_{i+1} . O seu núcleo é G_{i+1}^V , pois $\frac{\sigma\pi}{\pi} \in U_{i+1}$ se e somente se $\sigma\pi - \pi \in (\mathfrak{P} \cdot S_M)^{i+2}$, se e somente se $\sigma \in G_{i+1}^V$. O homomorfismo independe da escolha do gerador π de $\mathfrak{P} \cdot S_M$; de fato, se π' for um outro gerador, então $\pi' = \pi \cdot \varepsilon$ para um certo $\varepsilon \in U_0$, logo $\frac{\sigma\pi'}{\pi'} = \frac{\sigma\pi}{\pi} \cdot \frac{\sigma\varepsilon}{\varepsilon}$ com $\frac{\sigma\varepsilon}{\varepsilon} \in U_{i+1}$. $\square$

A hipótese de p ser totalmente ramificado em L pode ser eliminada:

(21.16) COROLÁRIO. Substituindo-se M por $M^T = R^T \backslash \mathfrak{p}^T$, a afirmação do Teorema (21.15) vale sem a hipótese de p ser totalmente ramificado em L .

Demonstração. Como $\mathfrak{p}^T = \mathfrak{P} \cap R^T$ é totalmente ramificado em L , por (21.6), a afirmação de (21.15) vale para os grupos $G_i^V(\mathfrak{P} | K^T)$ e os grupos U_i definidos em relação ao anel S_{M^T} . Por (21.4) e (21.11) temos que $G_i^V = G_i^V \cap G^T = G_i^V \cap \text{Aut}(L | K^T) = G_i^V(\mathfrak{P} | K^T)$. $\square$

Compondo ψ_i com os respectivos isomorfismos definidos em (21.14) e observando que $\mathcal{L} = S/\mathfrak{P}$ é canonicamente isomorfo a $S_{M^T}/\mathfrak{P} \cdot S_{M^T}$ por (11.8b), concluímos:

(21.17) COROLÁRIO. a) G^T/G_1^V é canonicamente isomorfo a um subgrupo do grupo multiplicativo de $\mathcal{L}$.

b) Para todo $i \geq 1$, G_i^V/G_{i+1}^V é isomorfo a um subgrupo do grupo aditivo de $\mathcal{L}$.

Recordamos que todo subgrupo finito do grupo multiplicativo de qualquer corpo é cíclico, e que sua ordem não é divisível pela característica do corpo (veja (3.1) e (3.2)). Por outro lado, o grupo aditivo de um corpo possui como subgrupos finitos obviamente apenas o grupo trivial no caso de característica zero, e p -grupos elementares (isto é, grupos isomorfos a produtos finitos $Z \times \dots \times Z$, onde Z tem ordem p) no caso de características $p \neq 0$.

Um subgrupo Δ de um grupo finito Γ será chamado p -subgrupo de Sylow de Γ se Δ for um p -grupo (isto é, sua ordem for uma potência de p) e o índice $(\Gamma : \Delta)$ não for divisível por p . Pelo segundo teorema de Sylow, os p -subgrupos de Sylow de Γ são conjugados em Γ dois a dois.

Estas observações permitem tirar de (21.17) as seguintes conclusões:

(21.18) COROLÁRIO. a) Se $\mathcal{L}$ tiver característica zero, então G^T será um grupo cíclico e G_1^Y será o grupo trivial.

b) Se $\mathcal{L}$ tiver característica $p \neq 0$, então G^T/G_1^Y será um grupo cíclico cuja ordem não é divisível por p , e para todo $i \geq 1$, G_i^Y/G_{i+1}^Y será um p -grupo elementar. Além disto, G_1^Y será o único p -subgrupo de Sylow de G^T .

Demonstração. a) Por (21.17), G^T/G_1^Y é cíclico e G_i^Y/G_{i+1}^Y é o grupo trivial para todo $i \geq 1$; logo $G_1^Y = G_2^Y = G_3^Y = \dots$. De (21.10) resulta que G_1^Y é trivial e que $G^T \cong G^T/G_1^Y$.

b) As afirmações relativas aos grupos G^T/G_1^Y e G_i^Y/G_{i+1}^Y resultam de (21.17). A ordem de G_1^Y é o produto das ordens dos grupos $G_1^Y/G_2^Y, \dots, G_{s-1}^Y/G_s^Y$, as quais são potências de p ; portanto, G_1^Y é um p -subgrupo de Sylow de G^T . É mesmo o único, pois G_1^Y é normal em G^T . $\square$

