Leis de Reciprocidade

Rodrigo Francisco Lopes

28 de março de 2006

LEIS DE RECIPROCIDADE

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Rodrigo Francisco Lopes e aprovada pela comissão julgadora.

Campinas, 23 de Fevereiro de 2004.

Prof.Dr: Paulo Roberto Brumatti.

Orientador

Banca examinadora
1. Prof. Dr. Paulo Roberto Brumatti
2. Prof. Dr. Antônio José Engler
3. Prof. Dr. Trajano Pires da N. Neto

Dissertação apresentada ao instituto de Matemática, Estatística e Computação Científica da UNICAMP, como requisito parcial para obtenção do título de MESTRE em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues – CRB8a / 2116

Lopes, Rodrigo Francisco
L881r Leis de reciprocidade / Rodrigo Francisco Lopes -- Campinas, [S.P. :s.n.], 2006.

Orientador : Paulo Roberto Brumatti
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos números. 2. Teoremas de reciprocidade. Somas gaussianas I. Brumatti, Paulo Roberto. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Reciprocity laws

Palavras-chave em inglês (Keywords): 1. Number theory. 2. Reciprocity theorems. 3. Gaussian sums.

Área de concentração: Álgebra

Titulação: Mestre em Matemática

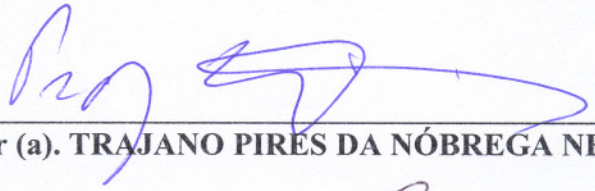
Banca examinadora: Prof. Dr. Paulo Roberto Brumatti (IMECC-UNICAMP)
Prof. Dr. Antonio José Engler (IMECC-UNICAMP)
Prof. Dr. Trajano Pires da Nóbrega Neto (IBILCE)

Data da defesa: 23/02/2006

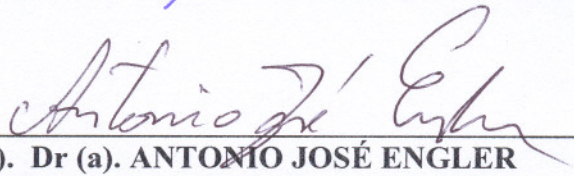
Dissertação de Mestrado defendida em 23 de fevereiro de 2006 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). PAULO ROBERTO BRUMATTI



Prof. (a). Dr (a). TRAJANO PIRES DA NÓBREGA NETO



Prof. (a). Dr (a). ANTONIO JOSÉ ENGLER

Agradecimentos

Ao meu orientador Paulo Roberto Brumatti, pela paciência e orientação.

À minha mãe, por todo carinho, compreensão e superação.

À minha avó, pelos cuidados e pelo amor.

Ao meu falecido pai, o qual eu guardo a certeza de ter sido um grande homem.

Aos meu falecidos avós, aos quais eu guardo as melhores lembranças.

Aos meus grandes amigos e à todos aqueles que fazem nossa passagem pela vida algo prazeroso.

Meus sinceros agradecimentos.

Rodrigo

Sumário

Introdução

Nesta monografia temos o objetivo de estudar as leis de reciprocidade de graus 2, 3 e 4 (capítulo 5), bem como leis de reciprocidade racionais de graus 3 e 4 (capítulo 6) devidas à von Lienen [7] e Burde [1]. Para tal, daremos uma sucinta introdução da Teoria dos Números Algébricos e da Teoria dos Corpos Ciclotômicos no capítulo 2 seções 2.1 e 2.2 e, de tal forma, estaremos em condições no capítulo 3 de definirmos o símbolo de resíduos m-ésimos, o qual será fundamental para nosso trabalho. Poderíamos ter optado por um caminho diferente que envolveria menos teoria, qual seja, o de definir apenas os símbolos de resíduos de graus 2, 3 e 4, em vez de nos preocuparmos com o caso geral. Isto seria razoável, visto que os únicos casos particulares que estudaremos são estes, mas para deduzirmos as leis de reciprocidade racionais acima citadas usaremos um teorema devido à Charles Helou [4] que nos permite, dada uma lei de reciprocidade em $\mathbb{Z}[\zeta_m]$, ζ_m uma raíz m-ésima primitiva da unidade, m um inteiro positivo qualquer, obtermos uma lei de reciprocidade racional m-ésima. Se optássemos pelo caminho mais simples perderíamos a generalidade deste elegante teorema.

Para demonstrarmos as leis de reciprocidade de graus 2, 3 e 4 usaremos as somas de Gauss e as somas de Jacobi, cujas propriedades fundamentais serão demonstradas no capítulo 4. Iniciamos esta monografia com uma breve introdução histórica.

Capítulo 1

Breve introdução histórica

Dos registros que temos da Teoria dos Números na antiguidade se destacam os Elementos de Euclides, que datam por volta de 300 a.C., e a Aritmética de Diophanto, que data por volta de 200 d.C(de 13 livros que constituem o Aritmética apenas 6 chegaram aos nossos dias). Então até o século dezessete a Teoria dos Números - bem como a maioria das áreas do conhecimento - ficaram praticamente estacionadas. Com a chegada do Iluminismo uma reimpressão do livro de Diophanto chega às mãos do matemático amador Pierre de Fermat. O título de amador se deve unicamente a Fermat ser juiz de profissão e não devido à qualidade do seu trabalho; de fato, muito da Teoria dos Números que se faz hoje em dia é inspirada nas anotações que Fermat deixou nas margens de sua cópia de Diophanto e que foram publicadas posteriormente por seu filho. Além disso, Newton se inspirou nos trabalhos de Fermat para criar o Cálculo Diferencial e Integral.

Em [8] A. Weil diz que aqueles eram tempos confortáveis para um teórico dos números devido à pouca competição que eles enfrentavam. O que não era o caso do Cálculo Diferencial e Integral; com efeito, já naquela época houveram disputas entre Fermat e Descartes nesta área. No que diz respeito à Teoria dos Números, Fermat esteve praticamente isolado durante todo o século dezessete e o mesmo aconteceu com Euler em grande parte do século seguinte, até que Lagrange se juntou à ele. Mais tarde no século dezoito apareceu Legendre e já no século dezenove apareceu Gauss. O lado bom desse isolamento - continua Weil - é que o matemático podia se dedicar a problemas profundos sem se preocupar que outro matemático chegasse aos resultados antes dele. Por outro lado, Fermat e Euler chegaram a reclamar de falta de companhia neste campo. Talvez seja por isso que Fermat não deixou muitos registros de seus métodos e das demonstrações de suas afirmações, deixando assim para que Euler e outros o fizessem.

Euler ficou fascinado com afirmações que Fermat fizera para um primo ímpar p tais como:

$$\begin{array}{lll} p = x^2 + y^2, & x,\ y \in \mathbb{Z} & \Leftrightarrow \quad p \equiv 1 \pmod 4 \\ p = x^2 + 2y^2, & x,\ y \in \mathbb{Z} & \Leftrightarrow \quad p \equiv 1, 3 \pmod 8 \\ p = x^2 + 3y^2, & x,\ y \in \mathbb{Z} & \Leftrightarrow \quad p = 3 \textit{ ou } p \equiv 1 \pmod 3 \end{array}$$

No entanto, Fermat deixou a maioria de seus resultados sem demonstração. A busca de Euler pelas demonstrações pode ser acompanhada em sua correspondência com Goldbach. Goldbach era um matemático amador muito interessado em Teoria dos Números, mas talvez suas maiores contribuições foram a de ser correspondente de Euler, e, claro, a conjectura que leva seu nome, a saber que todo número par é a soma de dois números primos. Como correspondente, Goldbach foi uma grande motivação para Euler. Como Euler pode comunicar a alguém suas descobertas, assim como suas dificuldades, não ficou tão isolado quanto Fermat.

A investigação das equações acima levaram Euler naturalmente ao estudo dos números que são congruentes à um quadrado módulo um primo p (os resíduos quadráticos mod p) da seguinte maneira: se p é da forma $x^2 \pm Ny^2$, x, y, $N \in \mathbb{Z}$ então p, para algum par de inteiros x_0, y_0, deve dividir $x_0^2 \pm Ny_0^2$, onde x_0 e y_0 não são divisíveis por p. O que é equivalente à $\pm N \equiv (x_0/y_0)^2 \pmod p$.

Para um dado primo p o problema de decidir quais são seus resíduos quadráticos é de fácil tratamento (basta testar todos os resíduos). Mas o problema mais interessante é decidir para quais primos seria um dado N um resíduo quadrático. Este problema levou Euler a descoberta da Lei de Reciprocidade Quadrática (Para detalhes da sequência de raciocínios que levaram Euler de um problema à outro até à referida lei ver [3]).

A Lei de Reciprocidade Quadrática - por brevidade denotaremos LRQ - diz que para primos ímpares distintos p e q vale

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}.$$

Onde $\left(\frac{\cdot}{\cdot}\right)$ é o símbolo de Legendre (definição 3.2.3).

Euler não chegou a demonstrar a LRQ. Legendre, que a descobriu independentemente de Euler, deu uma demonstração incompleta e Gauss, que também a descobriu sozinho (com apenas dezessete anos), depois de mais de um ano tentando demonstrá-la, obteve sucesso.

Ao longo da vida Gauss daria outras cinco demonstrações. A motivação para a busca de outras demonstrações foi que logo que demonstrou a LRQ Gauss começou a encontrar evidências de Leis de reciprocidade para resíduos

de potências de graus mais altos. Contudo, seus primeiros esforços para demonstrá-las não foram bem sucedidos e isso o motivou a encontrar uma demonstração da LRQ cujos métodos elucidassem algum argumento para os graus mais elevados. Em sua sexta demonstração, que data de 1817, Gauss alcançou seus objetivos e logo seriam publicadas seus dois ensaios sobre resíduos biquadráticos.

Em seu primeiro ensaio, que data de 1828, Gauss desenvolveu os teoremas elementares da teoria e deu um critério para determinar o caracter biquadrático do número 2. Já em seu segundo ensaio, 1832, ele desenvolveu a teoria dos inteiros gaussianos, os quais seriam necessários para formular e para demonstrar o problema, e enunciou a Lei de Reciprocidade Biquadrática, mas deixou a demonstração para um terceiro ensaio (Para um breve apanhado histórico do surgimento das leis de reciprocidade cúbica e biquadrática ver [2]).

Gauss não chegou a publicar seu terceiro ensaio, provavelmente desencorajado pela curta demonstração que Jacobi o enviou da lei de reciprocidade biquadrática.

Em 1844, com 21 anos, Eisenstein publicou 25 artigos, entre eles estão as primeiras demonstrações das Leis de Reciprocidade Cúbica e Biquadrática que foram publicadas. Quanto à Lei de Reciprocidade Cúbica houve uma amarga disputa pela prioridade na demonstração entre Jacobi e Ensenstein. Em um artigo de 1846 Jacobi acusou Eisenstein de plágio alegando que já havia demonstrado a Lei de Reciprocidade cúbica em suas aulas de 1837.

Kummer considerou o problema de formular uma lei de reciprocidade de grau um primo k e desenvolveu a teoria dos corpos ciclotômicos para demonstrar uma lei de reciprocidade em tais corpos. Hilbert generalizou as leis de reciprocidade para corpos de números algébricos quaisquer e em seu nono problema Hilbert perguntou qual seria a lei de reciprocidade mais geral em um corpo de números algébricos.

A melhor resposta que temos para o nono problema de Hilbert hoje em dia é a Lei de Reciprocidade de Artin, que, apesar de conter as leis de reciprocidade cúbica e biquadrática como casos particulares, em pouco as lembra.

O problema de que forma uma lei de reciprocidade deve ter é abordado em [9] onde Wyman faz o seguinte comentário

> "Finally, I have to confess that I still do not know what a reciprocity law is, or what one should be. The reciprocity problem, like so many other number theory problems, can be stated in a very simple and concrete way. However, the simply stated problems are often the hardest, and a complete solution seems to be the far out of reach. In fact, we probably will not know what we

are looking for until we found it."

Acontece que na década de 70 foram desenvolvidas leis de reciprocidade racionais para resíduos de potências de graus mais altos que são mais facilmente reconhecidas como generalizações da lei de reciprocidade quadrática. Como por exemplo a lei de reciprocidade de Burde que diz que se p e q são primos tais que $p = a^2+b^2$ e $q = A^2+B^2$ com $a \equiv A \equiv 1 \pmod 4$ e $\left(\frac{p}{q}\right) = 1$, então

$$\left(\frac{p}{q}\right)_4 \cdot \left(\frac{q}{p}\right)_4 = (-1)^{\frac{(q-1)}{4}} \left(\frac{aB - bA}{q}\right)_4,$$

onde $\left(\ \right)_4$ é o símbolo de resíduos biquadráticos(definição 3.2.3).

Em [6], Lehmer expõe o que havia sido feito neste assunto até então e como resposta a questão levantada por Wyman [9] diz que seu artigo é para aqueles teóricos dos números que...

> "...believe that they know what a reciprocity law is and not only know what they are looking for but have actually been discovering new rational reciprocity laws..."

Atualmente, muitos pesquisadores têm contribuído para o surgimento de novas leis de reciprocidade racionais. Citamos em particular [4] onde o autor contribui com métodos para que dada uma lei de reciprocidade geral, uma racional seja obtida.

Finalizamos esta nota com as palavras de Weil [8]:

> "Number theory is not standing still."

Capítulo 2

Preliminares

Neste capítulo desenvolveremos os aspectos básicos da teoria dos números algébricos e da teoria dos corpos ciclôtomicos. Nosso objetivo central é desenvolver a teoria necessária para estudarmos o símbolo de resíduos m - ésimos e algumas leis de reciprocidade. Como todos os resultados podem ser encontrados em livros introdutórios da área, como [5], omitiremos as demonstrações.

2.1 Teoria dos números algébricos

Seja L/K uma extensão finita de corpos. A dimensão de L/K, $[L : K]$, será denotada por n.

Suponha que $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de L/K e $\alpha \in L$. Então $\alpha\alpha_i = \sum_j a_{ij}\alpha_j$, com $a_{ij} \in K$.

Definição 2.1.1 *A* **norma** *de α, $N_{L/K}(\alpha)$, é o determinante da matriz (a_{ij}). O* **traço** *de α, $T_{L/K}(\alpha)$, é $a_{11} + \cdots + a_{nn}$.*

Sabemos que a definição acima independe da escolha da base e sempre que o contexto permitir usaremos a notação $N(\alpha) = N_{L/K}(\alpha)$.

Os principais resultados sobre traços e normas são enunciados nas duas proposições que seguem.

Proposição 2.1.2 *Se $\alpha, \beta \in L$ e $a \in K$ então*

(a) $N(\alpha\beta) = N(\alpha)N(\beta)$.

(b) $N(a\alpha) = a^n N(\alpha)$.

(c) $T(\alpha + \beta) = T(\alpha) + T(\beta)$.

(d) $T(a\alpha) = aT(\alpha)$.

(e) *Se* $\alpha \neq 0$, *então* $N(\alpha^{-1}) = N(\alpha)^{-1}$.

(f) *Se L/K é separável, então T não é identicamente nulo.*

Sejam L/K separável e $\sigma_1, \ldots, \sigma_n$ os monomorfismos distintos de L sobre um fecho algébrico de K que deixam K fixo. Para $\alpha \in L$ denotaremos $\sigma_j(\alpha)$ por $\alpha^{(j)}$. Os elementos $\alpha^{(j)}$ são chamados de conjugados de α e $\alpha^{(1)} = \alpha$.

Proposição 2.1.3 *Se $\alpha \in L$, então $T(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)}$ e $N(\alpha) = \alpha^{(1)} \cdots \alpha^{(n)}$.*

Definição 2.1.4 *Se $\alpha_1, \ldots, \alpha_n$ é uma n-upla de elementos de L então o* **discriminante** *$D(\alpha_1, \ldots, \alpha_n)$ é definido por $D(\alpha_1, \ldots, \alpha_n) = det(T(\alpha_i\alpha_j))$.*

Temos os seguintes resultados acerca do cálculo de determinantes.

Proposição 2.1.5 *Suponha que $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_n$ são bases de L/K. Seja $\alpha_i = \sum_j a_{ij}\beta_j, a_{ij} \in K$. Então $D(\alpha_1, \ldots, \alpha_n) = det(a_{ij})^2 D(\beta_1, \ldots, \beta_n)$.*

Proposição 2.1.6 *Para $\alpha_1, \ldots, \alpha_n \in L$ e L/K separável temos*

$$D(\alpha_1, \ldots, \alpha_n) = det(\alpha_i^{(j)})^2.$$

Definição 2.1.7 *Um subcorpo F do corpo dos números complexos $\mathbb{C}$ é chamado* **corpo de número algébricos** *se $[F : \mathbb{Q}]$ é finito. Se F é um corpo de números algébricos, o subconjunto de F formado pelos inteiros algébricos de F é um anel D chamado de* **anel de inteiros algébricos de** *F.*

Proposição 2.1.8 *Seja Ω o conjunto de todos inteiros algébricos de $\mathbb{C}$. Então Ω é um anel.*

Temos o importante e útil resultado sobre o anel de congruência D/I, onde I é um ideal qualquer de D e D é o anel de inteiros de um corpo de números algébricos F.

Proposição 2.1.9 *Para qualquer ideal I não nulo, D/I é finito.*

Da proposição acima e do fato que todo domínio de integridade finito é corpo segue o seguinte corolário.

Corolário 2.1.10 *Todo ideal primo não nulo de D é maximal.*

Observamos que em geral D não é um domínio de fatoração única. Entretanto, D tem uma propriedade que é quase tão boa, a saber que todo ideal não nulo pode ser escrito de maneira única como produto finito de ideais primos. O que nos motiva a seguinte definição.

Definição 2.1.11 *Seja A um domínio de integridade. Se todo ideal não nulo de A pode ser escrito de maneira única como produto finito de ideais primos então dizemos que A é um* **domínio de Dedekind**.

Muitos anéis importantes são domínios de Dedekind.

Proposição 2.1.12 *D é um domínio de Dedekind.*

Seja P um ideal primo não nulo de D. Observamos que $P \cap \mathbb{Z}$ é não nulo. De fato, para $\alpha \in P$, tome $a_0, \ldots, a_{m-1} \in \mathbb{Z}$ tais que $a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} + \alpha^m = 0$, onde $a_i \in \mathbb{Z}$ e $a_0 \neq 0$. Segue que $a_0 = -(a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} + \alpha^m) \in P \cap \mathbb{Z}$.

