UNIDADES CICLOTOMICAS

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pelo Sr. SAMUEL TANAAMI e aprovada pela Comissão Julgadora

Campinas, 16 de Junho de 1989.

T M Vishwanathan

Prof. Dr. Tenkasi M. Viswanathan
Co-orientador

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Matemática.

AGRADECIMENTOS

Ao Professor Francisco Thaine Prada, pela sugestão do assunto e valiosa orientação.

Ao Professor Tenkasi Muthukrishna Viswanathan, co-orientador, pela segura orientação em um trabalho já iniciado.

Ao Professor Trajano Pires da Nóbrega Neto, pela imprescindível colaboração no desenvolvimento do presente trabalho.

Aos professores e funcionários do Departamento de Matemática e Estatística da ESALQ/USP, pela amizade.

Ao CNPq e à Capes, pelo apoio financeiro.

Dedico

com muito amor

à Raquel e

à Priscila.

INDICE

INTRODUÇÃO

Este trabalho desenvolve um estudo de certos subgrupos de unidades do grupo de todas as unidades de corpos ciclotômicos e corpos afins. Grupos de unidades têm sido objetos de profundos estudos devido à equação de Fermat

$$X^p + Y^p = Z^p,$$

sendo $p \geq 3$ um número primo.

Se ζ é uma raiz primitiva p-ésima da unidade, então a equação acima fatora-se como

$$\prod_{i=0}^{p-1} (X + Y\zeta^i) = Z^p.$$

As primeiras tentativas de solucionar o problema de Fermat, assim, passaram por essa fatoração no corpo $K=\mathbb{Q}(\zeta)$, supondo inocuamente a validade da fatoração única no anel $A=\mathbb{Z}[\zeta]$ dos inteiros desse corpo. Infelizmente a fatoração única não é válida. Pode-se enunciar um importante resultado nesta direção:

TEORMA 1 (BRAUER-SIEGEL): "Existe apenas um número finito de primos p tal que vale a fatoração única em $\mathbb{Z}[\zeta]$."

A tentativa de recuperar de alguma maneira a fatoração única levou Kummer (cerca de 1850) a construir uma teoria de divisores. A abordagem moderna usa a teoria de ideais de Dedekind (cerca de 1890). Nessa situação pode-se enunciar dois resultados clássicos de grande importância:

TEOREMA 2: "Se K é um corpo numérico, então o número h de classes de ideais de K é finito."

TEOREMA 3 (KUMMER): "Se $K=\mathbb{Q}(\zeta_p)$ e p não divide o número h de classes de ideais de K, então vale o primeiro caso do Teorema de

Fermat para o expoente p, isto é, não existem soluções inteiras x,y,z não triviais com p|xyz."

Assim, o interesse passou para o número h e, no caso de corpos ciclotômicos, para seus fatores. Conseqüentemente, o cálculo de h tornou-se um problema importante.

É nessa altura que entram os grupos de unidades. Começamos com um resultado mais abrangente:

TEOREMA 4 (DIRICHLET): "Seja K um corpo numérico de grau n. Entre os isomorfismos de K em $\mathbb{C}$, assumiremos que existem r_1 isomorfismos reais e $2r_2$ complexos. Assim, $n=r_1+2r_2$. Seja $r=r_1+r_2-1$. Então, o grupo E das unidades do anel A dos inteiros de K é um grupo abeliano finitamente gerado com posto r. Ou seja, existem unidades independentes $u_1,\ldots,u_r$ tais que toda unidade u de K tem uma única representação na forma

$$u = \zeta u_1^{n_1}\cdots u_r^{n_r},$$

onde $n_1,\ldots,n_r$ são inteiros e ζ é uma raiz da unidade de K."

A importância de subgrupos de índice finito vem do seguinte resultado:

TEOREMA 5: "Sejam $K=\mathbb{Q}(\zeta)$, $K^+=\mathbb{Q}(\zeta+\zeta^{-1})=K\cap\mathbb{R}$ o subgrupo maximal real de K e h e h^+ seus respectivos números de classes. Então $h=h^+h'$, onde h' é um inteiro positivo. Isto é, h^+ divide h. Mais ainda, h^+ é igual ao índice $[E^+:E_0]$, onde E^+ é o grupo das unidades de K^+ e K_0 é o grupo gerado pelas unidades

$$\theta_k = \frac{\operatorname{sen}(k\pi/p)}{\operatorname{sen}(\pi/p)} \quad (k=2,\ldots,(p-1)/2)$$

do corpo K."

Mais recentemente, Sinnott (1980) e Thaine (1988) têm destacado outros subgrupos de unidades de índice finito. Neste trabalho, estudaremos dois destes subgrupos:

i) de Ramachandra, um grupo C' gerado por -1 e ζ_s (Acta Arithmetica 12(1966), 165-173).

ii) de Sinnott, chamado de grupo de unidades ciclotômicas.

Mais precisamente, temos as definições:

"Sejam $f \not\equiv 2 \pmod 4$ e $f = \prod_{j=1}^{k} p_j^{a_j}$ sua decomposição em primos. Para $1<s<f/2$, com $(s,f)=1$, definamos

$$\xi_s = \zeta^{d_s} \prod_{e_j}{}' \frac{1-\zeta^{sf_j}}{1-\zeta^{f_j}}, \quad d_s = \frac{1}{2}(1-s) \sum_{e_j}{}' f_j$$

onde $f_j = \prod_{j=1}^{k} p_j^{a_j e_j}$, ζ é uma raiz primitiva f-ésima da unidade e o produto é estendido sobre todos os $e_j = 0$ ou 1, $j = 1,\ldots,k$, exceto $e_1 = e_2 = \cdots = e_k = 1$.

Os ξ_s acima definidos são unidades reais. Então, chamamos de C' o subgrupo gerado por -1 e os ξ_s."

"Se E é o grupo de unidades de $\mathbb{Q}(\zeta)$, então

$$C = \left\{ \pm \zeta^j \prod_{i=1}^{f-1} (1-\zeta^i)^{r_i} \in E : j, r_i \in \mathbb{Z} \right\}$$

é chamado grupo das unidades ciclotômicas de $\mathbb{Q}(\zeta)$."

O principal resultado deste trabalho consiste em mostrar que o subgrupo C é de índice finito no grupo E de todas as unidades. O capítulo III é dedicado à prova desse resultado. A técnica consiste em descer para o corpo real $K^+=\mathbb{Q}(\zeta+\zeta^{-1})$ onde trabalhamos com o subgrupo C' e demonstramos que $[E^+:C']$ é finito, sendo E^+ o grupo das unidades de K^+. Nesse estágio empregamos resultados que relacionam as L-séries e o número de classes de corpos ciclotômicos. Mostramos, então, que $[E^+:C^+]$ é finito, onde $C^+=C\cap E^+$ e, utilizando a igualdade $[E:C]=[E^+:C^+]$ (devido a Sinnott), provamos o resultado desejado.

O capítulo II apresenta as ferramentas analíticas necessárias sobre as L-séries $L(s,\chi)$, $s>1$, associadas a caracteres de Dirichlet χ. Os resultados mais importantes são dados pelos Teorema II.2.8 e seus corolários que apresentam as conexões entre as L-séries e o número de classes dos corpos ciclotômicos.

No capítulo I apresentamos o corpo ciclotômico, uma base integral deste corpo, bem como alguns fatos básicos de grande relevância. Apresentamos também os reguladores, que desempenham papel relevante na prova do principal teorema deste trabalho.

CAPÍTULO I

I.1 CORPOS CICLOTÔMICOS

Introduziremos, neste parágrafo, os corpos ciclotômicos, bem como alguns importantes conceitos a eles relacionados. Definiremos o polinômio ciclotômico e mostraremos que ele é irredutível. Mostraremos que o corpo ciclotômico dá origem a extensões abelianas de $\mathbb{Q}$ e situaremos neste quadro o Teorema de Kronecker-Weber sobre extensões abelianas de $\mathbb{Q}$, ilustrando-o por meio de um exemplo quadrático.

DEFINIÇÃO I.1.1. Chamamos de corpo ciclotômico a toda extensão $\mathbb{Q}(\zeta)$ de $\mathbb{Q}$ obtida pela adjunção de uma raiz da unidade ζ.

DEFINIÇÃO I.1.2. Seja m inteiro maior ou igual a 1 e ζ uma raiz primitiva m-ésima da unidade. O polinômio

$$\Phi_m(X) = \prod_{(k,m)=1} (X - \zeta^k)$$

é denominado m-ésimo polinômio ciclotômico.

As raízes de Φ_m são precisamente as raízes primitivas m-ésimas da unidade e $\partial\Phi_m = \varphi(m)$, φ função de Euler.

TEOREMA I.1.1. Se m é inteiro maior ou igual a 1, então os coeficientes de $\Phi_m(X)$ são inteiros, isto é, $\Phi_m(X) \in \mathbb{Z}[X]$.

DEMONSTRAÇÃO:

Provemos por indução sobre m.

Se m=1, está claro, pois $\Phi_1(X) = X-1$.

Suponha que $m \geq 2$ e que a afirmação seja válida para $1 \leq n < m$.

Como toda raiz m-ésima da unidade é uma raiz primitiva de grau $d|m$, então

$$X^m-1 = \prod_{d|m} \Phi_d(X)$$

Pela hipótese de indução, o polinômio $F = \prod_{\substack{d|m \\ d\neq m}} \Phi_d$ tem coeficientes inteiros e é mônico.

Então, os coeficientes de $\Phi_m(X) = (X^m-1)/F(X)$ também são inteiros. ■

TEOREMA I.1.2. Para qualquer inteiro positivo m, o polinômio ciclotômico Φ_m é irredutível sobre $\mathbb{Q}$.

DEMONSTRAÇÃO:

Seja $f(X)$ o polinômio minimal de ζ sobre $\mathbb{Q}$, ζ raiz primitiva m-ésima da unidade. Então, $f(X)$ divide X^m-1, ou seja, $X^m-1 = f(X)\cdot h(X)$, com f e h polinômios mônicos. Pelo lema de Gauss, segue que f e h têm coeficientes inteiros. Afirmo que, se p é um número primo que não divide m, então ζ^p é também uma raiz de f. De fato:

Suponha que ζ^p não seja raiz de f. Como ζ^p é raiz de X^m-1, ζ^p é uma raiz de h. Uma vez que $f(X)$ é o polinômio minimal de ζ e como ζ é raiz de $h(X^p)$, resulta que ζ é uma raiz comum dos polinômios $f(x)$ e $h(X^p)$. Logo,

$$h(X^p) = f(X)\cdot g(X).$$

Como f tem coeficientes inteiros e é mônico, g também tem coeficientes inteiros.

Consideremos, agora, o homomorfismo

$$\sigma : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_p[X]$$

$$r \longmapsto \bar{r}$$

onde $\sigma|_{\mathbb{Z}}$ é o homorfismo canônico de $\mathbb{Z}$ em $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ e $\sigma(X) = X$.