Pela teoria de Galois, ao subgrupo G_i^Y é associado um corpo K_i^Y entre K e L , chamado o i -ésimo corpo de ramificação de $\mathfrak{P}$ sobre K , para todo $i \in \mathbb{N}$; obviamente $K^T = K_0^Y \subseteq K_1^Y \subseteq K_2^Y \subseteq \dots \subseteq K_s^Y = K_{s+1}^Y = \dots = L$. De (21.18) e (21.9) resulta o seguinte:

(21.19) COROLÁRIO. a) No caso em que $\mathcal{L}$ tem característica zero, temos que $K_1^Y = K_2^Y = \dots = L$.

b) No caso em que $\mathcal{L}$ tem característica $p \neq 0$, para todo $i \geq 1$ a extensão $L|K_i^Y$ é finita galoisiana e $\text{Aut}(L|K_i^Y) = G_i^Y$ é um p -grupo; em particular, $\text{Aut}(L|K_1^Y)$ é o único p -subgrupo de Sylow de $\text{Aut}(L|K^T)$. Além disto, K_{i+1}^Y/K_i^Y é finita galoisiana e $\text{Aut}(K_{i+1}^Y|K_i^Y)$ é p -elementar.

c) $K_1^Y|K^T$ é finita galoisiana e $\text{Aut}(K_1^Y|K^T)$ é canonicamente isomorfo a um subgrupo de $\mathcal{L}^*$. Em particular, este grupo é cíclico e, se $\mathcal{L}$ tiver característica $p \neq 0$, sua ordem não será divisível por p .

d) Para todo $i \in \mathbb{N}$, $K_i^Y|K^Z$ é finita galoisiana.

Analogamente aos corpos K^Z e K^T , o corpo K_1^Y pode ser caracterizado por uma propriedade de "ser o menor"; de fato:

(21.20) TEOREMA. Suponhamos que $\mathcal{L}$ tenha característica $p \neq 0$. Seja $K^T \subseteq K' \subseteq L$. Então teremos que $K_1^Y \subseteq K'$ se e somente se $e(\mathfrak{P}|K')$ for uma potência de p .

Demonstração. Como $\mathfrak{p}^T$ é totalmente ramificado em L , $\mathfrak{p}' = \mathfrak{P} \cap (S \cap K')$ também o é; logo $e(\mathfrak{P}|K') = [L:K']$; portanto $e(\mathfrak{P}|K')$ será uma potência de p se e somente se $\text{Aut}(L|K')$ for um p -grupo. De (21.19b) concluímos que isto ocorrerá se e somente se $\text{Aut}(L|K') \subseteq \text{Aut}(L|K_1^Y)$, se e somente se $K_1^Y \subseteq K'$. $\square$

Para poder tratar simultaneamente os casos em que $\mathcal{L}$ tem característica zero ou $p \neq 0$, convém introduzir o *expoente característico* de um corpo. Este será definido como 1 quando a característica for zero, e igual à característica quando esta for $p \neq 0$.

Seja p o expoente característico de $\mathcal{L}$; então $\tilde{e} = p^t \cdot \tilde{e}$ onde $t \in \mathbb{N}$ e $\text{MDC}(p, \tilde{e}) = 1$ (em particular $p^t = 1, \tilde{e} = e$ no caso $p = 1$). Sejam $R^V = S \cap K_1^V$ e $\mathfrak{p}^V = \mathfrak{P} \cap R^V$. Então:

(21.21) COROLÁRIO. a) $[L : K_1^V] = e(\mathfrak{P} | K_1^V) = p^t$.

b) $[K_1^V : K^T] = e(\mathfrak{p}^V | K^T) = \tilde{e}$, e $\text{Aut}(K_1^V | K^T)$ é canonicamente isomorfo ao grupo $W_e(\mathcal{L})$.

Demonstração. De (21.6) concluímos que $[L : K_1^V] \cdot [K_1^V : K^T] = [L : K^T] = p^t \cdot \tilde{e}$, $[L : K_1^V] = e(\mathfrak{P} | K_1^V)$ e $[K_1^V : K^T] = e(\mathfrak{p}^V | K^T)$. De (21.20) resulta que $[L : K_1^V]$ é uma potência de p e que $\text{MDC}(p, [K_1^V : K^T]) = 1$; portanto, $[L : K_1^V] = p^t$ e $[K_1^V : K^T] = \tilde{e}$. Como o grupo $\text{Aut}(K_1^V | K^T)$ tem ordem $[K_1^V : K^V] = \tilde{e}$, o subgrupo de $\mathcal{L}^*$ ao qual é canonicamente isomorfo por (21.10 c), é igual a $W_e(\mathcal{L})$, por (3.1). $\square$