Como $P \cap \mathbb{Z}$ é não nulo e claramente é um ideal primo de $\mathbb{Z}$ segue que é gerado por um primo p. Vimos que (p) (agora visto como ideal em D) pode ser decomposto de maneira única como produto de ideais primos de D. Suponha $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$.

Proposição 2.1.13 *Na situação acima os P_is são exatamente os ideais de D tais que $P_i \cap \mathbb{Z} = p\mathbb{Z}$.*

Vemos que D/P_i é um corpo finito contendo $\mathbb{Z}/p\mathbb{Z}$. Portanto o número de elementos de D/P_i deve ser da forma p^{f_i}, $f_i \geq 1$.

Das considerações acima temos a seguinte definição.

Definição 2.1.14 *O número e_i é chamado* **índice de ramificação** *de P_i. O número f_i é chamado* **grau de inércia** *de P_i. Se existe i tal que $e_i > 1$, então dizemos que (p)* **se ramifica em** *D. Se $g = 1$ e $e_1 = 1$, então dizemos que (p)* **é inerte em** *D.*

Existe uma importante relação entre os números e_i, f_i e n, $i = 1, \ldots, g$.

Proposição 2.1.15 $\sum_{i=1}^{g} e_i f_i = n$.

O seguinte resultado será usado mais adiante.

Proposição 2.1.16 *Seja $P \subset D$ um ideal primo e seja p^f o número de elementos em D/P. Se $m \in \mathbb{N}^*$, então o número de elementos em D/P^m é p^{mf}.*

Suponha agora que $F/\mathbb{Q}$ é uma extensão galoisiana, isto é, que todos monomorfismos de F em $\mathbb{C}$ tem F como imagem. Suponha que G é o grupo de Galois de $F/\mathbb{Q}$. Se D é o anel de inteiros algébricos de F, I é um ideal qualquer de D e $\sigma \in G$, então $\sigma I = \{\sigma(\alpha); \alpha \in I\}$ também é um ideal. Temos também que $\sigma D = D$, e, portanto, $D/\sigma I = \sigma D/\sigma I \approx D/I$. Em particular vemos que se P é um ideal primo então σP também é um ideal primo. Nestas condições temos o seguinte resultado:

Proposição 2.1.17 *Seja $p \in \mathbb{Z}$ um número primo. Suponha que P_i e P_j sejam ideais primos de D contendo p. Então existe $\sigma \in G$ tal que $\sigma P_i = P_j$.*

Da proposição acima segue que dados P_i e P_j contendo p existe σ tal que $D/P_i \approx D/\sigma P_i \approx D/P_j$. Segue que $f_i = f_j$ e, portanto, todos f_i's são iguais.

Suponha $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. Suponha também que $\sigma \in G$ é tal que $\sigma P_1 = P_i$, aplicando σ nos dois lados da decomposição de (p) obtemos

$$(p) = (\sigma P_1)^{e_1} (\sigma P_2)^{e_2} \cdots (\sigma P_g)^{e_g}.$$

Vemos que e_1 é expoente de P_1 e de $\sigma P_1 = P_i$. Pela unicidade da decomposição em ideais primos temos que $e_1 = e_i$ e consequentemente todos e_i's são iguais. Formalizamos a discussão acima na seguinte proposição que é uma versão mais forte da proposição 2.1.15.

Proposição 2.1.18 *Suponha que $F/\mathbb{Q}$ é uma extensão galoisiana. Seja $p \in \mathbb{Z}$ um primo e suponha $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. Então $e_1 = e_2 = \ldots = e_g$ e $f_1 = f_2 = \ldots = f_g$. Se e e f denotam esses valores em comum, então $efg = n$.*

Se nas considerações da proposição acima temos $e = 1$ e $f = 1$, então $g = n$. Se tivermos $e = n$, então $f = g = 1$. Estas situações nos motivam a seguinte definição.

Definição 2.1.19 *No primeiro caso acima dizemos que (p)* **se decompõem completamente em** *D. No segundo caso dizemos que p* **se ramifica completamente**.

2.2 Corpos ciclotômicos

Sejam m um inteiro positivo e $\zeta_m = e^{(2i\pi)/m}$. O número complexo ζ_m é uma raíz primitiva m - ésima da unidade, isto é, ζ_m, bem como todas as suas potências, satisfazem a equação $x^m - 1 = 0$. Como para $a, a' \in \mathbb{Z}$, $a \equiv a' \pmod{m}$ temos que $\zeta_m^a = \zeta_m^{a'}$, observamos que $x^m - 1 = (x-1)(x-\zeta_m)\cdots(x-\zeta_m^{m-1})$. Sendo assim o corpo $\mathbb{Q}(\zeta_m)$ é corpo de raízes de $x^m - 1$ e, portanto, a extensão $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ é galoisiana.

Definição 2.2.1 *O polinômio $\Phi_m(x) = \prod_{(a,m)=1}(x - \zeta_m^a)$ é chamado o m -* **ésimo polinômio ciclotômico**.

As raízes de $\Phi_m(x)$ são precisamente as m - ésimas raízes primitivas da unidade.

Como $\Phi_m(x)$ é o produto de $\phi(m)$ fatores lineares (onde ϕ é função de Euler, $\phi(m)$ é igual ao número de inteiros entre 1 e m que são primos com m), observamos que o grau de $\Phi_m(x)$ é igual à $\phi(m)$.

Segue da definição que os coeficientes de $\Phi_m(x)$ são combinações lineares de raízes m - ésimas da unidade e portanto são inteiros algébricos. Se G é o grupo de Galois de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, então para $\sigma \in G$ qualquer segue que $\sigma\Phi_m(x) = \prod(x - \sigma(\zeta_m^a)) = \Phi_m(x)$. Portanto $\Phi_m(x) \in \mathbb{Z}[x]$.

A seguinte proposição relaciona polinômios ciclôtomicos com $x^m - 1$.

Proposição 2.2.2 $x^m - 1 = \prod_{d|m} \Phi_d(x)$.

De agora em diante usaremos a notação D_m para o anel de inteiros de $\mathbb{Q}(\zeta_m)$.

Proposição 2.2.3 *Suponha que p seja um primo racional e que $p \nmid m$. Seja P um ideal primo de D_m contendo p. Então as classes de $1, \zeta_m, \ldots, \zeta_m^{m-1}$ em D_m/P são todas distintas. Se f denota o grau de inércia de P então $p^f \equiv 1 \pmod{m}$.*

A seguir apresentamos uma importante proposição e suas importantes consequências.

Proposição 2.2.4 *O polinômio $\Phi_m(x)$ é irredutível em $\mathbb{Z}[x]$.*

Corolário 2.2.5 $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$.

Corolário 2.2.6 *Seja G o grupo de Galois de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Suponha que $\sigma \in G$ e que $\sigma\zeta_m = \zeta_m^{\theta(\sigma)}$. A aplicação $\theta : G \to U(\mathbb{Z}/m\mathbb{Z})$ definida por $\sigma \mapsto \theta(\sigma)$ é um isomorfismo.*

Daremos a seguir um resultado sobre a decomposição de primos que não dividem m.

Proposição 2.2.7 *Seja p um primo, $p \nmid m$. Seja f o menor inteiro positivo tal que $p^f \equiv 1 \pmod{m}$. Então em $D_m \subset \mathbb{Q}(\zeta_m)$ temos que*

$$(p) = P_1 P_2 \cdots P_g,$$

onde para todo i, P_i é primo, $P_i \neq P_j$ se $i \neq j$ e P_i tem grau de inércia f, para $i, j = 1, \ldots, g$. Além disso, $g = \phi(m)/f$.

Definimos para p primo tal que $p \nmid m$, o automorfismo σ_p de $\mathbb{Q}(\zeta_m)$ definido por $\sigma_p(\zeta_m) = \zeta_m^p$.

Usando a mesma notação da proposição acima temos o seguinte corolário.

Corolário 2.2.8 *Seja $P = P_i$. Considere o subgrupo de G dado por $G(P) = \{\sigma \in G; \sigma(P) = P\}$. Então $G(P)$ é um subgrupo cíclico gerado por σ_p.*

Quanto aos primos que dividem m apresentaremos os seguintes resultados.

Proposição 2.2.9 *Seja l um primo em $\mathbb{Z}$. Então, em $\mathbb{Q}(\zeta_l)$, l se ramifica completamente. Mais precisamente, seja $L = (1 - \zeta_l)$. Então L é um ideal primo e $(l) = L^{l-1}$. Portanto L tem grau de inércia* 1.

Proposição 2.2.10 *Sejam P um ideal primo de D_m e $P \cap \mathbb{Z} = p\mathbb{Z}$. Se p é ímpar, então P se ramifica se, e somente se, $p \mid m$. Se $p = 2$, então P se ramifica se, e somente se,* $4 \mid m$.

O anel D_m é caracterizado pela seguinte proposição.

Proposição 2.2.11 $D_m = \mathbb{Z}[\zeta_m]$.

Capítulo 3

O símbolo de resíduos m - ésimos

Neste capítulo, usando as propriedades dos corpos ciclôtomicos, vamos definir um dos objetos centrais desta dissertação, a saber, o símbolo de resíduos de potências m - ésimas, ou, simplesmente, símbolo de resíduos m - ésimos. Também vamos demonstrar suas principais propriedades.

3.1 A norma de um ideal

Precisaremos de alguns resultados adicionais da teoria de corpos de números algébricos.

Sejam $K/\mathbb{Q}$ um corpo de números algébricos, D o anel de inteiros de K, e I um ideal. Assumimos ao longo deste capítulo que os ideais são não nulos.

Definição 3.1.1 *Definimos a* **norma** *de I, $N(I)$, como sendo o número de elementos em D/I.*

Proposição 3.1.2 *Se I, $J \subset D$ são ideais, então $N(IJ) = N(I)N(J)$.*

Demonstração: Se I e J são primos entre si, então pelo teorema do resto chinês $D/IJ \approx D/I \oplus D/J$. Portanto, o resultado segue neste caso.

Seja $I = P_1^{a_1} P_2^{a_2} \cdots P_t^{a_t}$ a decomposição prima de I. Afirmamos que $N(I) = (N(P_1))^{a_1}(N(P_2))^{a_2} \cdots (N(P_t))^{a_t}$. Como P_i e P_j são primos entre si para $i \neq j$, pelo que vimos acima basta mostrarmos que $N(P^a) = (N(P))^a$

para um ideal primo P qualquer. Mas, isso segue diretamente da proposição 2.1.16.

Agora, para o caso geral basta decompormos I e J, multiplicarmos e usar a afirmação acima. Reorganizando os termos de forma conveniente concluímos a proposição.

■

Proposição 3.1.3 *Suponha que $K/\mathbb{Q}$ seja uma extensão galoisiana com grupo de Galois G. Então*

$$\prod_{\sigma \in G} \sigma(I) = (N(I)).$$

DEMONSTRAÇÃO: Como ambos os lados da expressão acima são multiplicativos em I, basta mostrarmos que o resultado é válido para um ideal primo P.

Sejam $P_1, P_2, \ldots, P_g$ os ideais primos distintos no conjunto $\{\sigma(P); \sigma \in G\}$. Considerando o subgrupo de G, $G(P) = \{\sigma \in G; \sigma(P) = P\}$, e observando que $G(P)$ tem g classes laterais, pelo teorema de lagrange segue que $|G| = g|G(P)|$.

Observamos que $P_1, P_2, \ldots, P_g$ são exatamente os ideais primos da decomposição de $(p) = P \cap \mathbb{Z}$ em D. Assim, pela proposição 2.1.18 temos que $efg = n = [K : \mathbb{Q}] = |G|$. O que implica que $|G(P)| = ef$.

Usando a proposição 2.1.17 e novamente a proposição 2.1.18 temos que

$$\prod_{\sigma \in G} \sigma(P) = (P_1 P_2 \cdots P_g)^{ef} = (p)^f = (p^f).$$

E a demonstração está completa.

■

Proposição 3.1.4 *Suponha que $K/\mathbb{Q}$ seja uma extensão galoisiana com grupo de Galois G. Sejam $\alpha \in D$ e $I = (\alpha)$ o ideal principal gerado por α. Então $N(I) = |N(\alpha)|$.*

DEMONSTRAÇÃO: Da proposição acima e da proposição 2.1.3 segue que

$$(N(I)) = \prod_{\sigma \in G} \sigma(I) = \prod \sigma((\alpha)) = \prod (\sigma(\alpha)) = (\prod \sigma(\alpha)) = (N(\alpha)).$$

Portanto $N(I)$ e $N(\alpha)$ diferem por uma unidade. Como ambas pertencem à $\mathbb{Z}$ e, por definição, $N(I)$ é sempre positiva, segue que $N(I) = |N(\alpha)|$.

■

3.2 O símbolo de resíduos m - ésimos

Sejam m um inteiro positivo e D_m o anel de inteiros de $\mathbb{Q}(\zeta_m)$. Sejam P um ideal primo de D_m que não contenha m e $q = N(P) = |D_m/P|$. Pela proposição 2.2.3 sabemos que as classes de $1, \zeta_m, \ldots, \zeta_m^{m-1}$ são todas distintas em D_m/P e que $q \equiv 1 \pmod{m}$.

Proposição 3.2.1 *Seja $\alpha \in D_m$, tal que $\alpha \notin P$. Existe um inteiro i, único módulo m, tal que*

$$\alpha^{(q-1)/m} \equiv \zeta_m^i \pmod{P}.$$

DEMONSTRAÇÃO: Como o grupo multiplicativo de D_m/P tem $q-1$ elementos temos que $\alpha^{q-1} \equiv 1 \pmod{P}$. Portanto

$$\prod_{i=0}^{m-1} (\alpha^{(q-1)/m} - \zeta_m^i) \equiv 0 \pmod{P}.$$

Como P é um ideal primo segue que D_m/P é um domínio de integridade e, portanto, existe i, $0 \leq i \leq m-1$ tal que $\alpha^{(q-1)/m} \equiv \zeta_m^i \pmod{P}$. Sabemos que se $i \not\equiv j \pmod{m}$ então $\zeta_m^i \neq \zeta_m^j$ e pela proposição 2.2.3 segue que $\zeta_m^i \not\equiv \zeta_m^j \pmod{P}$. Portanto i é único módulo m.

■

Definição 3.2.2 *Sejam $\alpha \in D_m$ e P um ideal primo que não contém m. Definimos o* **símbolo de resíduos m - ésimos** *, $\left(\frac{\alpha}{P}\right)_m$, como segue:*

(a) $\left(\frac{\alpha}{P}\right)_m = 0$ *se* $\alpha \in P$.

(b) *Se α não pertence à P, então $\left(\frac{\alpha}{P}\right)_m$ é a única raíz m - ésima da unidade tal que $\alpha^{(N(P)-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P}$.*

Trabalharemos essencialmente com os seguintes casos particulares da definição acima.

Definição 3.2.3 *Quando* $m = 2$ *usaremos a notação* $\left(\frac{a}{b}\right)_2 = \left(\frac{a}{b}\right)$ *e neste caso chamaremos o símbolo de resíduos* 2 *- ésimos de* **símbolo de Legendre**. *Quando* $m = 3$ *chamaremos o símbolo de resíduos* 3 *- ésimos de* **símbolo de resíduos cúbicos**. *Quando* $m = 4$ *diremos* **símbolo de resíduos biquadráticos**.

Antes de demonstrarmos as principais propriedades do símbolo de resíduos m - ésimos precisaremos dos seguintes lemas.

Lema 3.2.4 *Sejam* a, b *inteiros e* $d = (a, m)$. *A congruência* $ax \equiv b \pmod{m}$ *tem solução se, e somente se,* $d \mid b$. *Se* $d \mid b$, *então existem exatamente* d *soluções módulo* m.

DEMONSTRAÇÃO: Se x_0 é uma solução, então $ax_0 - b = my_0$ para algum $y_0 \in \mathbb{Z}$. Portanto $ax_0 - my_0 = b$. Como $d \mid (ax_0 - my_0)$ segue que $d \mid b$.

Reciprocamente, suponha que $d \mid b$. Seja $c = b/d$. Sabemos que existem inteiros x_0' e y_0' tais que $ax_0' - my_0' = d$. Multiplique ambos os lados da última equação por c. Então $a(x_0'c) - m(y_0'c) = b$. Tome $x_0 = x_0'c$. Segue que $ax_0 \equiv b \pmod{m}$ e mostramos que $ax_0 \equiv b \pmod{m}$ tem solução se, e somente se $d \mid b$.

Suponha que $ax_0 \equiv b \pmod{m}$ e $ax_1 \equiv b \pmod{m}$. Segue que $a(x_1 - x_0) \equiv 0 \pmod{m}$. Tome $a' = a/d$ e $m' = m/d$. Vimos que $m \mid a(x_1 - x_0)$ e portanto $m' \mid a'(x_1 - x_0)$. Como m' e a' são primos entre si, segue que $m' \mid (x_1 - x_0)$, ou, equivalentemente, $x_1 = x_0 + km'$ para algum inteiro k. Vimos que dada uma solução x_0 tem-se que qualquer outra solução x_1 deve ser da forma $x_1 = x_0 + km'$, para algum k.

Reciprocamente, dada uma solução x_0 vemos facilmente que todo número da forma $x_0 + km'$, $k \in \mathbb{Z}$ deve ser solução.

Vamos mostrar que dada uma solução x_0, o conjunto $x_0, x_0 + m', \ldots, x_0 + (d-1)m'$ contém todas as soluções distintas módulo m. Suponha que para $i, j \in \{1, 2, \ldots, d-1\}$ vale que $x_0 + im' \equiv x_0 + jm' \pmod{m}$. Como $m/m' = d$, segue que $i \equiv j \pmod{d}$ e, portanto, $i = j$.

Agora, suponha que exista uma solução $x_1 = x_0 + km'$ tal que x_1 não pertence à $x_0, x_0 + m', \ldots, x_0 + (d-1)m'$. Pelo algoritmo euclideano sabemos que existem inteiros r, s, $0 \leq s < d$, tais que $k = rd + s$. Portanto, $x_1 = x_0 + sm' + rm$ e x_1 é equivalente à $x_0 + sm'$. O que completa a demonstração.