Temos $\bar{h}(X^p) = \bar{f}(X) \cdot \bar{g}(X)$.

Se $h(X) = \sum_{i=0}^{s} b_i X^i$, então $\bar{h}(X) = \sum_{i=0}^{s} \bar{b}_i X^i$ e, como $\bar{b}_i^p = \bar{b}_i$, temos

$$\bar{h}(X^p) = \sum_{i=0}^{s} \bar{b}_i X^{ip} = \sum_{i=0}^{s} \bar{b}_i^p X^{ip}$$

$$= \left(\sum_{i=0}^{s} \bar{b}_i X^i \right)^p = \bar{h}(X)^p$$

e, então, $\bar{h}^p = \bar{f}\,\bar{g}$.

Daqui resulta que se $\bar{v} \in \mathbb{Z}_p[X]$ é um fator irredutível e mônico de $\bar{f}$, então $\bar{v} | \bar{h}$ e, logo, $\bar{f}$ e $\bar{h}$ apresentam um fator comum.

Mas, $X^m - \bar{1} = \bar{f}(X)\bar{h}(X)$ e, portanto, $X^m - \bar{1}$ tem raiz múltipla. Isto é uma contradição, bastando tomar a derivada, uma vez que $p \nmid m$.

Portanto, ζ^p é também uma raiz de f.

Seja agora, ζ' uma raiz qualquer de Φ_m. Então, $\zeta' = \zeta^k$, onde k é relativamente primo com m. Se $k = p_1 p_2 \cdots p_t$, então, pelo visto acima, ζ^{p_1} é uma raiz de f. Analogamente, trocando ζ por ζ^{p_1}, concluímos que $\zeta^{p_1 p_2}$ é uma raiz de f. Continuando esse processo, concluímos que ζ^k é uma raiz de f.

Portanto, qualquer raiz de Φ_m é também uma raiz de f e, então, $\Phi_m = f$, mostrando assim que Φ_m é irredutível sobre $\mathbb{Q}$. ■

No decorrer da prova do último resultado, mostramos o seguinte

COROLÁRIO I.1.3. Seja ζ uma raiz primitiva m-ésima da unidade.

Então, $$[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(m),$$

onde $\varphi(m)$ é a função de Euler. ∎

TEOREMA I.1.4. Seja m um inteiro positivo e ζ uma raiz primitiva m-ésima da unidade. Então, $\mathbb{Q}(\zeta)$ é uma extensão galoisiana de $\mathbb{Q}$ cujo grupo de Galois G de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ é isomorfo ao grupo multiplicativo $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$ dos inteiros primos a m, mod m.

DEMONSTRAÇÃO:

Como $\mathbb{Q}(\zeta)$ é o corpo de decomposição do polinômio separável X^m-1, segue que a extensão $\mathbb{Q}(\zeta)|\mathbb{Q}$ é galoisiana.

Seja $\sigma \in G$ um automorfismo de $\mathbb{Q}(\zeta)$. Então, $\sigma(\zeta) = \zeta^k$, k unicamente determinado mod m, pois

$$(\sigma(\zeta))^m = \sigma(\zeta^m) = 1$$

Afirmo que $(k,m) = 1$. De fato:

Se $(k,m) = d > 1$, então $k = db$. Logo, $\sigma(\zeta) = \zeta^{db}$, ou seja, $(\sigma(\zeta))^{m/d} = 1$. Então, $\sigma(\zeta^{m/d}) = 1$. Como σ é injetivo, $\zeta^{m/d} = 1$. Mas isto é uma contradição, pois ζ é uma raiz primitiva m-ésima da unidade. Portanto, $\sigma \in G$ leva raiz primitiva m-ésima da unidade em raiz primitiva m-ésima da unidade.

Definamos a função

$$\begin{aligned} \psi: G &\longrightarrow \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \\ \sigma_k &\longmapsto \bar{k} \end{aligned}$$

onde

$$\begin{aligned} \sigma_k: \mathbb{Q}(\zeta) &\longrightarrow \mathbb{Q}(\zeta) \\ \zeta &\mapsto \zeta^k \quad , \text{ com } (k,m) = 1 \end{aligned}$$

Como

$$\sigma_k\sigma_l(\zeta) = \sigma_k(\sigma_l(\zeta)) = \sigma_k(\zeta^l) = (\sigma_k(\zeta))^l = (\zeta^k)^l = \zeta^{kl},$$

a função ψ é homomorfismo, pois

$$\psi(\sigma_k\sigma_l) = \overline{kl} = \overline{k}\ \overline{l} = \psi(\sigma_k)\ \psi(\sigma_l)$$

A função ψ é injetiva, pois se $\psi(\sigma_k) = \overline{1}$, então $\sigma_k(\zeta) = \zeta^1 = \zeta$, ou seja, σ_k é o elemento neutro de G. Como ambos os grupos são de ordem $\varphi(m)$, segue que a função ψ é também sobrejetiva. Assim ψ é um isomorfismo de G sobre $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$.

Tem-se de imediato a seguinte conseqüência importante:

COROLÁRIO I.1.5. A extensão galoisiana $\mathbb{Q}(\zeta)|\mathbb{Q}$ é abeliana. ■

Vale mencionar aqui dois resultados importantes que tratam de extensões abelianas de $\mathbb{Q}$:

TEOREMA I.1.6. Se K é um corpo intermediário, $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta)$, sendo ζ raiz primitiva m-ésima da unidade, então K é galoisiano e abeliano sobre $\mathbb{Q}$.

DEMONSTRAÇÃO:

Segue do fato de que um subgrupo de um grupo abeliano é normal e grupo fator de uma grupo abeliano é abeliano. ■

A recíproca do Teorema I.1.6 é o clássico Teorema de Kronecker-Weber. A sua prova foge dos nossos propósitos e indicamos ao leitor interessado [11] Washington, Theorem 14.1, p. 319.

TEOREMA I.1.7. Se $K|\mathbb{Q}$ é uma extensão abeliana de grau finito, então existe uma raiz da unidade ζ tal que $K \subseteq \mathbb{Q}(\zeta)$.

EXEMPLO: Como exemplo, vamos olhar para uma extensão quadrática $\mathbb{Q}(\sqrt{d})$ que define uma extensão abeliana de $\mathbb{Q}$.

Mostraremos que $\mathbb{Q}(\sqrt{d})$ está contido num corpo ciclotômico $\mathbb{Q}(\zeta_m)$ para algum $m \geq 2$. Para alcançar essa meta vamos lembrar da definição de somas de Gauss principal

$$S = \sum_{\nu} \left(\frac{\nu}{p}\right)\zeta_p^{\nu},$$

onde p é um primo ímpar, ζ_p é uma raiz primitiva p-ésima da unidade, a soma é tomada sobre um sistema reduzido de resíduos mod p e $\left(\frac{\nu}{p}\right)$ é o símbolo quadrático de Legendre, isto é,

$$\left(\frac{\nu}{p}\right) = \begin{cases} 1 & \text{se } \nu \equiv x^2 \pmod{p} \\ -1 & \text{se } \nu \not\equiv x^2 \pmod{p} \end{cases} \quad \text{para algum } x \in \mathbb{Z}$$

Assim, $S \in \mathbb{Q}(\zeta_p)$.

Afirmo que $S^2 = \left(\frac{-1}{p}\right)p = \pm p$. De fato:

Temos $S^2 = \sum_{\nu,\mu} \left(\frac{\nu}{p}\right)\left(\frac{\mu}{p}\right)\zeta_p^{\nu+\mu} = \sum_{\nu,\mu} \left(\frac{\nu\mu}{p}\right)\zeta_p^{\nu+\mu}$. Quando ν percorre um sistema reduzido de resíduos módulo p, o mesmo ocorre com $\nu\mu$, para qualquer μ fixo. Então,

$$S^2 = \sum_{\nu,\mu} \left(\frac{\nu\mu^2}{p}\right)\zeta_p^{\mu(\nu+1)} = \sum_{\nu,\mu} \left(\frac{\nu}{p}\right)\zeta_p^{\mu(\nu+1)}$$

$$= \sum_{\mu} \left(\frac{-1}{p}\right)\zeta_p^{0} + \sum_{\nu \neq -1} \left(\frac{\nu}{p}\right) \sum_{\mu} \zeta_p^{\mu(\nu+1)} = \left(\frac{-1}{p}\right)(p-1) + (-1) \sum_{\nu \neq -1} \left(\frac{\nu}{p}\right)$$

$$= \left(\frac{-1}{p}\right)p - \sum_{\nu} \left(\frac{\nu}{p}\right) = \left(\frac{-1}{p}\right)p.$$

Voltando ao exemplo, temos que $K = \mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadrados. Então $d = \pm 2^e p_1 \cdots p_r$, onde $e = 0$ ou 1, $r \geq 0$ e cada p_i é um primo ímpar. Segue-se que $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_r})$.

$\sqrt{-1}$ é uma raiz primitiva quarta da unidade, ζ_4.

$\sqrt{2}$ é expresso em termos de uma raiz primitiva oitava da unidade ζ_8, pois

$$\left(\zeta_8+\zeta_8^{-1}\right)^2 = \zeta_8^2 + \zeta_8^{-2} + 2 = \zeta_4 + \zeta_4^{-1} + 2 = 2 \text{ e, então,}$$

$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$.

Se p é um primo ímpar qualquer, então $\pm p = S^2$ e, portanto, ou $\sqrt{p} = S \in \mathbb{Q}(\zeta_p)$ ou $\sqrt{p} = \sqrt{-1}\cdot S \in \mathbb{Q}(\zeta_4,\zeta_p)$.

Combinando esses fatos, temos

$$K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_8,\zeta_{p_1},\ldots,\zeta_{p_r}) \subseteq \mathbb{Q}(\zeta_m),$$

onde $m = 8p_1\cdots p_r$ e ζ_m é uma raiz primitiva m-ésima da unidade, o que ilustra o Teorema de Kronecker-Weber.

PROPOSIÇÃO I.1.8. Sejam $L = \mathbb{Q}(\zeta)$, ζ raiz primitiva m-ésima da unidade, onde $m > 2$ e $K = \mathbb{Q}(\zeta+\zeta^{-1}) = \mathbb{Q}(\zeta)^+$. Então K é o maior subcorpo real de L.

DEMONSTRAÇÃO:

Seja σ o automorfismo conjugação em $\mathbb{C}$, isto é,

$$\sigma(\zeta) = \zeta^{-1}$$

Como σ tem ordem 2, o corpo fixo de σ, denotado M, é um corpo real e

$$[L:M] = 2 \text{ e } [M:\mathbb{Q}] = \frac{\varphi(m)}{2}$$

Como K é um corpo real fixado pontualmente por σ, então $K \subseteq M$.