A parte superior do quadro na página 181 pode ser refinada, através da inserção do corpo K_1^V , da seguinte maneira:

grupo de Galois	corpo	ideal primo	índice de ramificação	grau de inércia
G_1^V	$\left\{ \begin{array}{c} L \\ \\ K_1^V \end{array} \right\}$	$\left\{ \begin{array}{c} \mathfrak{P} \\ \\ \mathfrak{p}^V \end{array} \right\}$	p^t	1
$W_e(\mathcal{L}) \cong G^T/G_1^V$	$\left\{ \begin{array}{c} \\ K^T \end{array} \right\}$	$\left\{ \begin{array}{c} \\ \mathfrak{p}^T \end{array} \right\}$	$\tilde{e}$	1

Isto mostra, que a ramificação existente entre K^T e L se obtém em duas etapas. Na passagem de K^T a K_1^V ocorre a *ramificação mansa* (isto é, $\text{MDC}(p, e(\mathfrak{p}^V | K^T)) = 1$), seguida pela *ramificação selvagem* (isto é, $e(\mathfrak{P} | K_1^V) = p^t$) na passagem de K_1^V a L ; o selvagismo desta ramificação pode ser descrita pelos grupos p -elementares $G_1^V/G_2^V, G_2^V/G_3^V, \dots, G_{s-1}^V/G_s^V$. Evidentemente, não ocorrerá nenhuma ramificação selvagem quando $\mathcal{L}$ tiver característica zero.

A cadeia $G^Z \supseteq G^T \supseteq G_1^V \supseteq \dots \supseteq G_s^V$ de subgrupos normais de G^Z fornece ainda o seguinte:

- (21.22) TEOREMA. a) $G^T = \text{Aut}(L|K^T)$ é um grupo solúvel.
 b) Se $\mathcal{G} = \text{Aut}(\mathcal{L}|\mathcal{K})$ for um grupo solúvel, então G^Z também o será.

Demonstração. a) Na cadeia acima indicada, os grupos quocientes $G^T/G_1^V, G_1^V/G_2^V, \dots, G_{s-1}^V/G_s$ são grupos abelianos, por (21.17), e G_s^V é o grupo trivial, por (21.10); portanto, G^T é solúvel.

b) Como $\mathcal{G}$ é isomorfo a G^Z/G^T por (21.1), da solubilidade de $\mathcal{G}$ resulta a de G^Z/G^T . Sendo G^Z/G^T e G^T solúveis, o grupo G^Z também o é. $\square$

Note-se que $\mathcal{G}$ será solúvel (e mesmo cíclico) quando $\mathcal{K}$ for um corpo finito e, em particular, quando L for um corpo de números algébricos.

O Teorema (21.22) tem uma interessante consequência a respeito da possibilidade de L ser gerado por radicais:

- (21.23) COROLÁRIO. a) $L|K^T$ é uma extensão solúvel por radicais.
 b) Se $\mathcal{G}$ for solúvel, então $L|K^Z$ será uma extensão solúvel por radicais.

Note-se que, no caso em que L tiver característica $p \neq 0$, a noção “solúvel por radicais” deverá ser entendida no sentido da definição feita em Lang [20], Chapter VIII, §7, admitindo como “radicais” também as raízes de polinômios da forma $X^p - X - a$.

Observemos ainda que as ordens dos grupos de ramificação $G_0^V, G_1^V, \dots, G_s^V$ estão relacionadas com o diferente, mencionado no §13 (veja Ribenboim [28], Chapter 11, Theorem 3). Um estudo profundo dos grupos de ramificação, feito sob certas hipóteses adicionais, encontra-se em Serre [32], Chapitre IV.

EXERCÍCIOS

- 21.1. Prove que K^T (respectivamente K_1^V) é o maior corpo K' entre K e L tal que $e(p'|K) = 1$ (respectivamente $\text{MDC}(p, e(p'|K)) = 1$), sendo $p' = \mathfrak{P} \cap R'$, $R' = S \cap K'$ e p o expoente característico de $\mathcal{L}$.
- 21.2. Dado um corpo quadrático (respectivamente ciclotômico) L , caracterize os números primos p tais que
- $K^Z(\mathfrak{P}|K) = K$ e $K^T(\mathfrak{P}|K) = L$;
 - $K^T(\mathfrak{P}|K) = K$ e $K_1^V(\mathfrak{P}|K) = L$;
 - $K_1^V(\mathfrak{P}|K) = K$;
- sendo $\mathfrak{P}$ um ideal primo de I_L , acima de $p \cdot \mathbb{Z}$.