■

Lema 3.2.5 *Sejam F um corpo finito com q elementos e $\alpha \in F^*$. Então $x^m = \alpha$ tem solução se, e somente se, $\alpha^{(q-1)/d} = 1$, onde $d = (m, q-1)$. Se existem soluções, então existem exatamente d soluções.*

DEMONSTRAÇÃO: Seja γ um gerador de F^* e suponha que $\alpha = \gamma^a$ e $x = \gamma^b$. Então $x^m = \alpha$ é equivalente à $\gamma^{bm} = \gamma^a$, que é equivalente à, $mb \equiv a \pmod{q-1}$. Agora, pelo lema anterior (substituindo em sua notação x por b, a por m, b por a e lembrando que $d = (m, q-1)$), temos que $mb \equiv a \pmod{q-1}$ se, e somente se, $(m, q-1) = d \mid a$. E, como a ordem de γ é $q-1$, isso ocorre se, e somente se, $\alpha^{(q-1)/d} = \gamma^{a(q-1/d)} = 1$.

■

As primeiras propriedades elementares sobre o símbolo de resíduos m - ésimos são:

Proposição 3.2.6

(*a*) $\left(\frac{\alpha}{P}\right)_m = 1$ *se, e somente se,* $x^m \equiv \alpha \pmod{P}$ *é solúvel em* D_m.

(*b*) **Critério de Euler:** *Para todo* $\alpha \in D_m$, $\alpha^{(N(P)-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P}$.

(*c*) $\left(\frac{\alpha\beta}{P}\right)_m = \left(\frac{\alpha}{P}\right)_m \left(\frac{\beta}{P}\right)_m$.

(*d*) *Se* $\alpha \equiv \beta \pmod{P}$, *então* $\left(\frac{\alpha}{P}\right)_m = \left(\frac{\beta}{P}\right)_m$.

DEMONSTRAÇÃO: A parte (a) segue do lema 3.2.5 tomando $F = D_m/P$ e $q = N(P)$. A parte (b) segue diretamente da definição. Quanto à parte (c) basta observar que $\left(\frac{\alpha\beta}{P}\right)_m \equiv (\alpha\beta)^{(N(P)-1)/m} \equiv \alpha^{(N(P)-1)/m}\beta^{(N(P)-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m \left(\frac{\beta}{P}\right)_m \pmod{P}$. Para a parte (d) temos que se $\alpha \equiv \beta \pmod{P}$, então $\left(\frac{\alpha}{P}\right)_m \equiv \alpha^{(N(P)-1)/m} \equiv \beta^{(N(P)-1)/m} \equiv \left(\frac{\beta}{P}\right)_m \pmod{P}$. Pela proposição 2.2.3 segue que $\left(\frac{\alpha}{P}\right)_m = \left(\frac{\beta}{P}\right)_m$.

■

Corolário 3.2.7 *Seja P um ideal primo que não contenha m. Então*

$$\left(\frac{\zeta_m}{P}\right)_m = \zeta_m^{(N(P)-1)/m}.$$

DEMONSTRAÇÃO: Pela parte (b) da proposição acima vemos que $\left(\frac{\zeta_m}{P}\right)_m$ e $\zeta_m^{(N(P)-1)/m}$ são congruentes módulo P. Como ambos são raízes m - ésimas da unidade e m não pertence à P segue, pela proposição 2.2.3, que são iguais. ■

É importante que estendamos a definição de $\left(\frac{\alpha}{P}\right)_m$ de tal maneira que o símbolo $\left(\frac{\alpha}{\beta}\right)_m$ faça sentido para $\beta \in D_m$ e primo com m.

Definição 3.2.8 *Seja $I \subset D_m$ um ideal primo com (m). Seja $I = P_1P_2\cdots P_n$ uma decomposição prima de I. Para $\alpha \in D_m$ definimos $\left(\frac{\alpha}{I}\right)_m = \prod_i \left(\frac{\alpha}{P_i}\right)_m$. Se $\beta \in D_m$ é primo com m definimos $\left(\frac{\alpha}{\beta}\right)_m = \left(\frac{\alpha}{(\beta)}\right)_m$.*

A generalização feita acima tem as mesmas propriedades e elas são dadas no resultado abaixo.

Proposição 3.2.9 *Sejam I e J ideais co-primos com (m). Então*

(a) $\left(\frac{\alpha\beta}{I}\right)_m = \left(\frac{\alpha}{I}\right)_m\left(\frac{\beta}{I}\right)_m$.

(b) $\left(\frac{\alpha}{IJ}\right)_m = \left(\frac{\alpha}{I}\right)_m\left(\frac{\alpha}{J}\right)_m$.

(c) *Se α é primo com I e $x^m \equiv \alpha \pmod{I}$ é solúvel em D_m, então* $\left(\frac{\alpha}{I}\right)_m = 1$.

DEMONSTRAÇÃO: Para o item (a) basta decompormos I em ideais primos, usarmos a definição acima, aplicar o item (c) da proposição 3.2.6 e reagruparmos de forma conveniente usando a definição. O item (b) é demonstrado de maneira similar, basta decompormos IJ, aplicarmos a definição acima, reagruparmos de maneira conveniente e usarmos novamente a definição. O item (c) segue diretamente da definição e da proposição 3.2.6 item (b). Observamos que a recíproca de (c) é falsa. De fato, $\left(\frac{3}{5}\right)_2 = \left(\frac{3}{7}\right)_2 = -1$, e, no entanto, $\left(\frac{3}{35}\right)_2 = 1$.

■

Seja σ um automorfismo do grupo de Galois G de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Nos será útil observarmos o comportamento do símbolo $\left(\frac{\alpha}{I}\right)_m$ sob a ação de σ. No que segue usaremos a notação exponencial para automorfismos, isto é, se $\alpha \in D_m$ e I é um ideal de D_m, usaremos a seguinte notação $\sigma(\alpha) = \alpha^\sigma$ e $\sigma I = I^\sigma$.

Proposição 3.2.10 *Sejam I um ideal co-primo com (m) e $\sigma \in G$. Então*

$$\left(\frac{\alpha}{I}\right)^\sigma = \left(\frac{\alpha^\sigma}{I^\sigma}\right).$$

DEMONSTRAÇÃO: Como ambos os lados da igualdade acima são multiplicativos em I, será suficiente se demonstrarmos a proposição apenas para o caso $I = P$, P um ideal primo.

Pela definição 3.2.2 segue que

$$\alpha^{(N(P)-1)m} \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P}.$$

Aplicando σ à ambos os lados da igualdade acima obtemos

$$(\alpha^\sigma)^{(N(P)-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m^\sigma \pmod{P^\sigma}.$$

Como por definição $(\alpha^\sigma)^{(N(P)-1)/m} \equiv \left(\frac{\alpha^\sigma}{P^\sigma}\right)_m \pmod{P^\sigma}$, segue que $\left(\frac{\alpha}{P}\right)_m^\sigma \equiv \left(\frac{\alpha^\sigma}{P^\sigma}\right)_m \pmod{P^\sigma}$. Sendo $\left(\frac{\alpha}{P}\right)_m^\sigma$ e $\left(\frac{\alpha^\sigma}{P^\sigma}\right)_m$ raízes m - ésimas da unidade, segue a igualdade.

Observamos que usamos acima o fato que $N(P) = N(P^\sigma)$.

■

Capítulo 4

Somas de Gauss e de Jacobi

Neste capítulo vamos introduzir as noções de somas de Gauss e de Jacobi. Elas serão usadas no capítulo 5 para demonstrar as leis de reciprocidade quadrática, cúbica e biquadrática. Durante este capítulo p denotará um número primo, $F_p = \mathbb{Z}/p\mathbb{Z}$ o corpo finito com p elementos e F_p^* o seu grupo multiplicativo. Também denotaremos por ζ uma raíz primitiva p - ésima da unidade

4.1 Caracteres multiplicativos

Começamos esta seção com a seguinte definição.

Definição 4.1.1 *Um* **caracter multiplicativo** *é um homomorfismo multiplicativo χ de F_p^* no corpo dos números complexos $\mathbb{C}$.*

Exemplo 4.1.2

(*a*) *O caracter multiplicativo trivial ε que é definido por $\varepsilon(a) = 1\ \forall a \in F_p^*$.*

(*b*) *O símbolo de resíduos m - ésimos definido em 3.2.2.*

Quando estiver claro no contexto deveremos dizer apenas caracter ao invés de caracter multiplicativo.

Um caracter χ pode ser estendido à uma função de F_p definindo $\chi(0) = 0$ e $\varepsilon(0) = 1$.

As duas proposições que seguem apresentam algumas propriedades fundamentais dos caracteres.

Proposição 4.1.3 *Seja χ um caracter multiplicativo e $a \in F_p^*$. Então*

(a) $\chi(1) = 1$

(b) $\chi(a)$ *é uma* $(p-1)$ *- ésima raiz da unidade*

(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Onde o 1 *do lado esquerdo de* (a) *pertence à* F_p*, enquanto o* 1 *do lado direito pertence à* $\mathbb{C}$ *e a barra sobre* $\chi(a)$ *em* (c) *denota a conjugação complexa de* $\chi(a)$.

DEMONSTRAÇÃO: Para demonstrarmos (a) basta observarmos que $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$ e assim $\chi(1) = 1$. (b) segue do Pequeno Teorema de Fermat, de fato, $a^{p-1} = 1$ e portanto $\chi(a^{p-1}) = \chi(a)^{p-1} = 1$. Para a primeira igualdade de (c), utilizando (a), observamos que:

$$aa^{-1} = 1 \Rightarrow 1 = \chi(aa^{-1}) = \chi(a)\chi(a^{-1}) \Rightarrow \chi(a^{-1}) = \chi(a)^{-1}.$$

Para a segunda igualdade de (c), utilizando (b) e a norma complexa $|\cdot|$, segue que $|\chi(a)| = 1$, logo $\chi(a)\overline{\chi(a)} = \chi(a)\chi(a)^{-1}$ e então $\overline{\chi(a)} = \chi(a)^{-1}$.

■

Proposição 4.1.4 *Seja χ um caracter. Se $\chi \neq \varepsilon$, então $\sum_{t \in F_p} \chi(t) = 0$. Se $\chi = \varepsilon$ então $\sum_{t \in F_p} \chi(t) = p$.*

DEMONSTRAÇÃO: A última afirmação é clara. Suponha $\chi \neq \varepsilon$. Nesse caso existe $a \in F_p$ tal que $\chi(a) \neq 1$. Seja $T = \sum_{f \in F_p} \chi(f)$. Temos que $\chi(a)T = \sum_{t \in F_p} \chi(at) = T$ e assim $T = 0$, uma vez que $\chi(a) \neq 1$. Usamos que at percorre todo F_p conforme t o faz.

■

Os caracteres formam um grupo abeliano com identidade igual à ε, onde o produto e o inverso são definidos da seguinte forma:

$$\begin{array}{rccc} \chi\cdot\lambda : F_p^* & \to & \mathbb{C} \\ a & \mapsto & \chi(a)\lambda(a) \end{array} \qquad \begin{array}{rccc} \chi^{-1} : F_p^* & \to & \mathbb{C} \\ a & \mapsto & \chi(a)^{-1}. \end{array}$$

Vamos mostrar que este grupo é um grupo cíclico de ordem $p-1$.

Proposição 4.1.5 *O grupo dos caracteres é um grupo cíclico de ordem $p-1$. Se $a \neq 1 \in F_p^*$, então existe χ tal que $\chi(a) \neq 1$.*

DEMONSTRAÇÃO: Sabemos que F_p^* é cíclico. Tome g um gerador de F_p^*. Se $a = g^l$, então $\chi(a) = \chi(g)^l$, o que mostra que χ é unicamente determinado pelo valor de $\chi(g)$. Como $\chi(g)$ é uma $p-1$ ésima raiz da unidade e sabemos que existem exatamente $p-1$ delas, segue que o grupo de caracteres tem ordem no máximo $p-1$.

Defina o caracter λ por $\lambda(g^k) = e^{(2\pi ik)/p-1}$. Afirmamos que $p-1$ é o menor inteiro n tal que $\lambda^n = \varepsilon$. De fato, se $\lambda^n = \varepsilon$ então $\lambda(g)^n = \varepsilon(g) = 1$ o que implica $e^{(2\pi in)/p-1} = 1$ e portanto $p-1|n$. Como $\lambda^{p-1}(a) = \lambda(a^{p-1}) = \lambda(1)$, a afirmação segue e os caracteres $\varepsilon, \lambda, \ldots, \lambda^{p-2}$ são todos distintos e, pelo que vimos acima, são todos os caracteres.

Agora, se $a \in F_p^*$ e $a \neq 1$, então $a = g^l$ para algum $l \in \{1, \ldots, p-2\}$ e assim $\lambda(a) = \lambda(g^l) = e^{(2\pi il)/p-1} \neq 1$.

■

Temos o seguinte corolário da proposição acima.

Corolário 4.1.6 *Se $a \in F_p^*$ e $a \neq 1$, então $\sum_\chi \chi(a) = 0$.*

DEMONSTRAÇÃO: Seja $S = \sum_\chi \chi(a)$. Como $a \neq 1$, existe λ tal que $\lambda(a) \neq 1$. Daí, como $\lambda\chi$ percorre todos caracteres conforme χ o faz, segue que $\lambda(a)S = \sum_\chi \lambda(a)\chi(a) = \sum_\chi \lambda\chi(a) = S \Rightarrow (\lambda(a)-1)S = 0 \Rightarrow S = 0$.

■

4.2 Somas de Gauss

Nesta seção introduziremos o importante conceito de somas de Gauss bem como suas principais propriedades.

Definição 4.2.1 *Sejam χ um caracter sobre F_p e $a \in F_p$. A* **soma de Gauss** *sobre F_p pertencente ao caracter χ, $g_a(\chi)$, é definida por*

$$g_a(\chi) = \sum_{t \in F_p} \chi(t)\zeta^{at}.$$

O próximo resultado caracteriza a soma de gauss $g_a(\chi)$ em termos de a e do caracter χ.

Proposição 4.2.2 *Sejam χ um caracter sobre F_p e $a \in F_p$. Se $a \neq 0$ e $\chi \neq \varepsilon$, então $g_a(\chi) = \chi(a^{-1})g_1(\chi)$. Se $a \neq 0$ e $\chi = \varepsilon$, então $g_a(\varepsilon) = 0$. Se $a = 0$ e $\chi \neq \varepsilon$, então $g_a(\chi) = 0$. Se $a = 0$ e $\chi = \varepsilon$, então $g_a(\varepsilon) = p$.*

DEMONSTRAÇÃO: Se $a \neq 0$ e $\chi \neq \varepsilon$, então $\chi(a)g_a(\chi) = \chi(a)\sum_{t \in F_p} \chi(t)\zeta^{at} = \sum_{t \in F_p} \chi(at)\zeta^{at} = g_1(\chi)$. Se $a \neq 0$ e $\chi = (\varepsilon)$, então $g_a(\varepsilon) = \sum_{t \in F_p} \varepsilon(t)\zeta^{at} = \sum_{t \in F_p} \zeta^{at} = \sum_{t \in F_p} \zeta^t = 0$($\zeta$ é raíz de $1 + x + \cdots + x^{p-1}$). E, se $a = 0$, então $g_0(\chi) = \sum_{t \in F_p} \chi(t)\zeta^{0 \cdot t} = \sum_{t \in F_p} \chi(t) = p$ ou 0, dependendo se $\chi = \varepsilon$ ou $\chi \neq \varepsilon$ pela proposição 4.1.4.

■

A proposição anterior nos leva a tratar $g_1(\chi)$ de maneira especial e portanto a partir de agora denotaremos $g_1(\chi)$ por $g(\chi)$. E mais ainda, a partir dela temos que se $a \neq 0$ e $\chi \neq \varepsilon$, então $|g_a(\chi)| = |g|$. Na próxima proposição vamos calcular esse valor comum e para isto precisaremos do seguinte resultado.

Lema 4.2.3 *Dados $x, y \in \mathbb{Z}$ tem-se que $p^{-1}\sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x, y)$, onde $\delta(x, y) = 1$ se $x \equiv y \pmod{p}$ e $\delta(x, y) = 0$ se $x \not\equiv y \pmod{p}$.*

DEMONSTRAÇÃO: Se $x - y \equiv 0 \pmod{p}$, então $\zeta^{x-y} = 1$, e portanto $\sum_{t=0}^{p-1} \zeta^{(x-y)t} = p$. Se $a = x - y \not\equiv 0 \pmod{p}$, então $\zeta^{x-y} \neq 1$ e $\sum_{t=0}^{p-1} \zeta^{(x-y)t} = \sum_{t=0}^{p-1} \zeta^t = 0$.

■

Proposição 4.2.4 *Se $\chi \neq \varepsilon$, então $|g(\chi)| = \sqrt{p}$.*

DEMONSTRAÇÃO: Se $a \neq 0$, então pela proposição 4.2.2 temos $g_a(\chi) = \chi(a^{-1})g(\chi)$, assim, $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \overline{\chi(a^{-1})}\ \overline{g(\chi)} \overset{4.1.3}{=} \chi(a)\overline{g(\chi)}$ e portanto,

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g(\chi)\overline{g(\chi)} = |g(\chi)|^2.$$

Como $g_0(\chi) = 0$, somando a equação acima em a obtemos

$$\sum_{a \in F_p} g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|. \tag{4.1}$$

Por outro lado,

$$g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

Somando ambos os lados em a e usando o lema 4.2.3 temos

$$\sum_{a \in F_p} g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\delta(x,y)p = (p-1)p.$$

Substituindo o valor acima em 4.1 temos $(p-1)|g(\chi)|^2 = (p-1)p$ e então $|g(\chi)|^2 = p$.

■

Como consequência desta última proposição tem-se:

Corolário 4.2.5 *Se χ é um caracter multiplicativo qualquer então:*

$$g(\chi)g(\overline{\chi}) = \chi(-1)p.$$

DEMONSTRAÇÃO: Seja χ um caracter multiplicativo qualquer. Como $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$, segue que $\chi(-1) = \pm 1$ e portanto $\chi(-1) = \overline{\chi(-1)} = \chi(-1)^{-1}$. Então temos que

$$\overline{g(\chi)} = \sum_{t \in F_p} \overline{\chi(t)}\zeta^{-t} = \chi(-1)\sum_{t \in F_p} \overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\overline{\chi}).$$

Agora, o fato que $|g(\chi)|^2 = p$, pode ser escrito como

$$g(\chi)g(\overline{\chi}) = \chi(-1)p.$$

■

4.3 Somas de Jacobi

Nesta seção introduziremos o importante conceito de somas de Jacobi bem como suas principais propriedades.