Uma vez que ζ é uma raiz do polinômio

$$X^2-(\zeta+\zeta^{-1})X+1,$$

concluímos que

$$K = M \quad \blacksquare$$

Posteriomente, veremos que $\mathbb{Z}[\zeta+\zeta^{-1}]$ é o anel de inteiros de $\mathbb{Q}(\zeta)^+$.

1.2. ALGUNS RESULTADOS BÁSICOS

Neste parágrafo, definiremos traço, norma e valorização. Também enunciaremos, sem demonstração, as principais propriedades a eles relacionados.

Seja L uma extensão finita de grau n sobre K. Para qualquer $\alpha \in L$, a aplicação $\xi \mapsto \alpha\xi$ ($\xi \in L$) é uma transformação linear de L (considerado como um espaço vetorial sobre K). O polinômio característico $f_\alpha(X)$ dessa transformação é também chamado o polinômio característico do elemento $\alpha \in L$ em relação à extensão L|K. Se $(w_1, \ldots, w_n)$ é uma base para a extensão L|K e

$$\alpha w_i = \sum_{j=1}^{n} a_{ij} w_j \quad (a_{ij} \in K) \qquad (1)$$

então $f_\alpha(X) = \det(XI - (a_{ij}))$, onde I é a matriz identidade de ordem n.

O determinante e o traço da matriz (a_{ij}), definida por (1), não dependem da escolha da base $(w_1, \ldots, w_n)$. Temos, então, a seguinte definição:

DEFINIÇÃO I.2.1. O determinante $\det(a_{ij})$ da matriz (a_{ij}) de (1) é chamado a norma e seu traço $\sum_i a_{ii}$ é chamado o traço do elemento $\alpha \in L$ em relação à extensão L|K. A norma e o traço são denotados por $N_{L|K}(\alpha)$ e $Tr_{L|K}(\alpha)$, respectivamente.

Mencionaremos uma série de resultados relacionados à definição acima:

TEOREMA I.2.1. O polinômio característico $f_\alpha(X)$ de um elemento $\alpha \in L$

em relação à extensão L|K é uma potência de seu polinômio minimal sobre K.

Se $a \in K$, então a matriz da transformação linear $\xi \mapsto a\xi$ $(\xi \in L)$ será a matriz diagonal aI. Portanto, para todo elemento $a \in K$, temos

$$N_{L|K}(a) = a^n, \quad Tr_{L|K}(a) = na.$$

Quando transformações lineares são somadas ou compostas, suas matrizes são somadas ou multiplicadas (para uma base fixa), e, então para quaisquer elementos α e β de L, temos as fórmulas

$$N_{L|K}(\alpha\beta) = N_{L|K}(\alpha) \cdot N_{L|K}(\beta)$$

$$Tr_{L|K}(\alpha+\beta) = Tr_{L|K}(\alpha) + Tr_{L|K}(\beta).$$

A matriz da transformação linear $\xi \mapsto a\alpha\xi$ $(a \in K, \xi \in L)$ é obtida da matriz de transformação $\xi \mapsto \alpha\xi$ pela multiplicação de todos os elementos por a. Assim, temos a fórmula

$$Tr_{L|K}(a\alpha) = aTr_{L|K}(\alpha).$$

TEOREMA I.2.2. Sejam $\alpha \in L$, $f_\alpha(X)$ o polinômio característico de α em relação à extensão L|K e M|K uma extensão na qual $f_\alpha(X)$ se fatora em fatores lineares, $f_\alpha(X) = (X-\alpha_1)\cdots(X-\alpha_n)$. Então,

$$N_{L|K}(\alpha) = \alpha_1\alpha_2\cdots\alpha_n \text{ e}$$

$$Tr_{L|K}(\alpha) = \alpha_1+\alpha_2+\cdots+\alpha_n.$$

TEOREMA I.2.3. Sejam três corpos $K \subset L \subset M$, onde cada extensão é finita sobre o precedente e $\alpha \in M$. Então, temos as seguintes relações:

$$N_{M|K}(\alpha) = N_{L|K}(N_{M|L}(\alpha)) \text{ e}$$

$$Tr_{M|K}(\alpha) = Tr_{L|K}(Tr_{M|L}(\alpha)).$$

Definiremos, agora, o discriminante e, como acima, citaremos

alguns resultados importantes.

DEFINIÇÃO I.2.2. Sejam B um anel comutativo e A um subanel de B tal que B é um A-módulo livre de rank finito n. Se $x_1,\ldots,x_n \in B$, chamamos de discriminante do conjunto $(x_1,\ldots,x_n)$ o elemento de A definido pela relação

$$D_{B|A}(x_1,\ldots,x_n) = \det(Tr_{B|A}(x_i x_j)).$$

PROPOSIÇÃO I.2.4. Se $y_1,\ldots,y_n \in B$ é outro conjunto tal que $y_i = \sum_{j=1}^{n} a_{ij} x_j$ com $a_{ij} \in A$, então

$$D_{B|A}(y_1,\ldots,y_n) = (\det(a_{ij}))^2 D_{B|A}(x_1,\ldots,x_n).$$

PROPOSIÇÃO I.2.5. Sejam K um corpo finito ou de característica zero, L uma extensão de grau finito n de K e $\sigma_1,\ldots,\sigma_n$ os n K-isomorfismos distintos de L em um corpo algebricamente fechado C contendo K. Então, se $(x_1,\ldots,x_n)$ é uma base de L sobre K,

$$D_{L|K}(x_1,\ldots,x_n) = \det(\sigma_i(x_j))^2 \neq 0.$$

PROPOSIÇÃO I.2.6. Sejam K um corpo finito ou de característica zero, L=K[x] uma extensão de grau finito n de K e F(X) o polinômio minimal de x sobre K. Então,

$$D_{L|K}(1, x, \ldots, x^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{L|K}(F'(x)).$$

PROPOSIÇÃO I.2.7. Sejam três corpos K, L e M tais que $K \subset L \subset M$. Se

$(\alpha_1,\ldots,\alpha_n)$ é uma base de $L|K$ e $(\beta_1,\ldots,\beta_n)$ é uma base de $M|L$, então

$$D_{M|K}(\alpha_i\beta_j) = \pm D_{L|K}(\alpha_1,\ldots,\alpha_n)^{[M:L]} N_{L|K}[D_{M|L}(\beta_1,\ldots,\beta_n)].$$

PROPOSIÇÃO I.2.8. O discriminante de $\mathbb{Q}(\zeta_{p^n})$ é

$$d = d(\mathbb{Q}(\zeta_{p^n})) = \pm p^{p^{n-1}(pn-n-1)}.$$

DEMONSTRAÇÃO:

Sejam $m = p^n$ e $\zeta = \zeta_{p^n}$. Temos

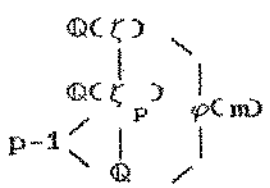
$$d = \pm N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\Phi_m'(\zeta)).$$

Também, $X^m-1 = (X^{m/p}-1)\Phi_m(X)$. Derivando, temos

$$mX^{m-1} = \frac{m}{p} X^{\frac{m}{p}-1}\Phi_m(X) + (X^{\frac{m}{p}}-1)\Phi_m'(X).$$

Logo, $m\zeta^{m-1} = (\zeta^{\frac{m}{p}}-1)\Phi_m'(\zeta)$ e, conseqüentemente,

$$\Phi_m'(\zeta) = \frac{m\zeta^{m-1}}{\zeta^{\frac{m}{p}}-1} = \frac{m\zeta^{m-1}}{\zeta_p^{-1}}.$$



Logo, $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(1-\zeta_p) = N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(N_{\mathbb{Q}(\zeta)|\mathbb{Q}(\zeta_p)}(1-\zeta_p))$

$$= [N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1-\zeta_p)]^{\frac{\varphi(m)}{p-1}}$$

$$= p^{\frac{\varphi(m)}{p-1}}.$$

Portanto, $$d = \pm \frac{N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(m\zeta^{m-1})}{N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(1-\zeta_p)}$$

$$= \pm \frac{n^{\varphi(n)}}{p^{\frac{\varphi(n)}{p-1}}} = \pm \left[p^{n-\frac{1}{p-1}} \right]^{\varphi(n)}$$

$$= \pm \left[p^{\frac{pn-n-1}{p-1}} \right]^{p^{n-1}(p-1)} = \pm p^{p^{n-1}(pn-n-1)}. \quad \blacksquare$$

PROPOSIÇÃO I.2.9. O discriminante de $\mathbb{Q}(\zeta_n)$ é

$$d = d(\mathbb{Q}(\zeta_n)) = \pm \frac{n^{\varphi(n)}}{\prod_{p \mid n} p^{\varphi(n)/p-1}}.$$

DEMONSTRAÇÃO:

Temos $X^n-1 = \prod_{d \mid n} \Phi_d(X) = \prod_{\substack{d \mid n \\ d<n}} \Phi_d(X)\Phi_n(X)$. Derivando, temos

$$nX^{n-1} = (X^n-1) \sum_{\substack{d \mid n \\ d<n}} \frac{\Phi'_d(X)}{\Phi_d(X)} + \prod_{\substack{d \mid n \\ d<n}} \Phi_d(X)\Phi'_n(X).$$

Logo, $n\zeta^{n-1} = \prod_{\substack{d \mid n \\ d<n}} \Phi_d(\zeta)\Phi'_n(\zeta)$ e, conseqüentemente,

$$\Phi'_n(\zeta) = \frac{n\zeta^{n-1}}{\prod_{\substack{d \mid n \\ d<n}} \Phi_d(\zeta)}.$$

Temos $X^m-1 = \prod_{d \mid m} \Phi_d(X)$. Logo, $\zeta^m-1 = \prod_{d \mid m} \Phi_d(\zeta)$ e, assim,

$$\zeta_{\frac{n}{m}}-1 = \prod_{d \mid m} \Phi_d(\zeta) \qquad (2)$$

Se n/m não é potência de primos, então $N_{\mathbb{Q}(\zeta) \mid \mathbb{Q}}(\Phi_d(\zeta)) = \pm 1$. Logo, só nos interessa o caso em que n/m é potência de primo. Seja $n = p_1^{a_1} \cdots p_s^{a_s}$. Para que n/m seja potência de primo é necessário que $m = \frac{n}{p_j^{a_j-i}}$, $1 \leq j \leq s$, $0 \leq i \leq a_j-1$. Logo, pela equação (2),

$$\zeta_{p_j}^{-1} = \prod_{d \mid \frac{n}{p_j}} \Phi_d(\zeta) \quad , \quad 1 \leq j \leq s.$$

Para cada p_j, $1 \leq j \leq s$, temos, pela proposição anterior que

$$N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(1-\zeta_{p_j}) = p_j^{\frac{\varphi(n)}{p_j - 1}}.$$

Portanto, $d = \pm N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\Phi_n'(\zeta)) = \pm \dfrac{n^{\varphi(n)}}{\prod\limits_{p \mid n} p^{\varphi(n)/p-1}}$. ∎

Vejamos, agora, alguns fatos sobre valorizações.