- 21.3. Sejam $L|\mathbb{Q}$ uma extensão finita normal, p um número primo que não divida $[L:\mathbb{Q}]$ e $\mathfrak{P}$ um ideal primo de I_L acima de $p \cdot \mathbb{Z}$. Prove que $e(\mathfrak{P}|\mathbb{Q})$ divide $p^f - 1$, onde $f = f(\mathfrak{P}|\mathbb{Q})$.
- 21.4. Seja Φ o isomorfismo de $\text{Aut}(K^T|K^Z)$ sobre $\mathcal{G}$, definido em (21.4 b), e seja $\mathfrak{R}^{ZT}$ o conjunto dos corpos que estão entre K^Z e K^T . Prove que:
- Associando-se a cada $K' \in \mathfrak{R}^{ZT}$ o corpo $\mathcal{K}' = R'/\mathfrak{p}'$, onde $R' = S \cap K'$ e $\mathfrak{p}' = \mathfrak{P} \cap R'$, obtém-se uma bijeção de $\mathfrak{R}^{ZT}$ sobre o conjunto dos corpos que estão entre $\mathcal{K}$ e $\mathcal{L}$, tal que $\Phi(\text{Aut}(K^T|K')) = \text{Aut}(\mathcal{L}|\mathcal{K}')$.
 - No caso em que $\mathcal{K}$ é um corpo finito, a aplicação $K' \mapsto [K^T:K']$ é uma bijeção de $\mathfrak{R}^{ZT}$ sobre o conjunto dos divisores positivos de $f(\mathfrak{P}|K)$.
- 21.5. Seja ψ o isomorfismo de $\text{Aut}(K_1^V|K^T)$ sobre $W_2(\mathcal{L})$, indicado em (21.21 b), e seja $\mathfrak{R}^{TV}$ o conjunto dos corpos que estão entre K^T e K_1^V . Prove que: Associando-se a cada $K' \in \mathfrak{R}^{TV}$ o grau $e' = [K_1^V:K']$, obtém-se uma bijeção de $\mathfrak{R}^{TV}$ sobre o conjunto dos divisores positivos de e , tal que $\psi(\text{Aut}(K^T|K')) = W_2(\mathcal{L})$.
- 21.6. Generalize os resultados do §21 ao caso geral em que a extensão $\mathcal{L}|\mathcal{K}$ não é necessariamente separável. Prove, em particular, que $\mathcal{K}^T$ e $\mathcal{K}^V$ coincidem com o fecho separável de $\mathcal{K}$ em $\mathcal{L}$.
- 21.7. Sejam K um corpo de números algébricos, $L|K$ uma extensão finita normal, $\mathfrak{p}$ um ideal primo de I_K não-ramificado em L e $q = \mathfrak{N}\mathfrak{p}$. Prove que, para todo ideal primo $\mathfrak{P}$ de I_L acima de $\mathfrak{p}$:
- $G^Z(\mathfrak{P}|K)$ é um grupo cíclico, gerado pelo K -automorfismo ρ , univocamente determinado por $\rho\alpha = \alpha^q \in \mathfrak{P}$, para todo $\alpha \in I_L$. (Este é chamado o *automorfismo de Frobenius*, e é denotado por $(\mathfrak{P}, L|K)$.)
 - $(\sigma\mathfrak{P}, L|K) = \sigma \circ (\mathfrak{P}, L|K) \circ \sigma^{-1}$ para todo $\sigma \in \text{Aut}(L|K)$.
 - Se $K \subseteq K' \subseteq L$ então $(\mathfrak{P}, L|K') = (\mathfrak{P}, L|K)^{f'}$, sendo $f' = f(\mathfrak{P} \cap I_{K'}|K)$.
 - Se $K \subseteq L \subseteq L'$, sendo $L'|K$ normal, então

$$\theta^Z(\mathfrak{P}, L|K) = (\mathfrak{P} \cap I_{L'}, L'|K),$$

onde θ^Z é o homomorfismo indicado em (20.6). (Veja Samuel [30], §6.3).

EPÍLOGO

Como foi mencionado no prólogo, este livro tem como origem as notas de aula de um curso, de duração de um semestre, dado pelo autor em várias ocasiões. Isto explica a limitação deste livro, e o leitor deve ser advertido para o fato de que, através deste, aprendeu apenas uma ínfima parte da Teoria dos Números Algébricos, mesmo em relação ao estado de desenvolvimento da teoria até o início deste século, como se pode verificar facilmente consultando um dos livros clássicos de Hilbert [18], Hecke [16] ou Hasse [13]. Falta, em particular, a Teoria dos Corpos de Classes, que teve seu início no século passado e culminou na “Lei de Reciprocidade Geral” provada por Artin [2]. A história desta teoria, juntamente com uma ampla lista de referência, é apresentada em Hasse [14].