Definição 4.3.1 *Sejam χ e λ caracteres de F_p. A* **soma de Jacobi**, *$J(\chi, \lambda)$, é definida por:*

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b).$$

Enunciaremos na proposição a seguir as principais propriedades das somas de Jacobi.

Proposição 4.3.2 *Sejam χ e λ caracteres não triviais. Então*

(a) $J(\varepsilon, \varepsilon) = p$

(b) $J(\varepsilon, \chi) = 0$

(c) $J(\chi, \chi^{-1}) = -\chi(-1)$

(d) *Se $\chi\lambda \neq \varepsilon$ então*

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Demonstração: Para demonstramos (a) basta usarmos a definição. De fato, $J(\varepsilon, \varepsilon) = \sum_{a+b=1} \varepsilon(a)\varepsilon(b) = \sum_{a+b=1} 1 = p$. Para (b), usando a proposição 4.1.4, temos $J(\varepsilon, \chi) = \sum_{a+b=1} \varepsilon(a)\chi(b) = \sum_{a+b=1} \chi(b) = 0$.

Para demonstrarmos a parte (c) observamos que

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1 \\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right).$$

Tome $c = a/(1-a)$. Se $c \neq -1$ então $a = c/(1+c)$. Observe que se a varia sobre $F_p \setminus \{1\}$ então c varia sobre $F_p \setminus \{-1\}$. De fato, se $c = a/(1-a)$ e $c' = a'/(1-a')$, então

$$a \neq a' \Rightarrow a - aa' \neq a' - aa' \Rightarrow a/(1-a) \neq a'/(1-a') \Rightarrow c \neq c'.$$

Portanto,

$$J(\chi, \chi^{-1}) = \sum_{c \neq -1} \chi(c) \overset{4.1.4}{=} -\chi(-1).$$

Para a parte (d) repare que

$$g(\chi)g(\lambda) = \left(\sum_{x \in F_p} \chi(x)\zeta^x \right) \left(\sum_{x \in F_p} \lambda(y)\zeta^y \right) = \sum_{x,y \in F_p} \chi(x)\lambda(y)\zeta^{x+y} =$$

$$= \sum_{t \in F_p} \left(\sum_{x+y=t} \chi(x)\lambda(y)\zeta^t \right). \tag{4.2}$$

Se $t = 0$, então $\sum_{x+y=0} \chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \lambda(-1) \sum_x \chi\lambda(x) = 0$ (pela proposição 4.1.4 e o fato de $\chi\lambda \neq \varepsilon$).

Se $t \neq 0$, defina x' e y' tais que $x = tx'$ e $y = ty'$, daí, se $x + y = t$, então $x' + y' = 1$. Segue que

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t)J(\chi, \lambda).$$

E substituindo em 4.2 obtemos

$$g(\chi)g(\lambda) = \sum_{t \in F_p} \chi\lambda(t)J(\chi, \lambda)\zeta^t = g(\chi\lambda)J(\chi, \lambda).$$

■

Corolário 4.3.3 *Se χ, λ e $\chi\lambda$ são diferentes de ε, então $|J(\chi, \lambda)| = \sqrt{p}$*

DEMONSTRAÇÃO: Pela parte (d) acima e pela proposição 4.2.4 temos

$$|J(\chi, \lambda)| = \frac{|g(\chi)||g(\lambda)|}{|g(\chi\lambda)|} = \frac{\sqrt{p}\sqrt{p}}{\sqrt{p}} = \sqrt{p}.$$

■

Para demonstrarmos as leis de reciprocidade cúbica e biquadrática nos será muito útil obter relações entre somas de Gauss e de Jacobi, o que será feito nas seguintes proposições.

Proposição 4.3.4 *Suponha que $n > 2, p \equiv 1 \pmod{n}$ e que χ é um caracter de ordem n. Então*

$$g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}).$$

DEMONSTRAÇÃO: Pela parte (d) da proposição 4.3.2 temos que $g(\chi)^2 = J(\chi\chi)g(\chi^2)$. Multiplicando por $g(\chi)$ obtemos

$$g(\chi)^3 = J(\chi,\chi)g(\chi^2)g(\chi). \tag{4.3}$$

Novamente usando a proposição 4.3.2 parte (d) temos que

$$J(\chi,\chi^2)g(\chi^3) = g(\chi^2)g(\chi).$$

E substituindo em 4.3 obtemos

$$g(\chi)^3 = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3).$$

Continuando esse processo obtemos

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})g(\chi^{n-1}).$$

Agora, como $\chi^{n-1} = \chi^{-1} = \overline{\chi}$, e vimos no corolário 4.2.5 que $g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = \chi(-1)p$. Multiplicando ambos os lados da equação acima por $g(\chi)$ obtemos o resultado desejado.

■

Vimos que o grupo dos caracteres sobre F_p é um grupo cíclico de ordem $p-1$. Suponha que λ seja um gerador e que $p \equiv 1 \pmod{3}$. Se χ é um caracter de ordem 3 então $\chi = \lambda^{(p-1)/3}$, ou $\chi = \lambda^{2(p-1)/3}$. Dizemos que um caracter χ de ordem 3 é um caracter cúbico.

Temos o seguinte corolário da proposição acima:

Corolário 4.3.5 *Se χ é um caracter cúbico de F_p, então*

$$g(\chi)^3 = pJ(\chi,\chi).$$

DEMONSTRAÇÃO: Basta usar a proposição acima e o fato que $\chi(-1) = \chi((-1)^3) = \chi(-1)^3 = 1$.

■

Seja χ um caracter cúbico e $a \in F_p^*$ qualquer. Como $\chi(a)^3 = \chi^3(a) = 1$, então $\chi(a)$ é uma raíz cúbica da unidade. Segue que, $J(\chi, \chi) \in \mathbb{Z}[\omega]$, onde $\omega = e^{(2\pi i)/3} = (1 + \sqrt{-3})/2$ é uma raíz primitiva cúbica da unidade.

Proposição 4.3.6 *Suponha $p \equiv 1 \pmod 3$ e que χ seja um caracter cúbico da unidade. Seja $J(\chi, \chi) = a + b\omega$. Então,*

(*a*) $b \equiv 0 \pmod 3$.

(*b*) $a \equiv -1 \pmod 3$.

DEMONSTRAÇÃO: Iremos usar congruências no anel de inteiros algébricos. Usando apenas teoria dos números elementar temos que

$$g(\chi)^3 = \left(\sum_{t \in F_p} \chi(t)\zeta^t \right)^3 \equiv \sum_{t \in F_p} \chi(t)^3 \zeta^{3t} \pmod 3.$$

Como $\chi(0) = 0$ e $\chi(t)^3 = 1$ se $t \neq 0$, temos que $\sum_{t \in F_p} \chi(t)^3 \zeta^{3t} = \sum_{t \neq 0} \zeta^{3t} \equiv \sum_{t \neq 0} \zeta^t = -1 \pmod 3$. Portanto, pelo corolário 4.3, segue que

$$g(\chi)^3 = pJ(\chi, \chi) \equiv a + b\omega \equiv -1 \pmod 3.$$

Agora, repetindo este processo para $\overline{\chi}$ e reparando que da demonstração do corolário 4.2.5 segue que $\overline{g(\chi)} = g(\overline{\chi})$ temos

$$g(\overline{\chi})^3 = pJ(\overline{\chi}, \overline{\chi}) \equiv a + b\overline{\omega} \equiv -1 \pmod 3.$$

Subtraindo as duas equações acima temos $b(\omega - \overline{\omega}) = b\sqrt{-3} \equiv 0 \pmod 3$. Portanto, $-3b^2 \equiv 0 \pmod 9$ e $3b^2 \in \mathbb{N}$, o que implica $3|b$ em $\mathbb{Z}$. Como $a + b\omega \equiv -1 \pmod 3$, segue que $a \equiv -1 \pmod 3$. ∎

Capítulo 5

Leis de reciprocidade

Neste capítulo usaremos as somas de Gauss e de Jacobi para demonstrarmos as leis de reciprocidade quadrática, cúbica e biquadrática. Como usual (ver definições 3.2.2 e ??)denotaremos o símbolo de resíduos m - ésimos por $\left(\frac{\cdot}{\cdot}\right)_m$ e reservamos a notação $\left(\frac{\cdot}{\cdot}\right)$ para o símbolo de resíduos quadráticos, ou símbolo de Legendre. Antes de enunciarmos a lei de reciprocidade cúbica (biquadrática) será necessário desenvolver algumas propriedades do anel $\mathbb{Z}[\omega]$, ω sendo uma raíz primitiva de 1 ($\mathbb{Z}[i]$, o anel de Gauss).

5.1 A Lei de reciprocidade quadrática

Dado um primo ímpar p o símbolo de Legendre $\left(\frac{a}{p}\right)$, assume o valor 1 se a é um resíduo quadrático módulo p, -1 se a não é resíduo quadrático módulo p e 0 se $p \mid a$.

Durante esta seção, sempre que o contexto permitir, diremos apenas resíduo ao invés de resíduo quadrático.

A Lei de reciprocidade quadrática diz que:

Teorema 5.1.1 (Lei de reciprocidade quadrática) *Se p e q são primos ímpares distintos, então*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}.$$

Vamos demonstrar o teorema acima mais adiante. A lei de reciprocidade quadrática foi conjecturada por Euler e por Legendre e foi demonstrada pela primeira vez por Gauss. Os seguintes complementos da lei de reciprocidade quadrática foram demonstrados por Euler.

Proposição 5.1.2 *Se p é um primo ímpar, então*

(a) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

(b) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

DEMONSTRAÇÃO: A parte (a) segue diretamente do critério de Euler, proposição 3.2.6 (b). De fato, pelo critério de Euler temos $(-1)^{\frac{p-1}{2}}\equiv\left(\frac{-1}{p}\right) \pmod p$ e assim $(-1)^{\frac{p-1}{2}}=\left(\frac{-1}{p}\right)$.

Para a parte (b) seja $\zeta=e^{2\pi i/8}$ uma raiz primitiva oitava da unidade. Temos que $\zeta^8-1=0$, isto é $(\zeta^4-1)(\zeta^4+1)=0$. Como $\zeta^4\neq 1$ temos

$$\zeta^4+1=0\overset{\times\zeta^{-2}}{\Rightarrow}\zeta^2+\zeta^{-2}=0\Rightarrow(\zeta+\zeta^{-1})^2=\zeta^2+2+\zeta^{-2}=2.$$

Seja $\tau=\zeta+\zeta^{-1}$. Como ζ é um inteiro algébrico, ζ^{-1} é um inteiro algébrico e, consequentemente, τ é um inteiro algébrico.

No que segue usaremos congruências no anel de inteiros algébricos.

Seja p um primo ímpar em $\mathbb{Z}$ e repare que

$$\tau^{p-1}=(\tau^2)^{(p-1)/2}=2^{(p-1)/2}\equiv\left(\frac{2}{p}\right) \pmod p.$$

Segue que

$$\tau^p\equiv\left(\frac{2}{p}\right)\tau \pmod p \tag{5.1}$$

Como $\tau^p=(\zeta+\zeta^{-1})^p\equiv\zeta^p+\zeta^{-p} \pmod p$ e $\zeta^8=1$, segue que se $p\equiv\pm1 \pmod 8$, então $\tau^p\equiv\zeta^p+\zeta^{-p}=\zeta+\zeta^{-1}=\tau \pmod p$ e se $p\equiv\pm3 \pmod 8$, então $\tau^p\equiv\zeta^p+\zeta^{-p}=\zeta^3+\zeta^{-3}=-(\zeta+\zeta^{-1})\equiv-\tau \pmod p$(usamos que $\zeta^3=-\zeta^{-1}$).

Usando as considerações acima em 5.1 obtemos

$$(-1)^{\alpha}\tau \equiv \left(\frac{2}{p}\right)\tau \pmod{p},$$

onde $\alpha = (p^2-1)/8$(repare que $(-1)^{\alpha} = 1$ se $p \equiv \pm 1 \pmod 8$ e $(-1)^{\alpha} = -1$ se p $\equiv \pm 3 \pmod 8$).

Multiplicando por τ obtemos

$$(-1)^{\alpha}2 \equiv \left(\frac{2}{p}\right)2 \pmod{p} \Rightarrow$$

$$\Rightarrow (-1)^{\alpha} = \left(\frac{2}{p}\right).$$

■

Denotemos a soma de Gauss $g\left(\left(\frac{a}{p}\right)\right)$ apenas por g e $g_a\left(\left(\frac{a}{p}\right)\right)$ por g_a.

A relação $(\zeta+\zeta^{-1})^2 = 2$ nos motiva a encontrar uma relação onde 2 possa ser substituído por um primo ímpar p qualquer. Essa nova relação segue do corolário 4.2.5. De fato, ele nos diz que

$$g(\chi)g(\overline{\chi}) = \chi(-1)p.$$

Se χ é o símbolo de Legendre então $\overline{\chi} = \chi$ e pela proposição 5.1.2 (a) a equação acima pode ser escrita como

$$g^2 = (-1)^{(p-1)/2}p. \tag{5.2}$$

Agora vamos demonstrar a lei de reciprocidade quadrática.

DEMONSTRAÇÃO: Seja $p^* = (-1^{(p-1)/2})p$. Reescrevendo a equação 5.2 temos $g^2 = p^*$ que é o análogo da equação $\tau^2 = 2$ que estávamos procurando. Seja $q \neq p$ um primo ímpar. Usaremos congruências no anel de inteiros algébricos.

Pelo critério de Euler (proposição 3.2.6 (b)) temos que

$$g^{q-1} = (g^2)^{(q-1)/2} = (p^*)^{(q-1)/2} \equiv \left(\frac{p^*}{q}\right) \pmod{q}.$$

O que implica que

$$g^q \equiv \left(\frac{p^*}{q}\right)g \pmod{q}. \tag{5.3}$$

Mas,

$$g^q = \left(\sum_{t=0}^{p-1} \left(\frac{t}{p}\right)\zeta^t\right)^q \equiv \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)^q \zeta^{tq} = g_q \pmod{q}.$$

E, como $g_q = \left(\frac{q}{p}\right)g$ (proposição 4.2.2), segue que

$$g^q \equiv g_q = \left(\frac{q}{p}\right) g \pmod{q}. \tag{5.4}$$

De 5.3 e 5.4 temos

$$\left(\frac{p^*}{q}\right) g \equiv \left(\frac{q}{p}\right) g \pmod{q}.$$

Multiplicando ambos os lados por g, e usando que $g^2 = p^*$:

$$\left(\frac{p^*}{q}\right) p^* \equiv \left(\frac{q}{p}\right) p^* \pmod{q}$$

Como $(p, q) = 1$ a equação acima implica que

$$\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q} \Rightarrow \left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Finalmente, observamos que pela multiplicidade do símbolo de Legendre e pela proposição 5.1.2 (a) segue que

$$\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = (-1)^{(p-1/2)(q-1)/2} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

E o resultado segue do fato de $\left(\frac{p}{q}\right)^{-1} = \left(\frac{p}{q}\right)$.

■

5.2 O anel $\mathbb{Z}[\omega]$

As propriedades mais usuais do anel $\mathbb{Z}[\omega]$ serão enunciadas sem demonstração. As demonstrações podem ser encontradas em livros introdutórios como [5].

Vimos na proposição 2.2.11 que se ω é uma raiz cúbica primitiva da unidade então o anel de inteiros de $\mathbb{Q}[\omega]$ é igual à $\mathbb{Z}[\omega]$. Os elementos de $\mathbb{Z}[\omega]$ são números complexos que se escrevem, de maneira única, na forma $a+b\omega$, $a, b \in \mathbb{Z}$. Se $\alpha = a + b\omega \in Z[\omega]$, então definimos a norma de α, $N(\alpha)$, por $N(\alpha) = \alpha\overline{\alpha} = a^2 - ab + b^2$, onde $\overline{\alpha}$ é o conjugado complexo de α. Sabemos que $\mathbb{Z}[\omega]$ é um domínio euclideano e, consequentemente, $\mathbb{Z}[\omega]$ é um domínio fatorial.

Se α é um inteiro algébrico qualquer, então α é uma unidade se, e somente se, $N(\alpha) = \pm 1$. Usando isso pode-se provar o seguinte:

Proposição 5.2.1 *As unidades de* $\mathbb{Z}[\omega]$ *são* $1, -1, \omega, -\omega, \omega^2$, *e* $-\omega^2$.

Iremos agora classificar os números primos de $\mathbb{Z}[\omega]$.

Proposição 5.2.2 *Suponha que* p *e* q *sejam primos racionais. Se* $q \equiv 2 \pmod 3$, *então* q *é primo em* $\mathbb{Z}[\omega]$. *Se* $p \equiv 1 \pmod 3$, *então* $p = \pi\overline{\pi}$, *onde* π *é primo em* $\mathbb{Z}[\omega]$. *E* $3 = -\omega^2(1-\omega)^2$, *onde* $1-\omega$ *é primo em* $\mathbb{Z}[\omega]$.

Usaremos a partir de agora a seguinte notação. Um primo racional congruente à 2 módulo 3 será denotado por q e π denotará um primo complexo tal que $N(\pi) = p$, p um primo racional. Ocasionalmente π denotará um primo qualquer de $\mathbb{Z}[\omega]$, conforme o contexto permitir.

Nos será extremamente útil a noção de congruências em $\mathbb{Z}[\omega]$. Se $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ então dizemos que $\alpha \equiv \beta \pmod \gamma$ se γ divide $\alpha - \beta$. Como em $\mathbb{Z}$ as classes de congruência módulo γ podem ser consideradas como um anel, chamado o anel de classes residuais módulo γ e denotado por $\mathbb{Z}[\omega]/\gamma\mathbb{Z}[\omega]$.

Proposição 5.2.3 *Seja* $\pi \in \mathbb{Z}[\omega]$ *um primo. Então* $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ *é um corpo com* $N(\pi)$ *elementos.*

Da proposição acima segue o pequeno teorema de Fermat para $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$.

Proposição 5.2.4 *Se* $\pi \nmid \alpha$, *então* $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$.

Para enunciarmos a lei de reciprocidade cúbica precisaremos antes definir o conceito de primo primário em $\mathbb{Z}[\omega]$.