DEFINIÇÃO I.2.3. Seja p um número primo qualquer. Para todo inteiro não-nulo a, seja $\nu_p(a)=n\geq 0$ quando $p^n \mid a$ mas $p^{n+1} \nmid a$. Seja também $\nu_p(0)=\infty$. Se $x=a/b$ é um número racional qualquer (com $b\neq 0$), seja $\nu_p(x)=\nu_p(a)-\nu_p(b)$. Então ν_p, chamado valorização, está bem definido e satisfaz

$$\nu_p(x+y) \geq \min(\nu_p(x), \nu_p(y))$$

$$\nu_p(xy) = \nu_p(x)+\nu_p(y).$$

Mais ainda, se $\nu_p(x)\neq\nu_p(y)$, então $\nu_p(x+y) = \min(\nu_p(x), \nu_p(y))$ e $\nu_p(x) \geq 0 \Leftrightarrow p \mid x$.

Seja $\alpha\neq 0$ um elemento do anel A. Denotemos por $\nu_{\mathcal{P}}(\alpha)$ a potência na qual o ideal primo $\mathcal{P}$ entra na fatoração do ideal principal (α) em fatores primos. Claramente, $\nu_{\mathcal{P}}(\alpha)$ é caracterizado por $\mathcal{P}^{\nu_{\mathcal{P}}(\alpha)} \mid \alpha$ e $\mathcal{P}^{\nu_{\mathcal{P}}(\alpha)+1} \nmid \alpha$. Como zero é divisível por potências arbitrariamente grandes de $\mathcal{P}$, é natural colocarmos $\nu_{\mathcal{P}}(0) = \infty$.

Segue da definição acima que $\nu_{\mathcal{P}}(\alpha\beta) = \nu_{\mathcal{P}}(\alpha)+\nu_{\mathcal{P}}(\beta)$ e $\nu_{\mathcal{P}}(\alpha+\beta) \geq \geq \min(\nu_{\mathcal{P}}(\alpha), \nu_{\mathcal{P}}(\beta))$.

A função $\nu_{\mathcal{P}}(\alpha)$ pode ser estendida ao corpo de frações K do

anel A: para $\xi=\alpha/\beta \in K$ $(\alpha,\beta \in A)$ seja $v_{\mathfrak{p}}(\xi)=v_{\mathfrak{p}}(\alpha)-v_{\mathfrak{p}}(\beta)$.

Coloquemos $v_{\mathfrak{p}}(\gamma) = 1$ para o elemento $\gamma \in A$ tal que γ é divisível por $\mathfrak{p}$ mas não por $\mathfrak{p}^2$. Logo, $v_{\mathfrak{p}}(\gamma^k) = k$ para todo inteiro k. Então, $v_{\mathfrak{p}}(\alpha)$ toma todos os valores racionais.

DEFINIÇÃO I.2.4. Seja K um corpo. Uma função $v(\alpha)$, definida para $\alpha \in K$, é chamada valorização de K se satisfaz as seguintes condições:

i) $v(\alpha)$ toma todos os valores racionais quando α percorre todos os elementos não-nulos de K; $v(0)=\infty$;

ii) $v(\alpha\beta) = v(\alpha) + v(\beta)$;

iii) $v(\alpha+\beta) \geq \min(v(\alpha), v(\beta))$.

Temos $v(\alpha+\beta) = \min(v(\alpha), v(\beta))$ se $v(\alpha) \neq v(\beta)$.

I.3. UNIDADES DOS CORPOS CICLOTÔMICOS

Neste parágrafo, estabeleceremos alguns resultados sobre o anel dos inteiros de $\mathbb{Q}(\zeta)$ e sobre as unidades dos corpos ciclotômicos.

DEFINIÇÃO I.3.1. Seja R um anel comutativo com unidade e A um subanel de R. Dizemos que um elemento $x \in R$ é inteiro sobre A quando existem $n \geq 1$ elementos $a_0, a_1, \ldots, a_{n-1} \in A$ tais que $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. Se A é corpo, então $x \in R$ é inteiro sobre A se, e somente se, x é algébrico sobre A.

O próximo resultado é fundamental no estudo de números algébricos. Omitimos a sua prova, a qual nos referimos a [8] Samuel, Corollary 2, Proposition 1, p 29.

TEOREMA I.3.1. Seja K um corpo de números algébricos. Então

$$A = \left\{x \in K : x \text{ é inteiro sobre } \mathbb{Z}\right\}$$

é um sub-anel de K contendo $\mathbb{Z}$. A é denominado o anel dos inteiros de K.

TEOREMA 1.3.2. Sejam m um inteiro positivo e ζ uma raiz primitiva m-ésima da unidade. Então o anel A dos inteiros do corpo ciclotômico $\mathbb{Q}(\zeta)$ é $\mathbb{Z}[\zeta]$.

DEMONSTRAÇÃO:

Como ζ é raiz de $X^m - 1$, é claro que $\mathbb{Z}[\zeta] \subseteq A$.

Vamos mostrar que $A \subseteq \mathbb{Z}[\zeta]$ em três passos, divididos em três casos.

$1^{\underline{o}}$ CASO: $m = p$, sendo p um número primo.

Pelo Teorema I.1.2., o polinômio minimal de ζ sobre $\mathbb{Q}$ é

$$\Phi_p = X^{p-1}+X^{p-2}+\cdots+X+1$$

e, então, $[\mathbb{Q}(\zeta):\mathbb{Q}] = p-1$.

Portanto, $\{1,\zeta,\ldots,\zeta^{p-2}\}$ é uma base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$.

Seja $Tr = Tr_{\mathbb{Q}(\zeta)|\mathbb{Q}}$ a função traço. Como os conjugados de ζ^j são $\zeta,\zeta^2,\ldots,\zeta^{p-1}$ para $1 \leq j \leq p-1$, segue que

$$Tr(\zeta^j) = \zeta+\zeta^2+\cdots+\zeta^{p-1} = -1 \quad , \quad 1 \leq j \leq p-1 \qquad (1)$$

Além disso, $Tr(1) = 1\cdot[\mathbb{Q}(\zeta):\mathbb{Q}] = p-1$, pois $1 \in \mathbb{Q}$. Logo,

$$Tr(1-\zeta^j) = p \quad , \quad 1 \leq j \leq p-1 \qquad (2)$$

Como $\Phi_p = X^{p-1}+X^{p-2}+\cdots+X+1 = (X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{p-1})$, então

$$p = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1}) \qquad (3)$$

Logo, $p \in (1-\zeta)A$ e, então, $(1-\zeta)A \cap \mathbb{Z} \supseteq p\mathbb{Z}$.

Afirmo que $(1-\zeta)A \cap \mathbb{Z} = p\mathbb{Z}$. De fato:

Se $(1-\zeta)A \cap \mathbb{Z} \neq p\mathbb{Z}$, então $(1-\zeta)A \cap \mathbb{Z} = \mathbb{Z}$. Logo, $(1-\zeta)$ e seus conjugados $(1-\zeta^j)$, $1 \leq j \leq p-1$, são inversíveis em A. Então, por (3), p é também inversível em A, ou seja, p é inversível em $\mathbb{Q} \cap A = \mathbb{Z}$, uma contradição.

Mostremos, agora, que para qualquer $y \in A$,

$$Tr(y(1-\zeta)) \in p\mathbb{Z}. \qquad (4)$$

Sejam os elementos de A $y_1, y_2, \ldots, y_{p-1}$ conjugados de y.

Então,

$$\begin{aligned} Tr(y(1-\zeta)) &= y_1(1-\zeta)+y_2(1-\zeta^2)+\cdots+y_{p-1}(1-\zeta^{p-1}) \\ &= y^*(1-\zeta) \in (1-\zeta)A, \end{aligned}$$

pois $\frac{1-\zeta^j}{1-\zeta} = 1+\zeta+\cdots+\zeta^{j-1} \in A$. Mas, $Tr(y(1-\zeta)) \in \mathbb{Z}$ e, portanto,

$$Tr(y(1-\zeta)) \in (1-\zeta)A \cap \mathbb{Z} = p\mathbb{Z}.$$

Seja $x = a_0+a_1\zeta+\cdots+a_{p-2}\zeta^{p-2}$ um elemento de A, com $a_i \in \mathbb{Q}$. Provemos que $a_i \in \mathbb{Z}$. Temos $x\zeta = a_0\zeta+a_1\zeta^2+\cdots+a_{p-2}\zeta^{p-1}$. Efetuando a diferença, temos

$$x(1-\zeta) = a_0(1-\zeta)+a_1(\zeta-\zeta^2)+\cdots+a_{p-2}(\zeta^{p-2}-\zeta^{p-1}).$$

Tomando o traço, temos

$$Tr(x(1-\zeta)) = a_0 Tr(1-\zeta)+\cdots+a_{p-2}Tr(\zeta^{p-2}-\zeta^{p-1}).$$

Fazendo uso de (1) e (2), obtemos

$$Tr(x(1-\zeta)) = a_0 Tr(1-\zeta) = a_0 p.$$

Mas, por (4), $a_0 p = bp$, $b \in \mathbb{Z}$ e, então, $a_0 \in \mathbb{Z}$. Como $\zeta^{-1} = \zeta^{p-1}$, então $\zeta^{-1} \in A$ e, assim,

$$(x-a_0)\zeta^{-1} = a_1+a_2\zeta+\cdots+a_{p-2}\zeta^{p-3} \in A.$$

Repetindo-se o mesmo argumento, segue que $a_1 \in \mathbb{Z}$. Daí, aplicando-se sucessivamente o mesmo raciocínio, concluímos que cada $a_i \in \mathbb{Z}$.

Mostramos, assim, que no caso de $m = p$ um número primo, o anel dos inteiros $A = \mathbb{Z}[\zeta]$.

2º CASO: $m = p^k$, sendo p número primo e $k \geq 2$

Pelo teorema I.1.2. o polinômio irredutível de ζ é

$$\Phi_m(X) = X^{(p-1)p^{n-1}}+\cdots+X^{2p^{n-1}}+X^{p^{n-1}}+1 = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$$

$$= \prod_{(m,i)=1}(X-\zeta^i)$$

Portanto, se $t = \varphi(p^n) = (p-1)p^{n-1}$, então $(1,\zeta,\ldots,\zeta^{t-1})$ é uma base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$.