Foi mencionado também que, devido ao caráter introdutório deste livro, foi adotado o ponto de vista clássico, baseando a teoria na noção fundamental e intuitiva do anel dos números inteiros I_L de um corpo de números algébricos L . A alternativa, usada em alguns outros livros — como por exemplo, Hasse [15] e Weiss [37] — de partir da noção de valorização, tem a vantagem de conduzir diretamente ao poderoso “método local” que relaciona o corpo L com os seus completamentos, método este que se tem provado indispensável para se obter certos resultados mais profundos.

Vários resultados importantes da Teoria dos Números Algébricos não podem ser provados sem lançar mão do “método analítico”. Mencionemos neste contexto o teorema de Dirichlet sobre números primos numa progressão aritmética e a fórmula de números de classes h_L , ambos envolvendo a função zeta de Dedekind, definida como

$$\zeta_L(s) = \sum \frac{1}{(\mathfrak{N}\mathfrak{a})^s},$$

onde $\mathfrak{a}$ percorre os ideais de I_L , e convergente para $1 < s < \infty$. Uma excelente introdução a esse método (o qual está fora do âmbito deste livro) encontra-se em Borevich-Shafarevich [6].

Não podemos descrever neste contexto, nem em linhas gerais, o desenvolvimento mais recente da Teoria dos Números Algébricos. Uma certa visão deste desenvolvimento até 1965 pode ser obtida através do livro Cassels-Fröhlich [7]. Consultando esse livro, o leitor observará a importância que o "método cohomológico" tem para a Teoria dos Corpos de Classes, bem como para a solução (negativa) do problema da finitude de torres de corpos de classes, mencionado no §10.

REFERÊNCIAS

- [1] Apostol, T.M.: Introduction to analytic number theory. Springer-Verlag 1976.
- [2] Artin, E.: Beweis des allgemeinen Reciprocitätsgesetzes. Abh. Math. Sem. Univ. Hamburg 5 (1927), 353-363.
- [3] Atiyah, M.F., and Macdonald, I.G.: Introduction to commutative algebra. Addison-Wesley 1969.
- [4] Baker, A.: Transcendental number theory. Cambridge University Press 1975.
- [5] Barnes, E.S., and Swinnerton-Dyer, H.P.F.: The inhomogeneous minima of binary quadratic forms (I). Acta Mathematica 87 (1952), 259-323.
- [6] Borevich, Z.I., and Shafarevich, I.R.: Number theory. Academic Press 1966 (Tradução do original russo).
- [7] Cassels, J.W.S., and Fröhlich, A. (editors): Algebraic number theory. Thompson Book Co., Washington 1967.
- [8] Endler, O.: Valuation theory. Universitext. Springer-Verlag 1972.
- [9] Gilmer, R.: Multiplicative ideal theory. Marcel Dekker 1972.
- [10] Gonçalves, A.: Introdução à Álgebra. (Projeto Euclides) IMPA 1979.
- [11] Greub, W.H.: Linear Algebra. 2nd edition. Springer-Verlag 1963.
- [12] Hardy, G.H., and Wright, E.M.: An introduction to the theory of numbers. Oxford University Press 1954.
- [13] Hasse, H.: Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Jber. dt. MatVerein. 35 (1926), 1-55; 36 (1927), 233-311.
- [14] Hasse, H.: History of class field theory. Em [7], 266-279.
- [15] Hasse, H.: Number theory. Springer-Verlag 1980 (Tradução do original alemão: Zahlentheorie, Akademie-Verlag 1949).
- [16] Hecke, E.: Lectures on the theory of numbers. Springer-Verlag 1981 (Tradução do original alemão: Vorlesungen über die Theorie der algebraischen Zahlen. Akadem. Verlagsgesellschaft Leipzig, 1923).