Definição 5.2.5 *Se* π *é um primo em* $\mathbb{Z}[\omega]$, *dizemos que* π *é* **primário** *se* $\pi \equiv 2 \pmod 3$.

Esta definição de primário tem a função de eliminar a ambiguidade causada pelo fato de todo elemento diferente de zero de $\mathbb{Z}[\omega]$ ter seis associados. Isto é semelhante à considerarmos apenas primos positivos em $\mathbb{Z}$.

Se $\pi = q$, $\pi \neq 3$, é um primo racional e π não é primário, então $-\pi$ é primário. Se $\pi = a+b\omega$ é um primo complexo, a definição acima é equivalente a dizer que $a \equiv 2 \pmod 3$ e $b \equiv 0 \pmod 3$.

Proposição 5.2.6 *Suponha que $N(\pi) = p \equiv 1 \pmod 3$. Entre os associados de π exatamente um é primário.*

DEMONSTRAÇÃO: Os associados de $\pi = a + b\omega$ são:

(a) $\pi = a + b\omega$.

(b) $\omega\pi = -b + (a - b)\omega$.

(c) $\omega^2\pi = (b - a) - a\omega$.

(d) $-\pi = a - b\omega$.

(e) $-\omega\pi = b + (b - a)\omega$.

(f) $-\omega^2\pi = (a - b) + a\omega$.

Como $p = a^2 - ab + b^2$, não podemos ter a e b simultaneamente divisíveis por 3. Segue das partes a e b que podemos assumir que $3 \nmid a$. Das partes a e d segue que $a \equiv 2 \pmod 3$. Destas considerações e do fato que $p = a^2-ab+b^2$, segue que $1 \equiv 4 - 2b + b^2 \pmod 3$, ou $b(b - 2) \equiv 0 \pmod 3$. Se $3 \mid b$, então $a + b\omega$ é primário. Se $b \equiv 2 \pmod 3$, então $b + (b - a)\omega$ é primário.

Para mostrar a unicidade basta assumir que $a + b\omega$ é primário e verificar que do item b ao f nenhum número é primário.

■

5.3 A lei de reciprocidade cúbica

Durante esta seção nos será útil a notação $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$, onde π é um primo e α é um elemento qualquer de $\mathbb{Z}[\omega]$.

Teorema 5.3.1 (Lei de reciprocidade cúbica) *Sejam π_1 e π_2 primários, $N(\pi_1), N(\pi_2) \neq 3$, e $N(\pi_1) \neq N(\pi_2)$. Então*

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

A demonstração do teorema acima será dada mais adiante, no entanto observamos que temos três casos a considerar. O primeiro quando π_1 e π_2 são ambos racionais, o segundo quando π_1 é racional e π_2 é complexo, e o terceiro quando ambos π_1 e π_2 são complexos. O primeiro caso é o mais fácil de ser tratado e segue como corolário da seguinte proposição.

Proposição 5.3.2 *Se π é um primo e α é um elemento qualquer de $\mathbb{Z}[\omega]$, então*

(*a*) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.

(*b*) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.

DEMONSTRAÇÃO: Para a parte (*a*), se $\pi \mid \alpha$ o resultado é trivial. Se $\pi \nmid \alpha$, então basta repararmos que $\chi_\pi(\alpha) = 1, \omega$, ou ω^2 e $1^2 = \overline{1}, \omega^2 = \overline{\omega}$ e $(\omega^2)^2 = \omega = \overline{\omega^2}$.

Para a parte (*b*), pelo critério de Euler (proposição 3.2.6) temos que

$$\alpha^{(N(\pi-1))/3} \equiv \chi_\pi(\alpha) \pmod{\pi}$$

o que implica que

$$\overline{\alpha}^{(N(\pi-1))/3} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$$

.

Usamos o fato que $N(\overline{\pi}) = N(\pi)$. A equação acima, pelo critério de Euler, implica que $\chi_{\overline{\pi}}(\overline{\alpha}) = \overline{\chi_\pi(\alpha)}$.

■

Corolário 5.3.3 *Se q é um primo racional, $q \equiv 2 \pmod 3$, então $\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$. Se n é um inteiro racional primo com q, então $\chi_q(n) = 1$. Se p é um primo racional e p e q são primos entre si, então $\chi_p(q) = \chi_q(p)$.*

DEMONSTRAÇÃO: Como $\overline{q} = q$ temos pela proposição acima que $\chi_q(\overline{\alpha}) = \chi_{\overline{q}}(\overline{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha^2)$.

Como $n = \overline{n}$ temos que $\chi_q(n) = \overline{\chi_q(n)} = \chi_q(n)^2$, e uma vez que $\chi_q(n) \neq 0$ segue que $\chi_q(n) = 1$. Agora, temos claramente que se $p \neq q$ então $\chi_p(q) = \chi_q(p)$.

■

Os seguinte complemento da lei de reciprocidade cúbica determina o caracter cúbico das unidades.

Proposição 5.3.4 *Seja π um primo de $\mathbb{Z}[\omega]$. Então:*

(a) $\chi_\pi(-1) = 1$, *para todo primo* π.

(b) $\chi_\pi(\omega) = \omega^{(N(\pi)-1)/3}$, *se* $N(\pi) \neq 3$.

DEMONSTRAÇÃO: A parte (a) segue do fato que $-1 = (-1)^3$, logo $\chi_\pi(-1) = 1$, para todo primo π de $\mathbb{Z}[\omega]$. A parte (b) segue do critério do Euler. De fato, $\chi_\pi(\omega) \equiv \omega^{(N(\pi)-1)/3} \pmod{\pi}$, logo $\chi_\pi(\omega) = \omega^{(N(\pi)-1)/3}$. Agora, observe que pela proposição 5.2.2, $N(\pi) \equiv 1 \pmod 3$ para todo primo de $\mathbb{Z}[\omega]$ tal que $N(\pi) \neq 3$. Segue que $N(\pi) \equiv 1, 4, 7 \pmod 9$ e, como $\omega^n = \omega^{n'}$ se $n \equiv n' \pmod 3$, então $\chi_\pi(\omega) = 1, \omega, \omega^2$ dependendo se $N(\pi)$ é congruente módulo 9 à 1, 4, ou 7 respectivamente.

■

5.4 Demonstração da lei de reciprocidade cúbica

Seja π um primo complexo tal que $N(\pi) = p \equiv 1 \pmod 3$. Como $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ é um corpo de característica p (proposição 5.2.3), ele contém uma cópia de F_p. E como $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ tem exatamente p elementos ele é isomorfo à F_p. Este isomorfismo pode ser tomado como a função que identifica a classe de n em F_p à classe de n em $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$.

Esta identificação nos permite considerar χ_π como um caracter cúbico sobre F_p, no sentido da página 28 . Sendo assim podemos trabalhar com as

somas de Gauss $g_a(\chi_\pi)$ e as somas de Jacobi $J(\chi_\pi, \chi_\pi)$ para demonstrar a lei de reciprocidade cúbica.

A demonstração da lei de reciprocidade cúbica que daremos foi dada por Eisenstein e é muito similar a demonstração da lei de reciprocidade quadrática que demos na seção 5.1.

Antes precisaremos de alguns resultados.

Vimos no corolário 4.3.5 e na proposição 4.3.4 que

(*a*) $g(\chi)^3 = pJ(\chi, \chi)$.

(*b*) Se $J(\chi, \chi) = a + b\omega$, então $a \equiv -1 \pmod 3$ e $b \equiv 0 \pmod 3$.

Como $J(\chi, \chi)\overline{J(\chi, \chi)} = p$ (proposição 4.3.3), a parte (*b*) acima nos diz que $J(\chi, \chi)$ é um primo primário em $\mathbb{Z}[\omega]$ de norma p.

Lema 5.4.1 *Se k não divide $p-1$, então $1^k+2^k+\cdots+(p-1)^k \equiv 0 \pmod p$.*

DEMONSTRAÇÃO: Seja $S = 1^k + 2^k + \cdots + (p-1)^k$. Tome λ um gerador de F_p^*. Como $k \nmid p-1$, segue que $\lambda^k \neq 1$. Portanto, $\lambda^k S \equiv S \pmod p$ e assim $S \equiv 0 \pmod p$.

■

No que segue assuma que π é primário e que $N(\pi) = p$.

Lema 5.4.2 *Se π é um primo primário tal que $N(\pi) = p$, então $J(\chi_\pi, \chi_\pi) = \pi$.*

DEMONSTRAÇÃO: Suponha que $J(\chi_\pi, \chi_\pi) = \pi'$, onde π' é primário pelas considerações acima. Como $J(\chi_\pi, \chi_\pi)\overline{J(\chi_\pi, \chi_\pi)} = \pi'\overline{\pi}' \overset{4.3.2}{=} p = \pi\overline{\pi}$. Segue que $\pi | \pi'$, ou $\pi | \overline{\pi}'$.

Como todos os primos envolvidos são primários segue que $\pi = \pi'$, ou $\pi = \overline{\pi}'$. Usando a definição de soma de Jacobi e o critério de Euler temos que $J(\chi_\pi, \chi_\pi) = \sum_{x \in F_p} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{x \in F_p} x^{(p-1)/3}(1-x)^{(p-1)/3} \pmod \pi$.

Agora, repare que o polinômio $x^{(p-1)/3}(1-x)^{(p-1)/3}$ é de grau $2/3(p-1) < p-1$. Segue pelo lema acima que $\sum x^{(p-1)/3}(1-x)^{(p-1)/3} \equiv 0 \pmod p$ o que implica que $J(\chi_\pi, \chi_\pi) = \pi' \equiv 0 \pmod \pi$ e portanto $\pi = \pi'$. ■

Usando que $g(\chi)^3 = pJ(\chi, \chi)$ temos o seguinte corolário.

Corolário 5.4.3 $g(\chi_\pi)^3 = p\pi$.

Agora, vamos demonstrar a lei de reciprocidade cúbica.

Teorema 5.4.4 (Lei de reciprocidade cúbica) *Sejam π_1 e π_2 primários, $N(\pi_1), N(\pi_2) \neq 3$, e $N(\pi_1) \neq N(\pi_2)$. Então*

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

DEMONSTRAÇÃO: Como vimos temos três casos a considerar. Quando π_1 é racional e π_2 é complexo, π_1 e π_2 são complexos e π_1 e π_2 são racionais. O último caso demonstramos na página 37. Vamos agora demonstrar o primeiro caso.

Sejam $\pi_1 = q \equiv 2 \pmod 3$ e $\pi_2 = \pi$, $onde N(\pi) = p$.

Pelo corolário 5.4.3 temos que $g(\chi_\pi)^3 = p\pi$. Elevando os dois lados desta igualdade à $(q^2-1)/3$ obtemos $g(\chi_\pi)^{(q^2-1)} = (p\pi)^{(q^2-1)/3}$. O que, pelo critério de Euler implica que $g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi) \pmod q$. Como já vimos que se $(p,q) = 1$, então $\chi_p(q) = 1$ segue que

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi) g(\chi_\pi) \pmod q. \tag{5.5}$$

Usando a definição de somas de Gauss para analisar o lado esquerdo da equação acima, obtemos

$$g(\chi_\pi)^{q^2} = \left(\sum_{t \in F_p} \chi_\pi(t) \zeta^t \right)^{q^2} \equiv \sum_{t \in F_p} \chi_\pi(t)^{q^2} \zeta^{q^2 t} \pmod q.$$

Como $\chi_\pi(t)$ é uma raíz cúbica da unidade e $q^2 \equiv 1 \pmod 3$ temos que $\chi_\pi(t)^{q^2} = \chi_\pi(t)$. O que implica que $g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi) \pmod q$. Mas, pela proposição 4.2.2, temos que $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2}) g(\chi_\pi)$, logo

$$g(\chi_\pi)^{q^2} \equiv \chi_\pi(q^{-2}) g(\chi_\pi) \pmod q \tag{5.6}$$

Combinando as equações 5.5 e 5.6 temos $\chi_\pi(q^{-2}) g(\chi_\pi) \equiv \chi_q(\pi) g(\chi_\pi) \pmod q$. Multiplicando por $\overline{g(\chi_\pi)}$ temos que $\chi_\pi(q^{-2}) p \equiv \chi_q(\pi) p \pmod q$ e então $\chi_\pi(q^{-2}) \equiv \chi_q(\pi) \pmod q$. Como $-2 \equiv 1 \pmod 3$ e, $\chi_\pi(q)$ e $\chi_q(\pi)$ são raízes cúbicas da unidade, pela proposição 2.2.3,segue que

$$\chi_\pi(q) = \chi_q(\pi)$$

Agora, vamos demonstrar o segundo caso.

Sejam π_1 e π_2 são dois primos complexos tais que $N(\pi_i) = p_i \equiv 1 \pmod 3$, para $i = 1, 2$.

Sejam $\gamma_i = \overline{\pi_i}, i = 1, 2$. Como π_i é primário, é fácil ver que γ_i é primário. Temos também que $p_i = \pi_i\gamma_i, i = 1, 2$.

Pelo corolário 5.4.3 temos que $g(\chi_{\gamma_1})^3 = p_1\gamma_1$. Elevando à $(N(\pi_2)-1)/3 = (p_2-1)/3$ e tomando congruências módulo π_2, da mesma maneira que fizemos no primeiro caso, obtemos

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1). \tag{5.7}$$

Do mesmo modo, pelo corolário 5.4.3 temos que $g(\chi_{\pi_2})^3 = p_2\pi_2$. Elevando à $(N(\pi_1) - 1)/3 = (p_1 - 1)/3$ e tomando congruências módulo π_1 obtemos

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2). \tag{5.8}$$

Em 5.3.2 vimos que $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$ e que $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$, o que implica que

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2) \tag{5.9}$$

Agora, repare que

$$\begin{aligned}
\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) && \text{(eq. 5.7 vezes } \chi_{\pi_1}(\pi_2)) \\
&= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(\pi_2 p_2) && \text{(eq. 5.9)} \\
&= \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(\pi_1 p_1\gamma_1) && \text{(eq. 5.8)} \\
&= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1).
\end{aligned}$$

Cancelando $\chi_{\pi_2}(p_1\gamma_1)$ obtemos

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

■

5.5 O anel $\mathbb{Z}[i]$

Enunciaremos, sem demonstração, as propriedades mais usuais do anel de Gauss $\mathbb{Z}[i]$. As demonstrações podem ser encontradas em textos introdutórios como [5].

Os elementos de $\mathbb{Z}[i]$ são números complexos que se escrevem, de maneira única, na forma $a+bi, a, b \in \mathbb{Z}$. Se $\alpha = a+bi \in \mathbb{Z}[i]$, então definimos a norma de α, $N(\alpha) = \alpha\overline{\alpha} = a^2+b^2$, onde $\overline{\alpha}$ é o conjugado complexo de α. O anel $\mathbb{Z}[i]$ com a norma complexa é um domínio euclideano e, consequentemente, um domínio fatorial. Do fato que $N(\alpha) = 1$ se, e somente se, α é uma unidade, segue que as unidades de $\mathbb{Z}[i]$ são $\pm 1, \pm i$.

Os irredutíveis de $\mathbb{Z}[i]$ são descritos na seguinte proposição.

Proposição 5.5.1 *Sejam p e q primos racionais. Se $p \equiv 1 \pmod 4$, então existe um irredutível $\pi \in \mathbb{Z}[i]$ tal que $p = \pi\overline{\pi}$. Se $q \equiv 3 \pmod 4$, então q é irredutível em $\mathbb{Z}[i]$. O elemento $1+i$ é irredutível e $2 = -i(1+i)^2$.*

Assim como fizemos em $\mathbb{Z}[\omega]$, vamos definir o conceito de elemento primário de $\mathbb{Z}[i]$.

Definição 5.5.2 *Se $\alpha \in \mathbb{Z}[i]$ é tal que $N(\alpha) \neq 1$ e $\alpha \equiv 1 \pmod{(1+i)^3}$, então dizemos que α é* **primário**.

O seguinte resultado dá uma caracterização dos elementos primários de $\mathbb{Z}[i]$.

Proposição 5.5.3 *Se $\alpha = a + bi$ e $N(\alpha) \neq 1$, então α é primário se, e somente se, $a \equiv 1 \pmod 4$ e $b \equiv 0 \pmod 4$, ou, $a \equiv 3 \pmod 4$ e $b \equiv 2 \pmod 4$.*

DEMONSTRAÇÃO: Como $(1+i)^3 = -2+2i$, segue que $a+bi$ é primário se, e somente se,

$$\frac{(a-1)+bi}{-2+2i} = \frac{b-a+1}{4} + \frac{-b-a+1}{4}i \in \mathbb{Z}[i].$$

O que é equivalente à dizer que $a - b \equiv 1 \pmod 4$ e $a + b \equiv 1 \pmod 4$. Resolvendo esse sistema obtemos o resultado desejado.

■

Segue da proposição acima que se α é tal que $N(\alpha) \neq 1$ e $\alpha \equiv 1 \pmod 4$, então α é primário. Ainda, se α é primário, então $(1+i) \nmid \alpha$. Se q é um primo real tal que $q \equiv 3 \pmod 4$, então $-q$ é um irredutível primário. Quanto aos irredutíveis que dividem os primos racionais da forma $p \equiv 1 \pmod 4$ temos o seguinte resultado.

Proposição 5.5.4 *Seja $\alpha \in \mathbb{Z}[i]$ tal que $N(\alpha) \neq 1$ e $(1+i) \nmid \alpha$. Então existe uma única unidade u tal que $u\alpha$ é primário.*

DEMONSTRAÇÃO: Suponha $\alpha = a + bi$. Como $(1+i) \nmid \alpha$, segue que $2 \nmid N(\alpha) = a^2 + b^2$ logo a e b não são nem ambos pares, nem ambos ímpares.

Suponha a ímpar e b par. Se $a \equiv 1 \pmod 4$, então α é primário. Se $a \equiv 3 \pmod 4$, então $-\alpha$ é primário. Caso a seja par e b ímpar, temos que $i\alpha$, ou $-i\alpha$, devem ser primários, dependendo se $b \equiv 1$, ou $3 \pmod 4$.

Se tivéssemos $u_1\alpha$ e $u_2\alpha$ primários, onde u_1 e u_2 são unidades de $\mathbb{Z}[i]$, então como $(1+i) \nmid \alpha$ temos que $u_1 \equiv u_2 \pmod{(1+i)^3}$. Analisando todos os casos concluímos que $u_1 = u_2$.

■

Agora estamos em condições de enunciar este importante resultado sobre elementos primários.