Se r e s são inteiros com $(m,rs) = 1$, afirmo que $(\zeta^r-1)/(\zeta^s-1)$ é uma unidade de $\mathbb{Z}[\zeta]$. De fato, escrevendo $r \equiv st \pmod m$ para algum t, temos

$$\frac{\zeta^r-1}{\zeta^s-1} = \frac{\zeta^{st}-1}{\zeta^s-1} = 1+\zeta^s+\cdots+\zeta^{(t-1)s} \in \mathbb{Z}[\zeta].$$

Semelhantemente, $(\zeta^s-1)/(\zeta^r-1) \in \mathbb{Z}[\zeta]$.

Conseqüentemente, temos a igualdade de ideais $(1-\zeta) = (1-\zeta^i)$, sempre que $(i,m) = 1$.

Agora, como $p = \Phi_m(1) = \prod_{(m,i)=1} (1-\zeta^i)$, então $(p) = (1-\zeta)^t$.

Se $A(1-\zeta) = IJ$, sendo I e J ideais de A, então $p = N(1-\zeta) = NI \cdot NJ$. Logo, $NI = 1$ ou $NJ = 1$ e, portanto, o ideal $(1-\zeta)$ não fatora em A, sendo, então, um ideal primo de A.

Como $\mathbb{Q}(\zeta) = \mathbb{Q}(1-\zeta)$, então $(1, 1-\zeta, \ldots, (1-\zeta)^{t-1})$ é uma base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$. Como $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$, vamos mostrar que $A = \mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$.

Seja, então, $\alpha = b_0 + b_1(1-\zeta) + \cdots + b_{t-1}(1-\zeta)^{t-1}$, com $b_i \in \mathbb{Q}$. Mostremos que $b_i \in \mathbb{Z}$.

Seja ν a valorização normalizada correspondente ao ideal $(1-\zeta) = \mathcal{P}$. Logo, $\nu(1-\zeta) = 1$ e, como p se ramifica totalmente, $\nu(\mathbb{Q}) = t\mathbb{Z}$. Observe também que $\nu(\alpha) \geq 0 \ \forall \ \alpha \in A$.

Temos

$$\nu(b_i(1-\zeta)^i) = \nu(b_i) + i\nu(1-\zeta) = \nu(b_i) + i, \quad 0 \leq i \leq t.$$

Afirmo que esses números são todos distintos: De fato, se $\nu(b_i)+i = \nu(b_j)+j$ com $0 \leq i, j < t$, então $i-j = \nu(b_j) - \nu(b_i) \in t\mathbb{Z}$, o que é impossível, a não ser que $i=j$. Logo $\nu(\alpha) = \min(\nu(b_i(1-\zeta)^i))$. Como $\nu(\alpha) \geq 0$ e $\nu(b_i) \in t\mathbb{Z}$, segue que

$$\nu(b_i) \geq 0.$$

Portanto, nenhum b_i tem p no denominador. Logo,

$$\alpha = a_0 + a_1\zeta + \cdots + a_{t-1}\zeta^{t-1},$$

com $a_i \in \mathbb{Q}$, mas p não divide o denominador de nenhum a_i. Temos

$$\alpha^{\sigma_i} = a_0 + a_1\zeta^{\sigma_i} + \cdots + a_{t-1}(\zeta^{\sigma_i})^{t-1},$$

onde σ_i percorre $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, sendo $\alpha_{\sigma_1} = \alpha$.

Seja $\alpha_i = \alpha^{\sigma_i}$. Então temos

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_t \end{pmatrix} = \begin{pmatrix} 1 & \zeta & \cdots & \zeta^i & \cdots & \zeta^t \\ 1 & \sigma_2(\zeta) & \cdots & \sigma_2(\zeta)^i & \cdots & \sigma_2(\zeta)^t \\ \vdots & \vdots & & \vdots & & \vdots \\ 1 & \sigma_t(\zeta) & \cdots & \sigma_t(\zeta)^i & \cdots & \sigma_t(\zeta)^t \end{pmatrix}$$

Mas, o determinante Δ da matriz é um determinante de Vandermonde. Então,

$$\Delta = \prod_{\substack{1 \le i < j \le t \\ p \nmid i\,j}} (\zeta^i - \zeta^j) = (\text{raiz da unidade}) \prod_{\substack{i < j \\ p \nmid i\,j}} (1 - \zeta^{j-i})$$

Pela regra de Cramer,

$$a_i = \frac{\Delta_i}{\Delta},$$

onde Δ_i é o determinante da matriz pela substituição da i-ésima coluna por

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_t \end{pmatrix}$$

Logo, $\Delta a_i = \Delta_i \in A$, donde, $(\Delta a_i)^t = (\Delta_i)^t \in A$.

Então, $p^u a_i^t \in A \cap \mathbb{Q} = \mathbb{Z}$ para algum u. Como nenhum a_i tem p no denominador,

$$a_i \in \mathbb{Z}.$$

3º CASO: m > 2 inteiro qualquer.

Este caso fica provado aplicando-se o lema abaixo para corpos ciclotômicos e usando o 2º caso. ∎

LEMA I.3.3. Suponhamos que K e E sejam dois corpos numéricos linearmente disjuntos (isto é, $[KE:\mathbb{Q}] = [K:\mathbb{Q}][E:\mathbb{Q}]$) cujos discriminantes são relativamente primos. Então $\mathcal{O}_{KE} = \mathcal{O}_K \mathcal{O}_E$, onde $\mathcal{O}_F$ denota o anel dos inteiros de um corpo F.

DEMONSTRAÇÃO: Veja [3] Lang, p. 68. ∎

Passamos, agora a considerar o corpo ciclotômico real $\mathbb{Q}(\zeta)^+$.

COROLÁRIO I.3.4. Seja $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta+\zeta^{-1})$. Então, $\mathbb{Z}[\zeta+\zeta^{-1}]$ é o anel dos inteiros de $\mathbb{Q}(\zeta)^+$, onde ζ é uma raiz m-ésima da unidade, $m > 2$ inteiro.

DEMONSTRAÇÃO:

Note que $\zeta+\zeta^{-1} = 2\cos\frac{2\pi}{m}$ é real e que ζ satisfaz uma equação quadrática sobre $\mathbb{Q}(\zeta)^+$. Logo o grau $[\mathbb{Q}(\zeta):\mathbb{Q}(\zeta)^+]$ é 2 e o grau $[\mathbb{Q}(\zeta)^+:\mathbb{Q}] = \frac{1}{2}\varphi(m)$.

Suponhamos que

$$\alpha = a_0+a_1(\zeta+\zeta^{-1})+\cdots+a_N(\zeta+\zeta^{-1})^N$$

é um inteiro algébrico, com $N \leq \frac{1}{2}\varphi(m)-1$ e $a_i \in \mathbb{Q}$. Afirmamos que $a_i \in \mathbb{Z}$ $\forall i$, $0 \leq i \leq N$. Se não, removendo-se aqueles termos com $a_i \in \mathbb{Z}$, assumimos que $a_N \notin \mathbb{Z}$. Multiplicando-se por ζ^N e expandindo o resultado como um polinômio em ζ, temos que

$$\zeta^N\alpha = a_N+\cdots+a_N\zeta^{2N}$$

é uma inteiro algébrico em $\mathbb{Q}(\zeta)$, portanto em $\mathbb{Z}[\zeta]$.

Como $2N \leq \varphi(m)-2 \leq \varphi(m)-1$, então $\{1,\zeta,\ldots,\zeta^{2N}\}$ é um subconjunto de uma $\mathbb{Z}$-base para o anel $\mathbb{Z}[\zeta]$.

Portanto, $a_N \in \mathbb{Z}$, uma contradição. ∎

O seguinte resultado é bem interessante e destaca as raízes da unidade dentre todas as unidades.

LEMA I.3.5. Se α é um inteiro algébrico com todos os conjugados tendo valor absoluto 1, então α é uma raiz da unidade.

DEMONSTRAÇÃO:

Considere $\alpha \in \mathbb{Z}[\zeta]$, ζ uma raiz primitiva m-ésima da unidade, m inteiro maior ou igual a 1 e seja $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1,\ldots,\sigma_r\}$

onde $r = \varphi(m)$ e $\sigma_i(\zeta) = \zeta^i$, $(i,m) = 1$. Logo, por hipótese, $|\sigma_i(\alpha)| = 1$, $\forall\, \sigma_i \in G$. Tomemos o polinômio irredutível de α

$$P(X) = (X-\sigma_1(\alpha))\cdots(X-\sigma_t(\alpha))$$

$$= X^t-(\sigma_1(\alpha)+\cdots+\sigma_t(\alpha))X^{t-1}+\cdots+(\sigma_1(\alpha)\cdots\sigma_t(\alpha)).$$

Temos

$$|\sigma_1(\alpha)+\cdots+\sigma_t(\alpha)| \leq |\sigma_1(\alpha)|+\cdots+|\sigma_t(\alpha)| = t = \binom{t}{1} = \binom{t}{t-1},$$

$$|\sum_{i\neq j} \sigma_i(\alpha)\sigma_j(\alpha)| \leq \sum_{i\neq j} |\sigma_i(\alpha)|\ |\sigma_j(\alpha)| = \binom{t}{2} = \binom{t}{t-2}$$

e assim sucessivamente. Assim, $P(X) = X^t+a_{t-1}X^{t-1}+\cdots+a_0$, onde $|a_i| \leq \binom{t}{i}$. Seja $P_n(X)$ o polinômio irredutível de α^n. Como $|\alpha^n| = |\alpha|^n = 1$ e $|\sigma_i(\alpha^n)| = |\sigma_i(\alpha)|^n = 1$, então os coeficientes de $P_n(X)$ são majorados por $\binom{t}{i}$ $\forall n$. Uma vez que $\alpha \in \mathbb{Z}[\zeta]$, α e $\sigma_i(\alpha)$ são inteiros sobre $\mathbb{Z}$. Logo, $P(X) \in \mathbb{Z}[X]$, ou seja $a_i \in \mathbb{Z}$. Ora, existe apenas um número finito de polinômios com coeficientes inteiros a_i com a propriedade de que $|a_i| \leq \binom{t}{i}$.

Portanto, existem i, j tais que $\alpha^i = \alpha^j$, ou seja, $\alpha^{i-j} = 1$, donde α é uma raiz da unidade. ∎

DEFINIÇÃO 1.3.2. Seja A um domínio e K seu corpo de fração. Dizemos que dois elementos a e b de A são associados, denotado $a\sim b$, se $a|b$ e $b|a$.

O conjunto $U = \{a \in K | a\sim 1\}$ é um subgrupo de K e $U \subseteq A$. Os elementos de U são inversíveis em A e são chamados unidades do anel A. Às vezes, por abuso de linguagem, usaremos a expressão "unidades de K" para nos referirmos às unidades do anel A.