- [17] Hensel, K.: *Theorie der algebraischen Zahlen*. Teubner, Leipzig 1908.
- [18] Hilbert, D.: Die Theorie der algebraischen Zahlkörper. *Jber. dt. Mat.Verein.* 4 (1894), 175-546.
- [19] Jacobson, N.: *Basic Algebra I*. Freeman & Co., San Francisco 1974.
- [20] Lang, S.: *Algebra*. Addison Wesley 1965.
- [21] Lang, S.: *Algebraic Numbers*. Addison-Wesley 1964.
- [22] Larsen, M.D., and McCarthy, P.J.: *Multiplicative theory of ideals*. Academic Press 1971.
- [23] Lehmer, E.: On the magnitude of the coefficients of the cyclotomic polynomial. *Bulletin Amer. Math. Soc.* 42 (1936), 389-392.
- [24] LeVeque, D.J.: *Topics in number theory. I*. Addison Wesley 1956.
- [25] Lima, E.L.: *Curso de Análise. Vol. 2 (Projeto Euclides)* IMPA 1981.
- [26] Marcus, D.A.: *Number fields*. Springer-Verlag 1977.
- [27] Ribenboim, P.: *Tópicos de Teoria dos Números. Notas de Matemática*: IMPA 1966.
- [28] Ribenboim, P.: *Algebraic numbers*. Wiley-Interscience 1972.
- [29] Roquette, P.: On class field towers. Em [7], 231-249.
- [30] Samuel, P.: *Algebraic theory of numbers*. Kershaw Publ. Co. 1972 (Tradução do original francês: *Théorie algébrique des nombres*. Hermann, Paris 1967).
- [31] Scharlau, W., und Opolka, H.: *From Fermat to Minkowski*. Springer-Verlag 1984. (Tradução do original alemão: *Von Fermat bis Minkowski*. Springer-Verlag 1980).
- [32] Serre, J.P.: *Corps locaux*. Hermann, Paris 1962.
- [33] Stewart, I.N., and Tall, D.O.: *Algebraic number theory*. Chapman and Hall, London 1979.
- [34] van der Waerden, B.L.: *Modern algebra I*. Revised English edition. Frederick Ungar Publ. Co., New York 1953. (Tradução do original alemão: *Moderne Algebra*, Springer-Verlag 1936).
- [35] Viswanathan, T.M.: *Introdução à Álgebra e Aritmética*. Monografias de Matemática, IMPA 1979.
- [36] Voloch, J.F.: *A Lei de Reciprocidade Generalizada*. Dissertação de Mestrado, IMPA 1982.
- [37] Weiss, E.: *Algebraic number theory*. McGraw-Hill 1963.
- [38] Zariski, O., and Samuel P.: *Commutative algebra. I*. Van Nostrand 1958.

ÍNDICE DE NOTAÇÕES

$p_{\alpha, K}$	2	κ_p	118
$P_{\alpha K}, \partial$	2	$\left(\frac{c}{p}\right)$	127
$\text{disc}(F)$	3	$\left(\frac{c}{m}\right)$	129
$F_{\alpha, L K}, \mathcal{F}_{L K}, \mathcal{N}_{L K}$	4		
$\text{Aut}(N K), U(R), K^*$	5		
$Q(R), R_M, R/a$	6		
MDC, MMC	7	χ_L	138
M/N	8	ψ_L	140
$I_S(R)$	11	$\mathbb{I}_1, \ x\ , B_\rho, T_z$	145
I_L	12	vol	148
$W(L)$	17, 30	$\sigma_1, \dots, \sigma_s; \sigma_{s+1}, \bar{\sigma}_{s+1}, \dots, \sigma_{s+t}, \bar{\sigma}_{s+t}$	151
$\mathcal{O}$	19	$L^{s,t}; e_1, \dots, e_{s+t}; f_j, g_j$	152
$o(\alpha), W_n(K), \mathcal{O}_n(K)$	29	χ	153
$\varphi(n)$	31	$\mathcal{N}(\xi_1, \dots, \xi_s; \omega_1, \dots, \omega_t)$	154
Φ_n	32	$\mu; \mu_j; \lambda; \lambda_j; \emptyset$	156
$\text{disc}_{L K}(\alpha_1, \dots, \alpha_n)$	39	$e_1, \dots, e_{s+t-1}$	160
$\mathfrak{D}_{S R}$	43	$I_d; J_d; S_{d,n}; \mathcal{S}_d$	162
d_L	44	$U_e(S)$	163
k_σ	52	$V(S)$	164
$\sqrt{a}$	56	$V_e(S)$	165
$r \equiv s \pmod{a}$	57	$e_{d,n}$	166
CRT(n)	60	$\mathfrak{k}; \mathfrak{N}_k; \mathfrak{U}_k; \mathfrak{U}_{e,k}$	168
$(R:M)$	70	$e_k; \mathbb{I}_k(c)$	169
$\mathcal{M}, \mathcal{F}$	71	$G (= \text{Aut}(L K))$	173
$\mathcal{G}, \mathcal{H}, \mathcal{P}, \mathcal{J}$	72	$\sigma_S; e, e(\mathbb{P} K); f, f(\mathbb{P} K); r, r(\mathbb{P} K)$	174
$M N$	75	$\mathcal{X}, \mathcal{L}; G^Z(\mathbb{P} K), G^Z$	175
$\mathcal{E}\ell$	78	$\theta; \theta^Z$	176
h_R	79	$K^Z(\mathbb{P} K), K^Z; R^Z, p^Z, \mathcal{K}^Z$	177
$\mathfrak{H}_a$	84	$\mathcal{G}; G^T(\mathbb{P} K), G^T; \Phi$	179
h_L	88	$\mathcal{K}; K^T(\mathbb{P} K), K^T$	180
$n(a), m(\mathbb{P})$	89	$R^T, p^T, \mathcal{K}^T$	181
μ_L	91	$\theta^T; G^T(\mathbb{P} K), G^T$	182
e, p	96	U_i	184
$f(\mathbb{P} p), e(\mathbb{P} p)$	104	ψ_i	185
$\mathfrak{D}_{S R}, \mathfrak{D}_{S R}$	112	K_i^T	187
$e(\mathbb{P}), f(\mathbb{P}), \zeta_m, L_m, \Phi_m, I_m$	117	$e = p' \cdot \bar{e}; R^V, p^V$	188