Proposição 5.5.5 *Um elemento primário α pode ser escrito como produto de primários irredutíveis.*

DEMONSTRAÇÃO: Seja $\alpha = u\pi_1\pi_2\cdots\pi_m q_{m+1}q_{m+2}\cdots q_{m+n}$ uma decomposição em irredutíveis de α, onde $N(\pi_i) \equiv 1 \pmod 4$, $i = 1, \ldots, m$, e $q_i \equiv 3 \pmod 4$, $i = m+1, \ldots, m+n$ e, $N(u) = 1$.

Tome u_i uma unidade tal que $u_i\pi_i$ seja primário e ε uma unidade tal que $\varepsilon(-1^n)\prod_{i=1}^m u_i = u$. Agora, observe que $\alpha = \varepsilon\prod_{i=1}^m u_i\pi_i\prod_{i=m+1}^{m+n}(-1)q_i$ e que $\alpha \equiv 1 \pmod{(1+i)^3} \Rightarrow \varepsilon\prod_{i=1}^m u_i\pi_i\prod_{i=m+1}^{m+n}(-1)q_i \equiv 1 \pmod{(1+i)^3}$. Como $u_i\pi_i$ e $-q_i$ são primários, temos que $\varepsilon \equiv 1 \pmod{(1+i)^3} \Rightarrow \varepsilon = 1$. Portanto, $\alpha = \prod_{i=1}^m u_i\pi_i\prod_{i=m+1}^{m+n}(-1)q_i$ é uma decomposição em irredutíveis primários.

■

Seja π um elemento irredutível de $\mathbb{Z}[i]$. Como em $\mathbb{Z}[\omega]$ temos o seguinte resultado sobre o anel $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ das classes de equivalência módulo π.

Proposição 5.5.6 *O anel $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ é um corpo finito com $N(\pi)$ elementos.*

Da proposição acima segue o pequeno teorema de Fermat para $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$.

Proposição 5.5.7 *Se $\pi \nmid \alpha$, então $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$.*

5.6 A lei de reciprocidade biquadrática

Por conveniência durante esta seção utilizaremos a seguinte notação $\left(\frac{\alpha}{\beta}\right)_4 = \chi_\beta(\alpha)$.

A lei de reciprocidade biquadrática diz que:

Teorema 5.6.1 (Lei de reciprocidade biquadrática) *Sejam λ e π elementos primários relativamente primos de $\mathbb{Z}[i]$. Então,*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{(N(\lambda-1)/4)(N(\pi)-1)/4}.$$

Vamos demonstrar a lei de reciprocidade biquadrática mais adiante nesta seção.

Seja α um elemento primário de $\mathbb{Z}[i]$. Apresentaremos agora um resultado muito útil a respeito da paridade da $N(\alpha)$.

Lema 5.6.2 *Seja $\alpha = a + bi$ primário. Então $(N(\alpha) - 1)/4$ e $(a - 1)/2$ tem a mesma paridade.*

DEMONSTRAÇÃO: Da proposição 5.5.3 segue que se $\alpha = a + bi$ é primário, então $a \equiv 1 \pmod 4$ e $b \equiv 0 \pmod 4$, ou $a \equiv 3 \pmod 4$ e $b \equiv 2 \pmod 4$. No primeiro caso temos $(a^2 - 1)/4 \equiv 0 \equiv (a - 1)/2 \pmod 2$ e $b^2/4 \equiv 0 \pmod 2$, portanto $(N(\alpha) - 1)/4 \equiv (a - 1)/2 \pmod 2$. No segundo caso temos $(a^2 - 1)/4 \equiv 0 \pmod 2$ e $b^2/4 \equiv 1 \equiv (a - 1)/2 \pmod 2$, portanto $(N(\alpha) - 1)/4 \equiv (a - 1)/2 \pmod 2$.

■

Suponha $\lambda = a + bi$ e $\pi = c + di$. Devido ao lema acima podemos reescrever a lei de reciprocidade biquadrática da seguinte forma:

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{(a-1)/2(c-1)/2}.$$

Da expressão acima é fácil ver que se π ou λ é congruente à 1 módulo 4, então $\chi_\pi(\lambda) = \chi_\lambda(\pi)$. Entretanto, se ambos são congruentes à $3 + 2i$ módulo 4 (i.e., $a, c \equiv 3 \pmod 4$ e $b, d \equiv 2 \pmod 4$), então $\chi_\pi(\lambda) = -\chi_\lambda(\pi)$.

Agora demonstraremos dois resultados sobre o caracter biquadrático das unidades.

Proposição 5.6.3 *Se $\pi = a + bi$ é um primário irredutível, então $\chi_\pi(-1) = (-1)^{(a-1)/2}$.*

DEMONSTRAÇÃO: Usando o critério de Euler e o lema 5.6.2 temos que $\chi_\pi(-1) \equiv (-1)^{(N(\pi)-1)/4} \pmod \pi \Rightarrow \chi_\pi(-1) = (-1)^{(N(\pi)-1)/4} = (-1)^{(a-1)/2}$.

■

Proposição 5.6.4 *Se $n \neq 1$ é um inteiro racional, $n \equiv 1 \pmod 4$, então $\chi_n(i) = (-1)^{(n-1)/4}$.*

DEMONSTRAÇÃO: Repare que n pode ser negativo. Se $n = p$ é um primo positivo com $p \equiv 1 \pmod 4$, então podemos escrever $p = \pi\overline{\pi}$, π irredutível em $\mathbb{Z}[i]$. Pelo critério de Euler segue que

$$\chi_p(i) = \chi_\pi(i)\chi_{\overline{\pi}}(i) \equiv (i^{(p-1)/4})^2 = (-1)^{(p-1)/4} \pmod p.$$

O que implica que $\chi_p(i) = (-1)^{(p-1)/4}$.

Se $n = -q$, $q \equiv 3 \pmod 4$ primo, então, pelo critério de Euler, $\chi_{-q}(i) = i^{(q^2-1)/4} = ((i)^{q-1})^{(q+1)/4} = (-1)^{(-q-1)/4}$. Se $n \equiv 1 \pmod 4$ é um inteiro racional arbitrário, então $n = p_1 \cdots p_r q_1 \cdots q_s$, onde $p_i \equiv 1 \pmod 4$, $i = 1, \ldots, r$, $q_j \equiv 3 \pmod 4$, $j = 1, \ldots, s$, e s é par(caso contrário teríamos $n \equiv 3 \pmod 4$). Como s é par podemos escrever

$$n = p_1 \cdots p_r(-q_1) \cdots (-q_s). \tag{5.10}$$

Usando a multiplicidade do símbolo de resíduos biquadráticos e o que analisamos acima temos que

$$\chi_n(i) = i^{\sum(p_i-1)/4 \sum(-q_i-1)/4}.$$

Demonstraremos logo abaixo a seguinte afirmação.

Afirmação: Se $u_i \equiv 1 \pmod 4$, $i = 1, \ldots, v$, então $(\prod_{i=1}^v u_i - 1)/4 \equiv \sum_{i=1}^v (u_i - 1)/4 \pmod 4$.

Da afirmação acima e de 5.10 segue que

$$(n-1)/4 \equiv \sum_{i=1}^{r}(p_i - 1)/4 \sum_{j=1}^{s}(-q_j - 1)/4 \pmod 4.$$

Sendo assim,

$$\chi_n(i) = (-1)^{\sum_{i=1}^r (p_i-1)/4 \sum_{j=1}^s (-q_j-1)/4} = (-1)^{(n-1)/4}.$$

Agora, para demonstrarmos a afirmação observe que se $u = 4k + 1$ e $t = 4l + 1$ são dois inteiros, então $(ut - 1)/4 = (16kl + 4k + 4l + 1 - 1)/4 = 4kl + k + l \equiv k + l \pmod 4$. Como $(u-1)/4 + (t-1)/4 = k + l$, concluímos que $(ut-1)/4 \equiv (u-1)/4 + (t-1)/4 \pmod 4$. Como o produto de números côngruos à 1 módulo 4 continua côngruo à 1 módulo 4, o resultado segue por indução.

■

Observamos que pelo mesmo argumento usado em 5.3.2 (b) podemos demonstrar a seguinte proposição.

Proposição 5.6.5 *Se π é um primo e α é um elemento qualquer de $\mathbb{Z}[i]$, então*

$$\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha}).$$

Nas duas proposições que seguem iremos calcular alguns casos particulares do símbolo de resíduos biquadráticos.

Proposição 5.6.6 *Seja $q \equiv 3 \pmod 4$ um primo. Se $a \in \mathbb{Z}$ e $q \nmid a$, então $\chi_q(a) = 1$.*

DEMONSTRAÇÃO: Como $N(q) = q^2$, pelo critério de Euler e pelo Pequeno Teorema de Fermat, segue que

$$\chi_q(a) \equiv a^{(q^2-1)/4} = (a^{(q-1)})^{(q+1)/4} \equiv 1 \pmod q.$$

■

Proposição 5.6.7 *Sejam $a, b \in \mathbb{Z}$ tais que a é ímpar, $a \neq 1$, e $b \neq 0$. Se $(a, b) = 1$, então*

$$\chi_a(b) = 1.$$

DEMONSTRAÇÃO: Assuma $a > 0$. Escreva $a = \prod p_i \prod q_i$, onde, p_i e q_i são primos, $p_i \equiv 1 \pmod 4$ e $q_i \equiv 3 \pmod 4$. Devido à proposição 5.6.6 apenas resta verificar que $\chi_{p_i}(b) = 1$. Se $p_i = \pi\overline{\pi}$, π irredutível de $\mathbb{Z}[i]$, então $\chi_{p_i}(b) = \chi_\pi(b)\chi_{\overline{\pi}}(b) = \chi_\pi(b)\overline{\chi_\pi(b)} = 1$ pela proposição 5.6.5.

■

Na próxima seção desenvolveremos uma série de resultados que culminarão na demonstração da lei de reciprocidade biquadrática.

5.7 Demonstração da lei de reciprocidade biquadrática

Nesta seção desenvolveremos uma série de resultados que culminarão na demonstração da lei de reciprocidade cúbica. Para isto reservamos a notação π e λ para elementos primários de $\mathbb{Z}[i]$. A menos que seja dito o contrário π denota um elemento irredutível.

Suponha $N(\pi) = p \equiv 1 \pmod 4$ e seja χ_π o caracter de resíduos biquadráticos associado. Como $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ é um corpo finito com p elementos ele é isomorfo à $\mathbb{Z}/p\mathbb{Z} = F_p$ e podemos considerar χ_π como um caracter multiplicativo sobre F_p. Se $\zeta = e^{(2i\pi)/p}$ seja $g(\chi_\pi) = \sum_{j\in F_p} \chi_\pi(j)\zeta^j$ a soma de Gauss associada à χ_π. Se $\psi = \chi_\pi^2$ então ψ é o caracter multiplicativo não trivial de ordem 2 sobre F_p e portanto é o símbolo de Legendre. Lembramos ainda que $J(\chi_\pi, \chi_\pi)$ é a soma de Jacobi determinada por χ_π.

Proposição 5.7.1 *Usando as notações descritas acima tem-se*

$$J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)J(\chi_\pi, \psi).$$

DEMONSTRAÇÃO: Pela proposição 4.3.2 temos que $J(\chi_\pi, \chi_\pi) = g(\chi_\pi)^2/g(\psi)$. Portanto,

$$J(\chi_\pi, \chi_\pi)^2 = \frac{g(\chi_\pi)^4}{g(\psi)^2}.$$

Pela proposição 4.3.4 temos que $g(\chi_\pi)^4 = \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi_\pi, \psi)$ e pelo coroláro 4.2.5 $g(\psi)^2 = (-1)^{(p-1)/2}p = p$. Assim, a equação acima implica que

$$J(\chi_\pi, \chi_\pi)^2 = \chi_\pi(-1)J(\chi_\pi, \chi_\pi)J(\chi_\pi, \psi).$$

E cancelando $J(\chi_\pi, \chi_\pi)$ obtemos

$$J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)J(\chi_\pi, \psi).$$

■

Proposição 5.7.2 *Em relação à soma de Gauss tem-se*

$$g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi).$$

DEMONSTRAÇÃO: Na demonstração da proposição acima vimos que

$$g(\chi_\pi)^4 = J(\chi_\pi, \chi_\pi)^2 g(\psi)^2.$$

Pelo corolário 4.2.5 $g(\psi)^2 = (-1)^{(p-1)/2}p = p$. Substituindo na equação acima obtemos o resultado desejado.

■

Proposição 5.7.3 *O elemento* $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ *é primário.*

DEMONSTRAÇÃO: Mostraremos que $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) \equiv 1 \pmod{2+2i}$, o que é suficiente uma vez que $2 + 2i = (1 + i)^3(-i)$.

Pela definição de somas de Jacobi (4.3.1) temos que $J(\chi_\pi, \chi_\pi) = \sum_{t=2}^{p-1} \chi_\pi(t)$ $\chi_\pi(1-t)$. Observamos que o termo do somatório associado à $t = (p+1)/2$ é $\chi_\pi((p+1)/2)\chi_\pi(1-(p+1)/2) = \chi_\pi((p+1)/2)^2$. Também observamos que para todo $t \neq (p+1)/2$, o termo do somatório referente ao índice t e ao índice $p+(1-t)$ são iguais, i.e., $\chi_\pi(t)\chi_\pi(1-t) = \chi_\pi(p+(1-t))\chi_\pi(1-(p+(1-t)))$. Sendo assim podemos escrever

$$J(\chi_\pi, \chi_\pi) = 2\sum_{t=2}^{(p-1)/2} \chi_\pi(t)\chi_\pi(1-t) + \chi_\pi\left(\frac{p+1}{2}\right)^2.$$

Agora, faremos três observações acerca de resíduos módulo $2 + 2i$.

(1) $2\varepsilon \equiv 2 \pmod{2+2i}$, *onde* ε *é uma unidade qualquer de* $\mathbb{Z}[i]$.

De fato, se $\varepsilon = 1$ nada temos a fazer; se $\varepsilon = -1$, basta observarmos que $(2 + 2i)(1 - i) = 4$; se $\varepsilon = i$, basta observarmos que $(2 + 2i)i = 2i - 2$; e se $\varepsilon = -i$ nada temos a fazer.

(2) $p \equiv 1 \pmod{2+2i}$.

Como $p \equiv 1 \pmod 4$ e $(2 + 2i) \mid 4$ a observação segue.

(3) $\chi_\pi((p+1)/2)^2 = \chi_\pi(-1)$.

Como $(p+1)/2 \equiv 1/2 \pmod p$, temos que $\chi_\pi((p+1)/2)^2 = \chi_\pi((2)^{-1})^2 = \chi_\pi(2)^{-2}$. Uma vez que $\chi_\pi(2) = 1, -1, i, ou - i$, temos que $\chi_\pi(2)^2 = 1, ou - 1$, e portanto, $\chi_\pi((p+1)/2)^2 = \chi_\pi(2)^{-2} = \chi_\pi(2)^2$. Como $2 = -i(1+i)^2$, temos que $\chi_\pi((p+1)/2)^2 = \chi_\pi(-i(1+i)^2)^2 = \chi_\pi(-i)^2\chi_\pi((1+i)^2)^2 = \chi_\pi(-i)^2 = \chi_\pi(-1)$.

De (1) e (2) segue que $2\sum_{t=2}^{(p-1)/2}\chi_\pi(t)\chi_\pi(1-t) \equiv 2(p-3)/2 \equiv -2 \pmod{2+2i}$. Portanto, usando (3) temos

$$J(\chi_\pi,\chi_\pi) \equiv -2+\chi_\pi(-1) \pmod{2+2i}.$$

Da proposição 5.6.3 temos que $\chi_\pi(-1) = \pm 1$. Logo,

$$\chi_\pi(-1)J(\chi_\pi,\chi_\pi) \equiv -2+\chi_\pi(-1) \pmod{2+2i}.$$

Novamente por (1) acima temos que

$$\chi_\pi(-1)J(\chi_\pi,\chi_\pi) \equiv 1 \pmod{2+2i}.$$

■

Vamos agora encontrar o valor de $-\chi_\pi(-1)J(\chi_\pi,\chi_\pi)$.

Proposição 5.7.4 *Dado o elemento irredutível π tem-se que*

$$-\chi_\pi(-1)J(\chi_\pi,\chi_\pi) = \pi.$$

DEMONSTRAÇÃO: Pela proposição 5.5.4 vemos que é suficiente mostrar que $J(\chi_\pi,\chi_\pi)$ e π diferem por uma unidade uma vez que ambos são primários.

Pelo corolário 4.3.3, temos que $N(J(\chi_\pi,\chi_\pi)) = p$, e portanto $J(\chi_\pi,\chi_\pi)$ é irredutível. Mas, $J(\chi_\pi,\chi_\pi) \equiv \sum_{t=1}^{p-1} t^{(p-1)/4}(1-t)^{(p-1)/4} \pmod{\pi}$ (pelo critério de Euler) e assim da proposição 5.5.4 segue que $J(\chi_\pi,\chi_\pi) \equiv 0 \pmod{\pi}$. Logo $J(\chi_\pi,\chi_\pi)$ e π diferem por uma unidade e o resultado segue.

■

Estamos agora em posição de exibir a fatoração de $g(\chi_\pi)^4$.

Proposição 5.7.5 *A fatoração de $g(\chi_\pi)^4$ é dada por $g(\chi_\pi)^4 = \pi^3\overline{\pi}$.*

DEMONSTRAÇÃO: Pela proposição 5.7.2 temos que $g(\chi_\pi)^4 = pJ(\chi_\pi,\chi_\pi)^2$. Usando o fato que $\chi_\pi(-1) = \pm$, pela proposição 5.7.4 segue que $g(\chi_\pi)^4 = \pi\overline{\pi}\pi^2$.

■

Agora vamos demonstrar dois casos particulares da lei de reciprocidade biquadrática.