A estrutura do grupo das unidades de um corpo numérico é determinada pelo seguinte Teorema de Dirichlet:

TEOREMA I.3.6. Seja K um corpo numérico de grau n. Entre os isomorfismos de K em $\mathbb{C}$, assumiremos que existem r_1 isomorfismos reais e $2r_2$ complexos. Assim, $n = r_1+2r_2$. Seja $r = r_1+r_2-1$. Então, o grupo A^* das unidades de K é isomorfo a $\mathbb{Z}^r \times G$, onde G é um grupo cíclico composto de raizes da unidade contidos em K. Ou seja, existem unidades independentes $u_1,\ldots,u_r$ tais que toda unidade u de K tem uma única representação na forma

$$u = \zeta u_1^{n_1}\cdots u_r^{n_r},$$

onde $n_1,\ldots,n_r$ são inteiros e ζ é uma raiz da unidade de K.

Antes de vermos a demonstração (devido à Minkowski), enunciemos dois lemas que serão necessários:

LEMA I.3.7. Seja d o discriminante absoluto de K, A o anel dos inteiros de K e $\mathcal{A}$ um ideal inteiro não-nulo de A. Então $\sigma(A)$ e $\sigma(\mathcal{A})$ são redes, onde σ é o homomorfismo injetor

$$\begin{aligned} \sigma:\ K &\longrightarrow \mathbb{R}^{r_1}\times\mathbb{C}^{r_2} \\ x &\mapsto (\sigma_1(x),\ldots,\sigma_{r_1+r_2}(x)) \end{aligned}$$

$\sigma_1,\ldots,\sigma_{r_1}$ homomorfismos reais e $\sigma_{r_1+1},\overline{\sigma}_{r_1+1},\ldots,\sigma_{r_1+r_2},\overline{\sigma}_{r_1+r_2}$ homomorfismos complexos.

Mais ainda,

$$\mathrm{vol}(\sigma(A)) = 2^{-r_2}|d|^{1/2} \text{ e } \mathrm{vol}(\sigma(\mathcal{A})) = 2^{-r_2}|d|^{1/2}N(\mathcal{A}).$$

LEMA I.3.8. Seja H uma rede em $\mathbb{R}^n$, S um conjunto mensurável de $\mathbb{R}^n$ simétrico em relação a 0 e convexo, e suponha que S satisfaz uma das condições:

a) $\mathrm{vol}(S) > 2^n\mathrm{vol}(H)$

b) $\mathrm{vol}(S) \geq 2^n\mathrm{vol}(H)$ e S é compacto.

Então, $S \cap (H-\{0\}) \neq \emptyset$, ou seja, $S \cap H$ tem um ponto distinto

de zero.

DEMONSTRAÇÃO:

Voltando ao teorema, consideremos a aplicação

$$L:\ K^* \longrightarrow \mathbb{R}^{r_1+r_2}$$
$$x \mapsto (\log|\sigma_1(x)|,\ldots,\log|\sigma_{r_1+r_2}(x)|)$$

Como

$$\begin{aligned} L(xy) &= (\ldots,\log|\sigma_i(xy)|,\ldots) \\ &= (\ldots,\log|\sigma_i(x)||\sigma_i(y)|,\ldots) \\ &= (\ldots,\log|\sigma_i(x)|+\log|\sigma_i(y)|,\ldots) \\ &= (\ldots,\log|\sigma_i(x)|,\ldots)+(\ldots,\log|\sigma_i(y)|,\ldots) \\ &= L(x)+L(y), \end{aligned}$$

L é um homomorfismo do grupo multiplicativo K^* no grupo aditivo $\mathbb{R}^{r_1+r_2}$. Seja B um subconjunto compacto de $\mathbb{R}^{r_1+r_2}$ e $B' = \{x \in \Lambda^* : L(x) \in B\}$. Como B é limitado, existe $\beta > 0$ tal que se $x \in B'$, então $|L(x)| < \beta$.

Logo, $|\log|\sigma_i(x)|| < \beta$, $i = 1,\ldots,n$

$\Leftrightarrow -\beta < \log|\sigma_i(x)| < \beta \Leftrightarrow e^{-\beta} < |\sigma_i(x)| < e^{\beta}$ e, daí

$\alpha^{-1} < |\sigma_i(x)| < \alpha$ se $\alpha = e^{\beta}$, $i = 1,\ldots,n$.

Tomemos o polinômio característico de x:

$$(X-\sigma_1(x))(X-\sigma_2(x))\cdots(X-\sigma_n(x)) =$$
$$= X^n-(\sigma_1(x)+\cdots+\sigma_n(x))X^{n-1}+\cdots+(-1)^n(\sigma_1(x)\cdots\sigma_n(x))$$
$$= X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0 \in \mathbb{Z}[X].$$

Logo, $|a_i| \leq \binom{n}{i}\alpha^i$ e, então, existe um número finito de polinômios característicos possíveis para $x \in B'$. Conseqüentemente, x assume um número finito de valores, ou seja, B' é finito. O fato de B' ser finito implica imediatamente nos seguintes fatos:

i) O núcleo G de L é um grupo finito cíclico consistindo das raizes da unidade de K. De fato:

Se $x \in G$, então $L(x) = (0,0,\ldots,0)$, ou seja, $\log|\sigma_i(x)| = 0$ e, então, $|\sigma_i(x)| = 1 \ \forall\, i = 1,\ldots,r_1+r_2$. Logo, pelo Lema I.3.5, x é uma raiz da unidade de K. Então, $G \subseteq \langle$raizes da unidade de K$\rangle$.

Reciprocamente, se ζ é uma raiz da unidade de K, então, $\zeta^l = 1$ e $\sigma_i(\zeta)^l = 1$, para algum l. Logo, $|\sigma_i(\zeta)|^l = 1$ e $|\sigma_i(\zeta)| = 1$ e, então,

$$L(\zeta) = (\log|\sigma_1(\zeta)|,\ldots,\log|\sigma_{r_1+r_2}(\zeta)|)$$

$$= (\log 1,\ldots,\log 1) = (0,0,\ldots,0) \text{ e, então, } \zeta \in G.$$

Logo $\langle$raizes da unidade de K$\rangle \subseteq G$ e, portanto,

$$G = \langle\text{raizes da unidade de K}\rangle.$$

ii) Como foi visto acima, $L(A^*) \cap B$ é finito e, logo, $L(A^*)$ é um subgrupo discreto de $\mathbb{R}^{r_1+r_2}$ ([8] Samuel, §4.1, p. 53). Conseqüentemente, $L(A^*)$ é um $\mathbb{Z}$-módulo livre de posto $s \leq r_1+r_2$, isto é, existem elementos $v_1,\ldots,v_s$ de $\mathbb{R}^{r_1+r_2}$ linearmente independentes tais que $L(A^*) = \mathbb{Z}v_1+\mathbb{Z}v_2+\cdots+\mathbb{Z}v_s$. Logo, $L(A^*) \simeq \mathbb{Z}^s$.

Temos, então

$$L:\ A^* \longrightarrow L(A^*) \simeq \mathbb{Z}^s$$

Logo, $\frac{A^*}{G} \simeq \mathbb{Z}^s$. Afirmo que $A^* \simeq G\times\mathbb{Z}^s$. De fato:

Seja $\langle e_1,\ldots,e_s\rangle$ uma $\mathbb{Z}$-base de $L(A^*)$ e $x_1,\ldots,x_s \in A^*$ tais que $L(x_1) = e_1,\ldots,\ L(x_s) = e_s$. Suponhamos que $\zeta \in G$ e $a_1,\ldots,a_s \in \mathbb{Z}$ são tais que $\zeta x_1^{a_1}\cdots x_s^{a_s} = 1$.

Logo, $L(\zeta x_1^{a_1}\cdots x_s^{a_s}) = L(1) \Leftrightarrow L(\zeta)+\sum_{i=1}^{s} a_i L(x_i) = (0,0,\ldots,0) \Leftrightarrow$

$$\Leftrightarrow \sum_{i=1}^{s} a_i e_i = 0 \Leftrightarrow a_i = 0 \ \forall i \text{ e, daí } \zeta = 1.$$

Se $V = \langle x_1,\ldots,x_s\rangle$, então $V \cap G = 1$ e $V \simeq \mathbb{Z}^s$.

Seja, agora, $x \in A^*$. Logo,

$$L(x) = b_1 e_1 + \cdots + b_s e_s = L(x_1^{b_1} \cdots x_s^{b_s}).$$

Assim, $L\left(\dfrac{x}{x_1^{b_1} \cdots x_s^{b_s}}\right) = 0$ e, então, $\dfrac{x}{x_1^{b_1} \cdots x_s^{b_s}} = \zeta \in G$.

Logo, $x = \zeta x_1^{b_1} \cdots x_s^{b_s}$ e, portanto, $A^* \simeq G \times \mathbb{Z}^s$.

Resta mostrarmos que o posto s de $L(A^*)$ é igual a r_1+r_2-1. A desigualdade $s \leq r_1+r_2-1$ é fácil:

Temos $x \in A^* \Leftrightarrow N(x) = \pm 1$. Também,

$$\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_1+r_2} [\sigma_j(x)\overline{\sigma_j(x)}] \text{ e, logo,}$$

$$1 = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2, \text{ o que implica que}$$

$$0 = \sum_{i=1}^{r_1} \log|\sigma_i(x)| + 2 \sum_{j=r_1+1}^{r_1+r_2} \log|\sigma_j(x)|$$

Então, $L(A^*) \subseteq W$, onde W é o hiperplano definido por

$$W = \left\{ (y_1, \ldots, y_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : \sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0 \right\}$$

Como $\dim W = r_1+r_2-1$ e $\{v_1, \ldots, v_s\}$ são linearmente independentes sobre $\mathbb{R}$, $s \leq r_1+r_2-1$.

Mostremos, agora, que $L(A^*)$ contém $r = r_1+r_2-1$ vetores linearmente independentes (portanto, $s = r = r_1+r_2-1$ e $A^* \simeq G \times \mathbb{Z}^s$). Para isto, basta mostrarmos que para qualquer forma linear $f \neq 0$ em W, existe uma unidade u tal que $f(L(u)) \neq 0$.

Seja

$$\begin{array}{rccc} \psi: & W & \longrightarrow & \mathbb{R}^r \\ & (y_1, \ldots, y_{r+1}) & \mapsto & (y_1, \ldots, y_r) \end{array}$$

Como $y_1+\cdots+y_{r_1}+2y_{r_1+1}+\cdots+2y_{r_1+r_2} = 0$, temos $\ker \psi = 0$.

Seja, agora, f definida por

$$f: W \longrightarrow \mathbb{R}$$

$$\begin{array}{ccc} W & \xrightarrow{\psi} & \mathbb{R}^r \\ f\downarrow & & \\ \mathbb{R} & & \end{array} \qquad f(y_1,\ldots,y_{r+1}) = f(\psi^{-1}(y_1,\ldots,y_r)) = c_1y_1+\cdots+c_ry_r$$

com $c_i \in \mathbb{R}$

Fixe $\alpha \geq \left(\frac{2}{\pi}\right)^{r_2}|d|^{1/2}$.