ÍNDICE ALFABÉTICO

- A
 acima de (ideal primo), 100
 anel, 5
 artiniano, 68
 de frações, 6
 de valorização, 80
 dos inteiros algébricos, 12
 dos inteiros de Gauss, 23
 não trivial, 5
 noetheriano, 62
 quociente, 6
 anulado por (módulo), 82
 ARTIN, E., 141, 191
 artiniano, anel, 68
 automorfismo de Frobenius, 190
- B
 BARNES, E. S., 23
 base
 dual, 42
 de rede, 145
 de um módulo, 8
 integral, 15, 47
 bola, 144
- C
 carácter quadrático, 140
 CASSELS, J. W. S., 192
 C.C.A., C.C.D., 62, 68
 classes
 de ideais, 78
 primos mod n , 31
 condição
 de cadeia ascendente, 62
 de cadeia descendente, 68
 maximal, 62
 minimal, 68
 conjectura de Gauss, 23
 convexo (subconjunto de $\mathbb{L}$), 149
 corpo
 algebricamente fechado, 2
 ciclôtmico, 28, 33
 cúbico, 74, 209
 das raízes (de um polinômio), 4
 de decomposição, 177
 de classes de Hilbert, 92
 de frações, 6
 de inércia, 180
 de números algébricos, 9
 de quocientes, 6
 de ramificação, 187
 de restos, 83
 dos números de Gauss, 23
 fixo, 5
 perfeito, 3
 quadrático, 19
 quadrático imaginário, 23
 quadrático real, 23
 cota de Minkowski, 82, 91, 144
 critério de Eisenstein, 34, 112
 critério de Euler, 127
 critério de Gauss, 135
- D
 decomposição (de um ideal primo), 102
 decomposição primária, 69
 DEDEKIND, R., 55
 domínio de, 69
 função zeta de, 82, 191
 diferente, 112
 DIRICHLET, G. P. L.
 teorema de invertíveis de, 25, 159
 teorema sobre progressões aritméticas de, 120
 discriminante
 de um polinômio, 3
 de uma n -upla, 39
 de um corpo de números algébricos, 44
 discreto (subconjunto de $\mathbb{L}$), 145
 divisor não essencial de discriminante, 53
 domínio, 5
 de Dedekind, 69
 euclidiano, 22
 fatorial, 7
 principal, 7