Proposição 5.7.6 *Seja $q > 0$ um irredutível racional em $\mathbb{Z}[i]$. Então*

$$\chi_\pi(-q) = \chi_q(\pi).$$

DEMONSTRAÇÃO: Como $q \equiv 3 \pmod 4$ e χ_π tem ordem 4 temos que $\chi_\pi^q = \chi_\pi^3 = \chi_\pi^{-1} = \overline{\chi_\pi}$. Segue que

$$g(\chi_\pi)^q \equiv \sum_{j=1}^{p-1} \chi_\pi(j)^q \zeta^{qj} \equiv \sum_{j=1}^{p-1} \overline{\chi_\pi(j)} \zeta^{qj} = g_q(\overline{\chi_\pi}) \pmod q.$$

Pelo corolário 4.2.5 e pela proposição 4.2.2 temos que $g_q(\overline{\chi_\pi}) = \overline{\chi_\pi(q^{-1})} g(\overline{\chi_\pi})$. Mas, pela proposição 4.1.3 $\overline{\chi_\pi(q)^{-1}} = \chi_\pi(q)$. Sendo assim, a equação acima implica que

$$g(\chi_\pi)^q \equiv \chi_\pi(q) g(\overline{\chi_\pi}) \pmod q.$$

Por um lado temos que

$$(g(\chi_\pi)^4)^{(q+1)/4} = g(\chi_\pi)^{q+1} \equiv \chi_\pi(q) g(\chi_\pi) g(\overline{\chi_\pi}) \pmod q.$$

Pela proposição 5.7.5 temos que $(g(\chi_\pi)^4)^{(q+1)/4} = (\pi^3 \overline{\pi})^{(q+1)/4}$. Assim,

$$(\pi^3 \overline{\pi})^{(q+1)/4} \equiv \chi_\pi(q) g(\chi_\pi) g(\overline{\chi_\pi}) \pmod q.$$

Agora, observe que $\pi^q = (a + bi)^q \equiv a^q + b^q i^q \equiv a - bi = \overline{\pi} \pmod q$. Portanto,

$$\pi^{[(q+3)(q+1)]/4} \equiv \chi_\pi(q) g(\chi_\pi) g(\overline{\chi_\pi}) \pmod q.$$

Pelo corolário 4.2.5 $\overline{g(\chi_\pi)} = \chi_\pi(-1) g(\overline{\chi_\pi})$ e pela proposição 4.2.4 $N(g(\chi_\pi)) = p = \pi\overline{\pi}$. Com essas considerações, e com a observação que fizemos acima que $\pi^q \equiv \overline{\pi} \pmod q$, temos que

$$\pi^{[(q+3)(q+1)]/4} \equiv \chi_\pi(-1) \chi_\pi(q) \pi^{q+1} \pmod q.$$

o que implica que

$$\pi^{(q^2-1)/4} \equiv \chi_\pi(-q) \pmod q.$$

Mas, pelo critério de Euler, $\pi^{(q^2-1)/4} \equiv \chi_q(\pi) \pmod q$, logo

$$\chi_q(\pi) \equiv \chi_\pi(-q) \pmod q.$$

E, finalmente, como ambos os lados são raízes biquadráticas da unidade, pela proposição 2.2.3, temos que

$$\chi_q(\pi) = \chi_\pi(-q).$$

■

Como $-q$ é primário e $(N(q)-1)/4 = (q^2-1)/4$ é par, segue que a proposição acima é de fato um caso particular da lei de reciprocidade biquadrática.

Proposição 5.7.7 *Seja q um primo, $q \equiv 1 \pmod 4$. Então*

$$\chi_\pi(q) = \chi_q(\pi).$$

DEMONSTRAÇÃO: Como $q \equiv 1 \pmod 4$ e χ_π tem ordem 4, segue que $\chi_\pi^q = \chi_\pi$. Como pela proposição 4.2.2 e pela proposição 4.1.3 $g_q(\chi_\pi) = \chi_\pi(q^{-1})g(\chi_\pi) = \overline{\chi_\pi(q)}g(\chi_\pi)$ segue que

$$g(\chi_\pi)^q \equiv \sum_{j=1}^{p-1} \chi_\pi(j)^q \zeta^{qj} \equiv \sum_{j=1}^{p-1} \chi_\pi(j)\zeta^{qj} \equiv \overline{\chi_\pi(q)}g(\chi_\pi) \pmod q.$$

Multiplicando por $g(\chi_\pi)^3$ temos

$$g(\chi_\pi)^{q+3} \equiv \overline{\chi_\pi(q)}g(\chi)^4 \pmod q.$$

Agora, pela proposição 5.7.5, segue que

$$(\pi^3\overline{\pi})^{(q+3)/4} \equiv \overline{\chi_\pi(q)}\pi^3\overline{\pi} \pmod q.$$

Como ambos os lados da congruência acima pertencem à $\mathbb{Z}[i]$ e $(q,\pi) = (q,\overline{\pi}) = 1$, dividindo por $\pi^3\overline{\pi}$, obtemos

$$(\pi^3\overline{\pi})^{(q-1)/4} \equiv \overline{\chi_\pi(q)} \pmod q.$$

Se $q = \lambda\overline{\lambda}$, λ irredutível em $\mathbb{Z}[i]$, então pelo critério de Euler segue que

$$\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) \equiv \overline{\chi_\pi(q)} \pmod{(\lambda)}.$$

Como ambos os lados são raízes biquadráticas da unidade segue que

$$\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi(q)}$$

Usando o fato que $\chi_\lambda(\pi^3) = \chi_\lambda(\pi)^3 = \chi_\lambda(\pi)^{-1} = \overline{\chi_\lambda(\pi)}$ e a proposição 5.6.5, temos

$$\overline{\chi_\pi(q)} = \overline{\chi_\lambda(\pi)}\chi_\lambda(\overline{\pi}) = \chi_{\overline{\lambda}}(\overline{\pi})\chi_\lambda(\overline{\pi}) = \chi_q(\overline{\pi}).$$

Tomando os conjugados dos dois lados e usando novamente a proposição 5.6.5 segue que

$$\chi_\pi(q) = \chi_q(\pi).$$

■

Proposição 5.7.8 *Seja a um inteiro racional tal que $a \equiv 1 \pmod 4$ e λ primário (não necessariamente irredutível) tal que $(a, \lambda) = 1$. Então*

$$\chi_a(\lambda) = \chi_\lambda(a).$$

DEMONSTRAÇÃO: Suponha $a = \prod p_i \prod q_i$, onde p_i e q_i são primos racionais tais que $p_i \equiv 1 \pmod 4$ e $q_i \equiv 3 \pmod 4$. Sabemos que como $a \equiv 1 \pmod 4$ os $q_i s$ devem aparecer em uma quantidade par.

Pela proposição 5.5.5 e pela bimultiplicidade do símbolo de resíduos biquadráticos podemos supor λ irredutível.

Por sucessivas aplicações das proposições 5.7.6 e 5.7.7 temos que

$$\prod \chi_{p_i}(\lambda) \prod \chi_{q_i}(\lambda) = \prod \chi_\lambda(p_i) \prod \chi_\lambda(-q_i).$$

Novamente pela dupla multiplicidade do símbolo de resíduos biquadráticos e pelo fato de termos uma quantidade par de $q_i s$ segue que

$$\chi_a(\lambda) = \chi_\lambda(a).$$

■

Proposição 5.7.9 *Suponha que $\pi = a + bi$ e $\lambda = c + di$ sejam elementos primários não necessariamente irredutíveis, primos entre si. Se $(a, b) = 1$ e $(c, d) = 1$, então*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{(a-1)/2(c-1)/2}.$$

DEMONSTRAÇÃO: Das hipóteses segue que $(a,\pi)=(b,\pi)=(c,\lambda)=(d,\lambda)=1$. Como $(c,\lambda)=1$ temos que $\lambda bi = bci - bd \Rightarrow bi \equiv bdc^{-1} \pmod{\lambda} \Rightarrow a+b \equiv a+bdc^{-1} \pmod{\lambda} \Rightarrow c\pi \equiv ca+bd \pmod{\lambda}$.

A relação $c\pi \equiv ca+bd \pmod{\lambda}$ implica que $(ac+bd,\lambda)=(ac+bd,\pi)=1$. Portanto,

$$\chi_\lambda(c)\chi_\lambda(\pi) = \chi_\lambda(ac-bd). \tag{5.11}$$

e da mesma forma

$$\chi_\pi(a)\chi_\pi(\lambda) = \chi_\pi(ac-bd). \tag{5.12}$$

Tomando o conjugado de 5.12, multiplicando por 5.11 e usando a proposição 5.6.5 obtemos

$$\chi_\lambda(c)\chi_{\overline{\pi}}(a)\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\lambda\overline{\pi}}(ac+bd).$$

Usando o fato que $\chi^{-1} = \overline{\chi}$ para um caracter multiplicativo χ qualquer e, novamente, a proposição 5.6.5 obtemos

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\overline{\lambda}}\chi_\pi(a)\chi_{\lambda\overline{\pi}}(ac+bd). \tag{5.13}$$

Assuma que c, a, e $ac+bd$ não sejam unidades. Para um inteiro ímpar n defina $\varepsilon(n) = (-1)(n-1)/2$. Então, $\varepsilon(n)n \equiv 1 \pmod{4}$. De fato, se $n \equiv 1 \pmod{4}$, então $\varepsilon(n)=1$, e, se $n \equiv -1 \pmod{4}$, então $\varepsilon(n)=-1$ e, portanto, $\varepsilon(n)n \equiv (-1)(-1) = 1 \pmod{4}$. Temos também que $\varepsilon(ac+bd) = \varepsilon(a)\varepsilon(c)$. De fato, como λ e π são primários temos que b e $d \equiv 0$, ou $2 \pmod{4}$, e, portanto, $bd \equiv 0 \pmod{4}$. Então, nos resta verificar que $\varepsilon(ac) = \varepsilon(a)\varepsilon(c)$, o que segue se verificarmos os três casos possíveis, quais sejam, $a \equiv 1 \pmod{4}$ e $c \equiv 1 \pmod{4}$, $a \equiv 1 \pmod{4}$ e $c \equiv 3 \pmod{4}$, e, $a \equiv 3 \pmod{4}$ e $c \equiv 3 \pmod{4}$.

Observamos também que $\chi_\alpha(x) = \chi_\alpha(\varepsilon(x))\chi_\alpha(\varepsilon(x)x)$, e que, como $\varepsilon(x) = \pm 1$, pelo critério de Euler, $\chi_\alpha(\varepsilon(x)) = \pm 1$, o que impica que $\chi_{\overline{\alpha}}(\varepsilon(x)) = \overline{\chi_\alpha(\varepsilon(x))} = \chi_\alpha(\varepsilon(x))$.

Agora, usando as proposições 5.7.8 e 5.6.3, e o fato que $\varepsilon(x)^2 = 1$ podemos calcular o lado esquerdo da equação 5.13.

$$\begin{aligned}
\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} &= \varepsilon(a)^2\varepsilon(c)^2\chi_{\overline{\lambda}}(\varepsilon(c)c)\chi_\pi(\varepsilon(a)a)\chi_{\lambda\overline{\pi}}(\varepsilon(ac+bd)ac+bd) \\
&= \chi_\lambda(\varepsilon(c)^2)\chi_\pi(\varepsilon(a)^2)\chi_\lambda(\varepsilon(a))\chi_\pi(\varepsilon(a))\chi_c(\overline{\lambda})\chi_a(\overline{\pi})\chi_{ac+bd}(\lambda\overline{\pi}) \\
&= (-1)^{((a-1)/2(c-1)/2)2}\chi_c(\overline{\lambda})\chi_a(\pi)\chi_{ac+bd}(\lambda\overline{\pi}) \\
&= \chi_c(\overline{\lambda})\chi_a(\pi)\chi_{ac+bd}(\lambda\overline{\pi}).
\end{aligned} \tag{5.14}$$

Usando a proposição 5.6.7 e o fato que $\chi_\alpha(x) = \chi_\alpha(y)$ se $x \equiv y \pmod{\alpha}$ (segue da proposição 3.2.6) podemos calcular os três termos do lado direito da equação 5.14.

$$\begin{aligned}\chi_c(\overline{\lambda}) &= \chi_c(c - di) = \chi_c(-di) = \chi_c(i),\\ \chi_a(\pi) &= \chi_a(a + bi) = \chi_a(bi) = \chi_a(i),\\ \chi_{ac+bd}(\overline{\pi}\lambda) &= \chi_{ac+bd}((ad - bc)i) = \chi_{ac+bd}(i).\end{aligned}$$

Portanto temos a seguinte relação

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{(ac+bd)ac}(i).$$

Como $ac \equiv 1, \text{ou, } 3 \pmod 4$ e $bd \equiv 0 \pmod 4$ temos que $(ac+bd)ac \equiv 1 \pmod 4$. Sendo assim podemos usar a proposição 5.6.4 obtendo

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = (-1)^{((ac+bd)ac-1)/4}.$$

Se verificarmos todos os casos possíveis para os valores de a, b, c e d explicitados na proposição 5.5.3 concluímos que $(-1)^{((ac+bd)ac-1)/4} = (-1)^{(a-1)/2(c-1)/2}$. Portanto

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = (-1)^{(a-1)/2(c-1)/2}.$$

Como queríamos.

Quando $a, c,$ ou $ac+bd$ são unidades basta adaptarmos o mesmo raciocínio usado acima.

■

Estamos agora em posição de demonstrar a lei de reciprocidade biquadrática. Vamos enunciar novamente o teorema.

Teorema 5.7.10 (Lei de reciprocidade biquadrática) *Sejam λ e π elementos primários relativamente primos de $\mathbb{Z}[i]$. Então,*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{(N(\lambda-1)/4)(N(\pi)-1)/4}.$$

DEMONSTRAÇÃO: Para usarmos a proposição 5.7.9 considere $\pi = m(a + bi)$ e $\lambda = n(c + di)$, onde $(a, b) = 1$, $(c, d) = 1$ e $m, n \equiv 1 \pmod 4$. Observe que como π e λ são primários segue que existe uma decomposição tal que m e n são primários, assim $m, n \equiv 1 \pmod{2(-1 + i)^3}$, o que implica que $m, n \equiv 1 \pmod 4$.

Pela proposição 5.7.8 temos que $\chi_\pi(n) = \chi_n(\pi)$ e $\chi_\lambda(m) = \chi_m(\lambda)$. Temos também que pela proposição 5.6.7 $\chi_m(n) = \chi_n(m) = 1$. Como, $a+bi$ e $c+di$ são primários segue que

$$\begin{aligned}
\chi_\lambda(\pi) &= \chi_\lambda(a+bi) \\
&= \chi_m(\lambda)\chi_n(a+bi)\chi_{c+di}(a+bi) \\
&= \chi_m(\lambda)\chi_{a+bi}(n)\chi_{a+bi}(c+di)(-1)^{(a-1)/2(c-1)/2} \\
&= \chi_\pi(\lambda)(-1)^{(a-1)/2(c-1)/2}.
\end{aligned}$$

Como $m, n \equiv 1 \pmod 4$, segue que $(N(\pi)-1)/4 = (N(m)N(a+bi)-1)/4 \equiv (N(a+bi)-1)/4 \pmod 4$, e, da mesma forma $(N(\lambda)-1)/4 \equiv (N(c+di)-1)/4 \pmod 4$. Pelo lema 5.6.2 temos $(-1)^{(N(\pi)-1)/4(N(\lambda-1))/4} = (-1)^{(a-1)/2(b-1)/2}$. Sendo assim segue que

$$\chi_\lambda(\pi) = \chi_\pi(\lambda)(-1)^{(N(\pi)-1)/4(N(\lambda-1))/4}$$

■

Capítulo 6

Leis de reciprocidade racionais

Nosso objetivo neste capítulo é expor um método devido à Charles Helou [4] que deduz uma lei de reciprocidade racional m - ésima sempre que uma lei de reciprocidade m - ésima em $\mathbb{Z}[\zeta_m]$ é dada, onde ζ_m é uma raiz primitiva m - ésima da unidade. Aplicaremos este método aos casos $m = 3$ e 4 obtendo resultados devidos à von Lienen [7] e Burde [1].

6.1 O fator de inversão racional

Seja $m > 1$ um número natural. Sejam p e q primos racionais distintos tais que $p, q \equiv 1 \pmod{m}$. Sejam ζ_m a m - ésima raíz da unidade e $D_m = \mathbb{Z}[\zeta_m]$ o anel de inteiros de $\mathbb{Q}(\zeta_m)$. Segue da proposição 2.2.7 que se $p \equiv 1 \pmod{m}$, então a decomposição primária de (p) é da forma $(p) = P_1 P_2 \cdots P_{\phi(m)}$, onde ϕ é a função de Euler e os primos P_i, $i = 1, \ldots, \phi(m)$ são todos distintos e de grau de inércia 1. Em outras palavras, (p) se decompõem completamente (ver definição 2.1.19) em D_m.

Tome $P = P_i$ para algum i. Como P tem grau de inércia 1, segue que $N(P) = p$. Suponha que π e υ sejam elementos primos de D_m tais que $N(\pi) = p$ e $N(\upsilon) = q$. Assim, $D_m/(\pi) \approx \mathbb{Z}_p$. Devido à este isomorfismo existe um inteiro racional z satisfazendo $z \equiv \zeta_m \pmod{\pi}$, e z é único módulo p.

Apresentaremos agora uma importante definição.

Definição 6.1.1 *O m -ésimo fator de inversão racional de p e q, $\rho_m(p,q)$, é definido por*

$$\rho_m(p,q) = \left(\frac{p}{\upsilon}\right)_m \left(\frac{q}{\pi}\right)_m^{-1}.$$

Entendemos por lei de reciprocidade racional uma relação de reciprocidade entre caracteres de dois primos ímpares racionais que dependa unicamente de tais primos. Nossa definição é a mesma usada em [4]. Esta definição é mais geral do que a usada em [6], onde a autora exige também que o produto dos caracteres seja ± 1. Na proposição a seguir mostraremos que o valor de $\left(\frac{p}{\upsilon}\right)_m$ (respectivamente $\left(\frac{q}{\pi}\right)_m$) depende apenas de p e q, e não da escolha do irredutível υ (respectivamente π). Sendo assim, uma expressão para $\rho_m(p,q)$ pode ser chamada uma lei de reciprocidade racional m - ésima.

Proposição 6.1.2 *Com p e υ nas condições acima temos que $\left(\frac{p}{\upsilon}\right)_m = 1$ se, e somente se, $x^m \equiv p \pmod{q}$ para algum $x \in \mathbb{Z}$.*

Demonstração: Como $D_m/(\upsilon) \approx \mathbb{Z}_q$, temos que os inteiros $0, 1, \ldots, q-1$ formam um sistema completo de resíduos para as classes de resíduos de D_m módulo υ. Portanto $\left(\frac{p}{\upsilon}\right)_m = 1$ se, e somente se, $x^m \equiv p \pmod{\upsilon}$ para algum $x \in \mathbb{Z}$. Como para todo σ no grupo de Galois, G, de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ tem-se que $\sigma(x) = x$ e $\sigma(p) = p$, segue que, para qualquer tal σ, $x^m \equiv p \pmod{\sigma(\upsilon)}$. Uma vez que os conjugados de υ são elementos primos de D_m e não são associados dois a dois, podemos concluir que $q = N(\upsilon) \mid x^m - p$.