Para todo conjunto $\lambda = (\lambda_1,\ldots,\lambda_r)$ de r números positivos reais, definamos $\lambda_{r+1} > 0$ tal que

$$\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

Seja $B=\left\{(y_1,\ldots,y_{r_1},z_1,\ldots,z_{r_2}) \in \mathbb{R}^{r_1}\times\mathbb{C}^{r_2} : |y_i|\leq\lambda_i, |z_j|\leq\lambda_j\right\}$

O conjunto B é compacto, convexo, simétrico em relação a 0 e tem volume

$$v(B) = \prod_{i=1}^{r_1} 2\lambda_i \prod_{j=r_1+1}^{r_1+r_2} \pi\lambda_j^2 = \pi^{r_2}2^{r_1}\alpha \geq 2^{r_1}\pi^{r_2}\left(\frac{2}{\pi}\right)^{r_2}|d|^{1/2}$$

$$= 2^{r_1+r_2}|d|^{1/2} = 2^{r_1+2r_2}\,2^{-r_2}|d|^{1/2} = 2^n\, v(\sigma(A))$$

(conforme o Lema I.3.7)

Segue do Lema I.3.8 que existe um inteiro não nulo x_λ de A tal que $\sigma(x_\lambda) \in B$, isto é, $|\sigma_i(x_\lambda)| \leq \lambda_i$, $1 \leq i \leq r_1+2r_2$. Como $x_\lambda \in A-(0)$, temos

$$1 \leq |N(x_\lambda)| = \prod_{i=1}^{r_1} |\sigma_i(x_\lambda)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x_\lambda)|^2$$

$$\leq \prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha.$$

Por outro lado,

$$|\sigma_i(x_\lambda)| = |N(x_\lambda)| \prod_{\substack{j\neq i \\ 1\leq j\leq n}} |\sigma_i(x_\lambda)|^{-1} \geq \prod_{j\neq i} \lambda_i^{-1} = \lambda_i\alpha^{-1}, \ \forall i.$$

Temos assim

$\lambda_i\alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i$, $\forall i$, e, então,

$$1 \leq \frac{\lambda_i}{|\sigma_i(x_\lambda)|} \leq \alpha \quad e$$

$$0 \leq \log\lambda_i - \log|\sigma_i(x_\lambda)| \leq \log \alpha.$$

Como $L(x_\lambda) = (\log |\sigma_1(x_\lambda)|, \ldots, \log |\sigma_{r+1}(x_\lambda)|)$ e

$f(y) = c_1y_1+\cdots+c_ry_r$, $y \in W$, então

$$|f(L(x_\lambda)) - \sum_{i=1}^{r} c_i\log\lambda_i| = |\sum_{i=1}^{r} c_i(\log|\sigma_i(x)| - \log\lambda_i)|$$

$$\leq (\sum_{i=1}^{r} |c_i| \cdot |\log|\sigma_i(x)| - \log\lambda_i|)$$

$$\leq (\sum_{i=1}^{r} |c_i|)\log\alpha.$$

Seja β constante tal que $(\sum_{i=1}^{r} |c_i|)\log\alpha < \beta$ e $h \geq 1$ inteiro. Escolho r números reais positivos $\lambda_{i,h}$ $(i=1,\ldots,r)$ satisfazendo $\sum_{i=1}^{r} c_i\log\lambda_{i,h} = 2h\beta$. Consideremos $\lambda(h) = (\lambda_{1,h},\ldots,\lambda_{r,h})$ e $x_{\lambda(h)} = x_h$.

Temos que, para qualquer $h \geq 1$ inteiro, existe $x_h \in A-(0)$ tal que $|N(x_h)| < \alpha$ e $|f(L(x_h)) - 2h\beta| \leq \beta$, sendo α e β independentes de h. Então

$$-\beta < f(L(x_h))-2h\beta < \beta, \text{ ou seja}$$

$$(2h-1)\beta < f(L(x_h)) < (2h+1)\beta.$$

Se $h = 1$, $\beta < f(L(x_1)) < 3\beta$.

Se $h = 2$, $3\beta < f(L(x_2)) < 5\beta$ e assim por diante.

Logo, $f(L(x_i)) \neq f(L(x_j))$ $\forall\ i, j \geq 1$, $i \neq j$.

Temos $\alpha \geq |N(x_h)| = N(Ax_h) = \#\frac{A}{Ax_h} = q$. Logo, $q \in Ax_h$ e, então, Ax_h contém Aq. Como existe correspondência entre os ideais

de A que contém Aq e os ideais de $\frac{A}{Aq}$ e o número de ideais de $\frac{A}{Aq}$ é finito, existe um número finito de ideais da forma Ax_h.

Portanto, existem i, j , $i \neq j$ tais que $Ax_i = Ax_j$, ou seja, x_i e x_j são associados. Então, $x_i = ux_j$ para algum $u \in A^*$. Logo, $u = \frac{x_i}{x_j}$ e, então, $L(u) = L(x_i) - L(x_j)$.

Como f é linear, então $f(L(u)) = f(L(x_i)) - f(L(x_j)) \neq 0$. Assim, posto de $L(A^*) = \dim W^{\perp} = \dim W = r_1 + r_2 - 1$. ■

DEFINIÇÃO I.3.3. O conjunto (u_i) , i=1,...,r de unidades independentes que geram as unidades de K do teorema acima é chamado sistema fundamental de unidades de K.

EXEMPLO: Sejam p um número primo diferente de 2, ζ uma raiz primitiva p-ésima da unidade e K o corpo ciclotômico $\mathbb{Q}(\zeta)$. Temos $[K:\mathbb{Q}] = p-1$ (cf. Corolário I.1.3).

Como nenhum conjugado de ζ em $\mathbb{C}$ é real, então $r_1 = 0$, $2r_2 = p-1$ e, portanto, $r = \frac{p-3}{2}$.

DEFINIÇÃO I.3.4. Sejam $u = (u_1, \ldots, u_r)$ um sistema fundamental de unidades de K, $\delta_i = 1$ se $1 \leq i \leq r_1$ e $\delta_i = 2$ se $r_1+1 \leq i \leq r+1$. O número real positivo

$$R_K(u) = |\det(\delta_i \log|\sigma_i(u_j)|)|_{1 \leq i,j \leq r}$$

é chamado de regulador de K.

Observemos que um σ_i foi omitido. Mas, para qualquer k, $1 \leq k \leq r+1$, temos $N(u_k) = \pm 1 \Rightarrow |N(u_k)| = 1$.

Logo, $\left| \prod_{i=1}^{r_1+r_2} \sigma_i(u_k) \right| = 1$, ou seja,

$$\cdot \left| \prod_{i=1}^{r_1} |\sigma_i(u_k)| \cdot \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(u_k)|^2 \right| = 1.$$

Então,

$$\sum_{i=1}^{r_1} \log|\sigma_i(u_k)| + \sum_{i=r_1+1}^{r_1+r_2} 2\log|\sigma_i(u_k)| = 0$$

e, portanto,

$$\delta_i \log|\sigma_i(u_k)| = -(\delta_1 \log|\sigma_1(u_k)| + \cdots + \delta_{i-1} \log|\sigma_{i-1}(u_k)| +$$

$$+ \delta_{i+1} \log|\sigma_{i+1}(u_k)| + \cdots + \delta_{r_1+r_2} \log|\sigma_{r_1+r_2}(u_k)|).$$

Portanto, a possível mudança de sinal pela omissão de um σ_j diferente não ocorre, uma vez que tomamos o valor absoluto do determinante.

PROPOSIÇÃO I.3.9. Sejam $u = (u_1, \ldots, u_r)$ e $v = (v_1, \ldots, v_r)$ dois sistemas fundamentais de unidades de K (com $r = r_1+r_2-1$). Então

$$R_K(u) = R_K(v).$$

DEMONSTRAÇÃO:

Pelo Teorema de Dirichlet, podemos escrever

$$v_j = \zeta \prod_{k=1}^{r} u_k^{a_{kj}} \quad (\text{para todo } j = 1, \ldots, r),$$

onde $a_{kj} \in \mathbb{Z}$ e ζ é uma raiz da unidade de K.

De igual modo, podemos escrever

$$u_j = \zeta^* \prod_{k=1}^{r} v_k^{a'_{kj}} \quad (\text{para todo } j = 1, \ldots, r)$$

onde $a'_{kj} \in \mathbb{Z}$ e ζ^* é uma raiz da unidade de K.

Então, pela unicidade da representação de unidades, a matriz

(a_{kj}) é a inversa de (a_{kj}). Conseqüentemente $\det(a_{kj})=\det(a_{kj})$, ambos -1 ou ambos 1 e, assim, $|\det(a_{kj})| = |\det(a_{kj})| = 1$.

Portanto,

$$\begin{aligned} R_K(v) &= |\det(\delta_i \log|\sigma_i(v_j)|)| \\ &= |\det(\delta_i \log|\sigma_i(\zeta \prod_{k=1}^{r} u_k^{a_{kj}})|)| \\ &= |\det(\delta_i \sum_{k=1}^{r} a_{kj} \log|\sigma_i(u_k)|)| \\ &= |\det(a_{kj})|\ |\det(\delta_i \log|\sigma_i(u_k)|)| \\ &= R_K(u). \quad \blacksquare \end{aligned}$$

Vejamos, agora, um resultado de Kummer que desempenhou um papel importante na tentativa de provar o "Último Teorema de Fermat":

TEOREMA I.3.10. Seja ζ uma raiz primitiva p-ésima da unidade, p primo ímpar. Toda unidade u de $\mathbb{Q}(\zeta)$ pode ser escrita como

$$u = \zeta^h v,$$

onde v é uma unidade real de $\mathbb{Z}[\zeta]$.

DEMONSTRAÇÃO:

Seja u uma unidade de $\mathbb{Q}(\zeta)$. Então,

$$u = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}, \text{ com } a_i \in \mathbb{Z}.$$

Seu complexo conjugado, que também é uma unidade (pois $uv = 1$ implica $\bar{u}\,\bar{v} = 1$), é dado por

$$\bar{u} = a_0 + a_1\zeta^{-1} + a_2\zeta^{-2} + \cdots + a_{p-2}\zeta^{-(p-2)}.$$

Logo, $\left|\frac{u}{\bar{u}}\right|^2 = \frac{u\bar{u}}{\bar{u}u} = 1$, $\left|\frac{u}{\bar{u}}\right| = 1$ e $\frac{u}{\bar{u}} \in \mathbb{Z}[\zeta]$.

$\mathbb{Q}(\zeta)$ Seja $\sigma \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$.