- E EISENSTEIN, A.**
 critério de, 34, 112
 polinômio de, 113
 elemento
 algébrico sobre, 2
 inteiro sobre, 9
 invertível, 5
 irredutível, 7
 primo, 7
 separável sobre, 3
 transcedente sobre, 2
 equação de Pell, 144, 168
EULER, L.
 critério de, 127
 função de, 31
 euclidiano, domínio, 22
 expoente característico, 188
 extensão
 algébrica, 2
 de escalares, 47
 de ideais, 96
 finita, 1
 galoisiana, 4
 normal, 4
 separável, 3
- F fecho**
 algébrico (de um corpo), 2
 inteiro (de um anel), 11
FERMAT, P. de, 26
 Último Teorema de, 36
 fórmulas complementares, 134
FROBENIUS, F. G.,
 automorfismo de, 190
FRÖHLICH, A., 192
 função de Euler, 31
 função zeta de Dedekind, 82, 191
- G GALOIS, É.**
 grupo de, 5
 teorema fundamental de, 5
GAUSS, C. F., 135
 anel dos inteiros de, 23
 conjetura de, 23
 corpo dos números de, 23
 critério de, 135
 soma de, 143
GOLOD, E. S., 93
 grau de inércia, 84, 104
 grupo
 de decomposição, 175
 de Galois, 5
 de inércia, 179
 de ramificação, 182
- H HASSE, H.**, 191
HECKE, E., 191
HERMITE, C., 92
HILBERT, D., 191
 corpo de classes de, 92
 teorema de base de, 69
 homomorfismo canônico, 6
- I ideais comaximais**, 57
 ideal, 6
 discriminante, 43
 estendido, 96
 fracionário, 70
 fracionário invertível, 71
 fracionário principal, 72
 irredutível, 69
 maximal, 6
 primo, 6
 acima de, 100
 ramificado, 110
 totalmente decomposto, 106
 totalmente inerte, 106
 totalmente ramificado, 106
 principal, 6
 que se perde (num anel de frações), 97
 restrito, 96
 igualdade fundamental, 82, 104
 imersão (de um corpo de números algébricos)
 canônica, 153
 complexa, 151
 real, 151
 índice (de um inteiro algébrico), 52
 índice de ramificação, 104
 inteiro algébrico, 9
 inteiro sobre R , 9, 11
 integralmente fechado, 11, 14
 invertível fundamental, 25, 164
- J JACOBI, K. G. J.**
 símbolo de, 129
- K KRULL, W.**
 teorema de interseção de, 69
KUMMER, E. E., 36, 55, 117
 teorema de, 108
- L LEGENDRE, A.-M.**
 símbolo de, 127
 lei,
 de decomposição, 117, 140
 de reciprocidade generalizada, 141
 de reciprocidade quadrática, 132
 limitado (subconjunto de $\mathbb{L}$), 145
 localização, 6

- M malha (de uma rede), 146
 fundamental, 145
 método
 analítico, 82, 191
 cohomológico, 192
 geométrico, 82, 91, 144
 local, 191
 MINKOWSKI, H., 92
 cota de, 82, 91, 144
 teorema de, 149
 módulo, 7
 finitamente gerado, 8
 invertível, 71
 livre, 8
 noetheriano, 62
 quociente, 8
- N não-resto quadrático, 123
 NOETHER, E., 55
 noetheriano (anel, módulo), 62
 norma, 4
 absoluta, 22
 de ideais, 84
 em $\mathbb{Z}^n$, 154
 número
 algébrico, 9
 de classes, 79, 88
 inteiro livre de quadrados, 19
 primo decomposto, 26
 primo inerte, 26
 primo ramificado, 27
- O operação de fecho, 12
 "ordem" (de um corpo de números
 algébricos), 52
 maximal, 52
- P PELL, J.
 equação de, 144, 162
 p-grupo elementar, 186
 polinômio
 característico, 4
 ciclotômico, 33
 de Eisenstein, 113
 minimal, 2
 separável, 3
 posto (de um módulo), 47
 produto cartesiano (de R-módulos), 8
 p-subgrupo de Sylow, 186
- R radical, 56
 raiz da unidade, 17
 raiz n-ésima da unidade, 29
 primitiva, 29
 ramificação selvagem, 188
 ramificação mansa, 188
 rede, 145
 completa, 145
 representação logarítmica, 156
 resto quadrático, 123
 restrição de ideais, 96
 ROQUETTE, P., 93
- S SCHUR, I., 33
 semi-sistema mod m , 128
 natural, 130
 SHAFAREVICH, I. R., 93
 símbolo de Jacobi, 129
 símbolo de Legendre, 127
 simétrico (subconjunto de L), 149
 sistema de invertíveis
 fundamentais, 160
 soma de dois quadrados, 25
 solúvel por radicais, 189
 soma de Gauss, 143
 submódulo, 8
 SWINNERTON-DYER,
 H. P. F., 23
 SYLOW, L.
 p-subgrupo de, 186
- T teorema
 chinês de restos, 60
 de base de Hilbert, 69
 de Dirichlet sobre progressões
 aritméticas, 120
 de interseção de Krull, 69
 de invertíveis de
 Dirichlet, 25, 159
 de Kummer, 108
 de Minkowski (sobre pontos de
 rede), 149
 fundamental de Galois, 5
 going up, 101
 lying over, 101
 traço, 4
- U Último Teorema de Fermat, 36
 unit theorem, 144
- V valorização discreta, 81
 volume em L , 148
- W WEISS, E., 191

Esta obra foi produzida nas
oficinas da Imos Gráfica e Editora na
cidade do Rio de Janeiro