■

Se conhecemos uma lei de reciprocidade m - ésima em D_m, então temos uma expressão para $\left(\frac{a}{b}\right)_m \left(\frac{b}{a}\right)_m^{-1}$, onde $a, b \in D_m$, $a, b \notin (m)$, $a \notin (b)$ e $b \notin (a)$.

Definição 6.1.3 *Nas condições acima definimos o símbolo $e_m(a,b)$ pela expressão*

$$e_m(a,b) = \left(\frac{a}{b}\right)_m \left(\frac{b}{a}\right)_m^{-1}.$$

Daremos agora uma expressão para $\rho_m(p,q)$ que usa $e_m(p,\upsilon)$.

Teorema 6.1.4 *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio tal que $f(\zeta_m) = \upsilon$. Seja z um inteiro racional tal que $z \equiv \zeta_m \pmod{\pi}$. Então*

$$\rho_m(p,q) = e_m(p,\upsilon)\left(\frac{s}{\pi}\right)_m,$$

onde, s é um inteiro racional tal que

$$s \equiv \prod_k f(\zeta_m^k)^{k'-1} \pmod{p},$$

com k percorrendo um conjunto positivo de representantes de ${\mathbb{Z}_m}^*$, e k' um inteiro positivo tal que $kk' \equiv 1 \pmod{m}$.

DEMONSTRAÇÃO: Começaremos fazendo uma série de observações.

Seja G o grupo de Galois de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Pela proposição 2.1.3 temos que $p = \prod_{\sigma\in G}\sigma(\pi)$ e que $q = \prod_{\sigma\in G}\sigma(\upsilon)$. Assim, segue que

$$\rho_m(p,q) = \left(\frac{p}{\upsilon}\right)_m\left(\frac{q}{\pi}\right)_m^{-1} = \prod_{\sigma\in G}\left(\frac{\sigma(\pi)}{\upsilon}\right)_m\left(\frac{\sigma(\upsilon)}{\pi}\right)_m^{-1}. \tag{6.1}$$

Temos também que

$$\left(\frac{\sigma(\pi)}{\upsilon}\right)_m\left(\frac{\sigma(\upsilon)}{\pi}\right)_m^{-1} = e_m(\sigma(\pi),\upsilon)\left(\frac{\upsilon}{\sigma(\pi)}\right)_m\left(\frac{\sigma(\upsilon)}{\pi}\right)_m^{-1}. \tag{6.2}$$

Agora, pela proposição 3.2.10, temos que

$$\left(\frac{\upsilon}{\sigma(\pi)}\right)_m = \sigma\left(\frac{\sigma^{-1}(\upsilon)}{\pi}\right)_m$$

E, pela proposição 2.2.6, temos que para todo $\sigma \in G$ existe $k \in {\mathbb{Z}_m}^*$ tal que $\sigma(\zeta_m) = \sigma_k(\zeta_m) = \zeta_m^k$. Segue que $\sigma_k(\upsilon) = \sigma_k(f(\zeta_m)) = f(\zeta_m^k) \equiv f(z^k) \pmod{\pi}$. Como $\sigma_k^{-1} = \sigma_{k'}$, temos que $\sigma_k^{-1}(\upsilon) \equiv f(z^{k'}) \pmod{\pi}$. Usando estas considerações na equação acima, mais o fato que $a \equiv b \pmod{\pi}$ implica em $\left(\frac{a}{\pi}\right)_m = \left(\frac{b}{\pi}\right)_m$, obtemos

$$\left(\frac{\upsilon}{\sigma_k(\pi)}\right)_m = \sigma_k\left(\frac{\sigma_{k'}(\upsilon)}{\pi}\right)_m = \sigma_k\left(\frac{f(z^{k'})}{\pi}\right)_m = \left(\frac{f(z^{k'})}{\pi}\right)_m^k,$$

e também

$$\left(\frac{\sigma_k(\upsilon)}{\pi}\right)_m^{-1} = \left(\frac{f(z^k)}{\pi}\right)_m^{-1}.$$

Logo,

$$\left(\frac{\upsilon}{\sigma_k(\pi)}\right)_m \left(\frac{\sigma_k(\upsilon)}{\pi}\right)_m^{-1} = \left(\frac{f(z^{k'})}{\pi}\right)_m^k \left(\frac{f(z^k)}{\pi}\right)_m^{-1}.$$

Substituindo a última equação na equação 6.2 obtemos

$$\left(\frac{\sigma_k(\pi)}{\upsilon}\right)_m \left(\frac{\sigma_k(\upsilon)}{\pi}\right)_m^{-1} = e_m(\sigma_k(\pi), \upsilon)\left(\frac{f(z^{k'})}{\pi}\right)_m^k \left(\frac{f(z^k)}{\pi}\right)_m^{-1}.$$

Usando a bimultiplicidade de $e_m(,)$ e substituindo o resultado acima na equação 6.1 temos

$$\left(\frac{p}{\upsilon}\right)_m \left(\frac{q}{\pi}\right)_m^{-1} = e_m(p, \upsilon)\prod_k \left(\frac{f(z^{k'})^k}{\pi}\right)_m \prod_k \left(\frac{f(z^k)^{m-1}}{\pi}\right)_m,$$

onde $k \in {\mathbb{Z}_m}^*$. Observe que $\prod_k (f(z^{k'})^k/\pi)_m = \prod_k (f(z^k)^{k'}/\pi)_m$, o que implica

$$\left(\frac{p}{\upsilon}\right)_m \left(\frac{q}{\pi}\right)_m^{-1} = e_m(p, \upsilon)\prod_k \left(\frac{f(z^k)^{k'+m-1}}{\pi}\right)_m.$$

E cortando m do expoente, uma vez que o símbolo de resíduos m - ésimos é uma raíz m - ésima da unidade, obtemos a igualdade desejada.

■

6.2 Aplicações

Agora aplicaremos o teorema 6.1.4 para calcularmos os casos em que $m = 3$ e $m = 4$, obtendo teoremas devido à von Lienen [7] e Burde [1]. No que segue, usaremos a mesma notação do teorema 6.1.4, a saber, ζ_m é uma raíz m - ésima primitiva da unidade, $f(x) \in \mathbb{Z}[x]$ é um polinômio tal que $f(\zeta_m) = \upsilon$, z é um inteiro racional tal que $z \equiv \zeta_m \pmod{\pi}$, e s é um inteiro racional tal que $s \equiv \prod_k f(\zeta_m^k)^{k'-1} \pmod{p}$, com k percorrendo um conjunto positivo de representantes de ${\mathbb{Z}_m}^*$, e k' um inteiro positivo tal que $kk' \equiv 1 \pmod{m}$. Para sermos coerentes com a notação que usamos até agora usaremos $\zeta_3 = \omega$ e $\zeta_4 = i$.

Proposição 6.2.1 (von Lienen) *Seja ω uma raíz cúbica primitiva da unidade. Sejam $p, q \equiv 1 \pmod 3$ primos racionais. Sejam $\pi = a + b\omega$ e $\upsilon = c + d\omega$ primos primários de $\mathbb{Z}[\omega]$ tais que $N(\pi) = p$ e $N(\upsilon) = q$, onde a, b, c e $d \in \mathbb{Z}$. Então*

$$\rho_3(p, q) = \left(\frac{a^2(ac - bd)}{\pi}\right)_3.$$

DEMONSTRAÇÃO: Observamos que $p = a^2 - ab + b^2$ implica que $(p, a) = (p, b) = 1$. Seja b' o inverso de b módulo p. Como $\pi = a + b\omega \equiv 0 \pmod \pi$, temos que $z \equiv -ab' \pmod p$ (devido ao isomorfismo entre $D_m/\pi D_m$ e $\mathbb{Z}_p$).

Pela lei de reciprocidade cúbica (página 39) temos que $\left(\frac{\pi}{\upsilon}\right)_3 \left(\frac{\upsilon}{\pi}\right)_3^{-1} = 1$, logo $e_m(p, \upsilon) = e_m(\pi, \upsilon) e_m(\overline{\pi}, \upsilon) = 1$.

Calculando s, com $k \in \mathbb{Z}_3^*$, obtemos $s \equiv f(z^2) \pmod p$. Seja $f(\omega) = c + d\omega = \upsilon$. Observe que $\omega^2 \equiv z^2 \pmod p$ implica que $z^2 \equiv z' \pmod p$ e, portanto, $z^2 \equiv -a'b \pmod p$. Assim, $f(z^2) \equiv c - da'b \pmod \pi$. Portanto, aplicando o teorema 6.1.4, obtemos

$$\rho_3(p, q) = \left(\frac{c - da'b}{\pi}\right)_3.$$

Agora, basta observarmos que pelas proposições 4.1.3 (c) e 5.3.2 (a) segue que $\left(\frac{a'}{\pi}\right)_3 = \left(\frac{a^2}{\pi}\right)_3$. Portanto

$$\rho_3(p, q) = \left(\frac{a^2(ac - db)}{\pi}\right)_3.$$

■

Para aplicarmos o teorema 6.1.4 para o caso $m = 4$ precisaremos do lema que vem a seguir, mas antes fixaremos algumas notações. Dado um divisor n de m, denotaremos por N_n a norma relativa à extensão $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_n)$ e N a norma relativa à extensão $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, onde ζ_m é uma raiz primitiva m - ésima da unidade e ζ_n é uma raiz primitiva n - ésima da unidade.

Lema 6.2.2 *Sejam $p \equiv 1 \pmod m$ um primo racional e π um primo de $D_m = \mathbb{Z}[\zeta_m]$ tal que $N(\pi) = p$. Suponha que $d \mid m$. Sejam $n = m/d$ e $D_n = \mathbb{Z}[\zeta_n]$. Se $a \in D_n$, então*

$$\left(\frac{a}{\pi}\right)_m^d = \left(\frac{a}{N_n(\pi)}\right)_n.$$

DEMONSTRAÇÃO: Seja G o grupo de Galois da extensão $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_n)$. Se $\pi \mid a$, então para qualquer $\sigma \in G$ temos que $\sigma(\pi) \mid \sigma(a) = a$, agora como os conjugados de π são elementos primos de D_m e não são associados dois a dois, tem-se que $N_n(\pi) = \prod_{\sigma \in G} \sigma(\pi)$ divide a. E então

$$\left(\frac{a}{\pi}\right)_m^d = \left(\frac{a}{N_n(\pi)}\right)_n = 0.$$

Agora, suponha que $\pi \nmid a$. Por definição (3.2.2) temos que

$$\left(\frac{a}{\pi}\right)_m^d \equiv a^{d(p-1)/m} = a^{(p-1)/n} \pmod{\pi}.$$

Afirmamos que $N(N_n(\pi)) = p$. De fato, considere o homomorfismo de anéis $\varphi : D_n/N_n(\pi)D_n \to D_m/\pi D_m$, definido por $\varphi(x + (N_n(\pi))) = x + (\pi)$. Observe que se $\varphi(x + (N_n(\pi))) = x + (\pi) = 0 + (\pi)$, então $\pi \mid x$ e, usando o mesmo argumento usado acima tem-se que, $N_n(\pi) \mid x$, logo $x + (N(\pi)) = 0 + (N(\pi))$ e concluímos que φ é um homomorfismo injetor. Portanto $D_n/N_n(\pi)D_n$ é isomorfo à um subanel de $D_m/\pi D_m$. Usando o mesmo argumento temos que $\mathbb{Z}/p\mathbb{Z}$ é isomorfo à um subanel de $D_n/N(\pi)D_n$. Como $D_m/\pi D_m \approx \mathbb{Z}/p\mathbb{Z}$, segue que $D_n/N(\pi)D_n$ é um corpo de p elementos. Portanto, $N(N_n(\pi)) = p$.

Como, por definição,

$$a^{(p-1)/n} = a^{(N(N_n(\pi))-1)/n} \equiv \left(\frac{a}{N_n(\pi)}\right)_n \pmod{N_n(\pi)},$$

e $\pi \mid N_n(\pi)$, segue que

$$a^{(p-1)/n} \equiv \left(\frac{a}{N_n(\pi)}\right)_n \pmod{\pi}.$$

Portanto,

$$\left(\frac{a}{\pi}\right)_m^d \equiv \left(\frac{a}{N_n(\pi)}\right)_n \pmod{\pi}.$$

Como ambos os lados da congruência acima são raízes n - ésimas da unidade, pelo teorema 2.2.3, temos a igualdade que queríamos.

■

Proposição 6.2.3 *Seja i o número complexo tal que $i^2 = -1$. Sejam $p, q \equiv 1 \pmod 4$ primos racionais. Sejam $\pi = a+bi$ e $\upsilon = c+di$ primos primários de $\mathbb{Z}[i]$ tais que $N(\pi) = p$ e $N(\upsilon) = q$, onde a, b, c e $d \in \mathbb{Z}$. Então*

$$\rho_4(p,q) = (-1)^{(p-1)/4}\left(\frac{ad+bc}{p}\right)_2.$$

DEMONSTRAÇÃO: Observamos que $p = a^2+b^2$ implica que $(p,a) = (p,b) = 1$. Sejam a' e b' os inversos de a e b módulo p respectivamente. Como $\pi = a+bi \equiv 0 \pmod{\pi}$, temos que $i = z \equiv -ab' \pmod{p}$. Repare também que $p \mid (-ab'-a'b)$. De fato, $(-ab'-a'b) = -a'(a^2b'+b) = -a'b'(a^2+b^2) = -a'b'p$. E, portanto, $z \equiv -ab' \equiv a'b \pmod{p}$.

Pelo teorema 5.7.7 temos que $e_m(p,\upsilon) = \left(\frac{p}{\upsilon}\right)_4\left(\frac{\upsilon}{p}\right)_4 = 1$.

Calculando s, com $k \in \mathbb{Z}_4^*$, obtemos $s \equiv f(z^3)^2 \pmod{p}$. Seja $f(i) = c+di = \upsilon$. Observe que $ß^3 \equiv z^3 \pmod{p}$ implica que $z^3 \equiv z' \pmod{p}$ e, portanto, $z^3 \equiv ab' \pmod{p}$. Assim, $f(z^3) \equiv c+dab' \pmod{\pi}$. Logo ,usando que $\left(\frac{(b')^2}{\pi}\right)_4 = \pm 1$ e que $\left(\frac{b^{-1}}{\pi}\right)_4 = \left(\frac{b}{\pi}\right)_4^{-1}$ temos $\left(\frac{(b')^2}{\pi}\right)_4 = \left(\frac{b^2}{\pi}\right)_4$, obtemos

$$\rho_4(p,q) = \left(\frac{c+dab'}{\pi}\right)_4^2 = \left(\frac{b^2}{\pi}\right)_4\left(\frac{bc+ad}{\pi}\right)_4^2.$$

Agora, como $a^2+b^2 \equiv 0 \pmod{\pi}$, segue que $\left(\frac{b^2}{\pi}\right)_4 = \left(\frac{-a^2}{\pi}\right)_4 = \left(\frac{-1}{\pi}\right)_4\left(\frac{a^2}{\pi}\right)_4$. Pela proposição 5.6.3 temos que $\left(\frac{-1}{\pi}\right)_4 = (-1)^{(p-1)/4}$. Pelo lema acima segue que $\left(\frac{a^2}{\pi}\right)_4 = \left(\frac{a}{p}\right)_2$. Decompondo a em fatores primos, aplicando sucessivas vezes a lei de reciprocidade quadrática e usando que $p \equiv 1 \pmod{4}$, obtemos $\left(\frac{a}{p}\right)_2 = \left(\frac{p}{a}\right)_2 = \left(\frac{b^2}{a}\right)_2 = 1$. Logo, usando as considerações acima e aplicando o lema na expressão $\left(\frac{bc+ad}{\pi}\right)_4^2$, obtemos

$$\rho_4(p,q) = (-1)^{(p-1)/4}\left(\frac{bc+ad}{p}\right)_2.$$

■

Proposição 6.2.4 (Burde) *Seja i o número complexo tal que $i^2 = -1$. Sejam $p, q \equiv 1 \pmod{4}$ primos racionais. Sejam $\pi = a+bi$ e $\upsilon = c+di$ primos primários de $\mathbb{Z}[i]$ tais que $N(\pi) = p$ e $N(\upsilon) = q$, onde a, b, c e $d \in \mathbb{Z}$. Então*

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = (-1)^{(p-1)/4}\left(\frac{ad-bc}{p}\right)_2.$$

DEMONSTRAÇÃO: Para obtermos o teorema de Burde da proposição acima, basta substituirmos π por $\overline{\pi}$ e observarmos que $\left(\frac{q}{\pi}\right)_4 = \left(\frac{q}{\overline{\pi}}\right)_4^{-1}$.

■

Referências Bibliográficas

[1] K. Burde. Ein rationales biquadratisches reziprozitatsgesetz. *J. Reine Angew. Math.*, **235**, (1969), 175-184.

[2] M. J. Collisson. The origins of the cubic and biquadratic reciprocity laws. *Arch. Hist. Exact. Sci.*, **17**, no. 1 (1977), 63-69.

[3] D. A. Cox. Quadratic reciprocity: it's conjecture and application. *Amer. Math. Monthly*, **95**, no. 5 (1998), 442-448.

[4] C. Helou. On rational reciprocity. *Proc. Am. Math. Soc.*, **108**, no. 4 (1990), 861-866.

[5] K. Ireland, M. Rosen. *A classical introduction to modern number theory* 2-*ed.* Springer, 1990.

[6] E. Lehmer. Rational reciprocity laws. *Amer. Math. Monthly*, **85**, no. 6, (1978), 467-472

[7] H. von Lienen. Reelle kubische und biquadratische Legendre-Symbole. *J. Reine Angew. Math.*, **305**, (1979), $140 - 154$.

[8] A. Weil. Two lectures on number theory: Past and Present. A. Weil, *oeuvres scientifiques*, Vol. III, pp. 279-302. New York: Springer-Verlag, 1979.

[9] B. F. Wyman. What is a reciprocity law? *Amer. Math. Monthly*, **79**, (1972), 571-586.