$\Big|_{p-1}$

$\mathbb{Q}$

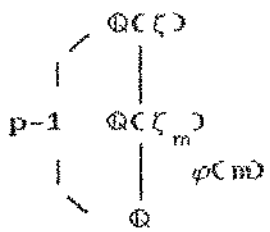
Então,

$$\left|\sigma\left(\frac{u}{\bar{u}}\right)\right|^2 = \left|\frac{\sigma(u)}{\sigma(\bar{u})}\right|^2 = \left|\frac{\sigma(u)}{\overline{\sigma(u)}}\right|^2 = \frac{\sigma(u)\cdot\overline{\sigma(u)}}{\overline{\sigma(u)}\cdot\sigma(u)} = 1$$

e, logo, $\left|\sigma\left(\frac{u}{\bar{u}}\right)\right| = 1$.

Temos, então, que $\frac{u}{\bar{u}}$ é um elemento de $\mathbb{Z}[\zeta]$ tal que ele e todos os seus conjugados têm módulo 1. Então, $\frac{u}{\bar{u}}$ é uma raiz da unidade de $\mathbb{Z}[\zeta]$, conforme o Lema I.3.5.

Seja H o grupo das raízes da unidade de $\mathbb{Q}(\zeta)$. Logo, H é cíclico e $H = (\zeta_m)$ sendo ζ_m uma raiz primitiva m-ésima da unidade.



Mas, $m = p^a t$, onde $a \geq 1$, $p \nmid t$. Temos $\varphi(m) \leq p-1$. Logo, $p^{a-1}(p-1)\varphi(t) \leq p-1$. Então, $a = 1$, $\varphi(t) = 1$ e, portanto, $t = 2$. Assim, $\frac{u}{\bar{u}} = \pm\zeta^k$, $0 \leq k \leq p-1$. Como $\zeta \equiv 1 \mod(1-\zeta)$, então $\zeta^j \equiv 1 \mod(1-\zeta)$ $j \geq 1$, pois $\zeta^j - 1 = (\zeta-1)(1+\zeta+\cdots+\zeta^{j-1}) \in (1-\zeta)\mathbb{Z}[\zeta]$.

Temos $u = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \equiv a_0 + a_1 + \cdots + a_{p-2} \mod(1-\zeta)$

$\equiv a \mod(1-\zeta)$, se $a \equiv a_0 + a_1 + \cdots + a_{p-2} \in \mathbb{Z}$.

Como $\bar{u} = a_0 + a_1\zeta^{-1} + \cdots + a_{p-2}\zeta^{-(p-2)} \equiv a_0 + a_1 + \cdots + a_{p-2} \mod(1-\zeta)$

$= a \mod(1-\zeta)$, então

$$u \equiv \bar{u} \mod(1-\zeta).$$

Vamos descartar a possibilidade de $\frac{u}{\bar{u}}$ ser igual a $-\zeta^k$.

Se $u = -\zeta^k\bar{u} \equiv -\bar{u} \mod(1-\zeta)$, então $a \equiv -a \mod(1-\zeta)$ e, logo, $2a \equiv 0 \mod(1-\zeta)$, ou seja, $2a \in (1-\zeta)$.

Uma vez que $(1-\zeta)$ é ideal primo, $2 \in (1-\zeta)$ ou $a \in (1-\zeta)$. Se $2 \in (1-\zeta)$, $2 \in (1-\zeta) \cap \mathbb{Z} = p\mathbb{Z}$ e, então, $p|2$, uma contradição. Logo, $a \in (1-\zeta)$, ou seja, $a \equiv 0 \bmod (1-\zeta)$. Assim, $u \equiv 0 \bmod (1-\zeta)$, isto é, $u \in (1-\zeta)$. Conseqüentemente, $(1-\zeta) = \mathbb{Z}[\zeta]$, uma contradição.

Dessa forma, $\dfrac{u}{\overline{u}} = +\zeta^k = \zeta^{2h}$ para algum h.

Temos $u\zeta^{-h} = \overline{u}\zeta^{h} = \overline{u\zeta^{-h}}$. Pondo $v = u\zeta^{-h}$, vemos que $\overline{v} = v$.

Portanto, $u = \zeta^h v$ com $v \in \mathbb{R}$. ∎

II.1. CARACTERES DE DIRICHLET

Neste parágrafo introduzimos alguns fatos básicos sobre os caracteres de Dirichlet.

DEFINIÇÃO II.1.1. Um homomorfismo χ de um grupo abeliano finito G no grupo multiplicativo dos complexos é chamado um caráter do grupo G

O caráter χ para o qual $\chi(x) = 1$ $\forall x \in G$ é chamado caráter principal.

Dado um caráter χ de G, definimos o caráter $\overline{\chi}$ de G por

$$\overline{\chi}(x) = \overline{\chi(x)} \ , \ x \in G,$$

onde $\overline{\chi(x)}$ é o conjugado complexo do número $\chi(x)$. Observe que $\overline{\chi} = \chi^{-1} = 1/\chi$.

Os caracteres são classificados em dois tipos: se $\chi(-1) = 1$, então χ é chamado par; se $\chi(-1) = -1$, então χ é chamado ímpar. Como $(\chi(-1))^2 = \chi((-1)^2) = \chi(1) = 1$, então $\chi(-1) = \pm 1$ e, portanto, todo caráter χ é par ou ímpar.

DEFINIÇÃO II.I.2. Um homomorfismo $\chi: \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \longrightarrow \mathbb{C}^*$ é chamado de caráter de Dirichlet módulo n.

DEFINIÇÃO II.I.3. Seja χ caráter de Dirichlet módulo n, $\chi: \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \longrightarrow \mathbb{C}^*$. Podemos definir um caráter módulo m $\chi': \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \longrightarrow \mathbb{C}^*$, $n|m$, como se segue:

Se $(a,m) = 1$ (e, portanto $(a,n) = 1$), ponha $\chi'(a) = \chi(a)$.

Se $(a,m) \neq 1$, ponha $\chi'(a) = 0$.

Dizemos que χ' é induzido pelo caráter χ .

TEOREMA II.1.1. Um caráter de Dirichlet χ' módulo m é induzido de

um caráter de Dirichlet χ módulo n $(n|m)$ se, e somente se, $\chi'(x) = 1$ se $(x,m) = 1$ e $x \equiv 1 \pmod{n}$.

DEMONSTRAÇÃO:

Se χ' é induzido de um caráter χ, então

$$\chi'(x) = \chi(x) \quad \forall\, x,\ (x,m) = 1.$$

Se $x \equiv 1 \pmod{n}$, então $\chi'(x) = \chi(x) = \chi(1) = 1$.

Reciprocamente, assumamos que para n divisor próprio de m, temos $\chi'(x) = 1$ para qualquer x tal que $(x,m) = 1$ e $x \equiv 1 \pmod{n}$. Para qualquer a, $(a,n) = 1$, podemos achar x_0 tal que $(x_0,m) = 1$ e $x_0 \equiv a \pmod{n}$. Coloquemos $\chi(a) = \chi'(x_0)$. Afirmo que o valor $\chi(a)$ não depende da escolha de x_0. De fato, se $x_0 \equiv x_0' \pmod{n}$, onde $(x_0',m) = 1$, então $x_0' \equiv x x_0 \pmod{m}$ para algum x primo com m, pois $(x_0,m) = (x_0',m) = 1$. Como $x \equiv 1 \pmod{n}$, temos por hipótese que $\chi'(x) = 1$. Então, $\chi'(x_0') = \chi'(x)\chi'(x_0) = \chi'(x_0)$. Pondo $\chi(a) = 0$ quando $(a,n) \neq 1$, obtemos χ. Como $\chi'(a) = \chi(a)$ para $(a,m) = 1$, então χ' é induzido pelo caráter χ. ■

Em termos de $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$, a situação é essa: o caráter χ' é induzido pelo caráter χ se $\chi' = \chi\theta$ para algum χ em $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$, onde θ é o homomorfismo canônico sobrejetor $\theta: \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \longrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$.

$$\begin{array}{ccc} \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* & \xrightarrow{\quad\chi'\quad} & \mathbb{C}^* \\ & {\scriptstyle\theta}\searrow \quad \nearrow{\scriptstyle\chi} & \\ & \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* & \end{array}$$

Então, χ' é induzido de χ se, e somente se χ é trivial em $\ker\theta$

TEOREMA II.1.2. Seja χ um caráter de Dirichlet mod f. Se χ é induzido de um caráter χ_1 mod n_1 e também de um caráter χ_2 mod n_2, então χ é induzido de um caráter χ_3 mod (n_1,n_2), onde $(n_1,n_2) = \text{mdc}\,(n_1,n_2)$.

DEMONSTRAÇÃO:

Suponhamos que χ é definido mod h, onde $n_1|h$ e $n_2|h$ e seja $d = (n_1, n_2)$. Pelo teorema anterior, é suficiente mostrarmos que se $(x,h) = 1$ e $x \equiv 1 \pmod{d}$, então $\chi(x) = 1$. Pelo Teorema do Resto Chinês, existe inteiro $a \equiv 1 \pmod{n_1}$, com $a \equiv x \pmod{n_2}$. Podemos assumir que $(a,h) = 1$. Seja $b \equiv xa^{-1} \pmod{h}$. Então $b \equiv 1 \pmod{n_2}$ e $b \equiv x \pmod{n_1}$. Uma vez que $x \equiv ab \pmod{h}$, então $\chi(x) = \chi(a)\ \chi(b) = 1$. ■

Dessa forma, chegamos ao menor divisor f_χ de f tal que χ não é induzido de um caráter mod n_3, para um divisor n_3 de f_χ, $n_3 \neq f_\chi$. Chamamos tal f_χ de condutor de χ.

Muitas vezes olharemos χ como uma aplicação $\mathbb{Z} \longrightarrow \mathbb{C}$, pondo $\chi(a) = 0$ se $(a, f_\chi) \neq 1$.

Chamamos de caráter primitivo ao caráter χ definido módulo seu condutor e denotaremos por χ_0.

TEOREMA II.1.3. Se $\chi: G \longrightarrow \mathbb{C}^*$ é um caráter não principal, então

$$\sum_{x \in G} \chi(x) = 0$$

DEMONSTRAÇÃO:

Como χ é não principal, existe $z \in G$ tal que $\chi(z) \neq 1$.

Se x percorre todos os elementos de G, então zx também percorre todos os elementos de G. Logo, se $S = \sum_{x \in G} \chi(x)$, então

$$S = \sum_{x \in G} \chi(zx) = \sum_{x \in G} \chi(z)\chi(x) = \chi(z)S.$$

Portanto, $S = 0$, uma vez que $\chi(z) \neq 1$. ■

No capítulo III, G será o grupo multiplicativo $\mathcal{R}_f$ de classes de resíduos primos com f módulo o subgrupo gerado pelas classes 1 e -1, isto é, $\mathcal{R}_f = \left(\frac{\mathbb{Z}}{f\mathbb{Z}}\right)^* \Big/ (\pm 1)$, onde $f > 1$ é um natural.

II.2. L-SÉRIES DE DIRICHLET

Este parágrafo destina-se a mostrar alguns fatos básicos sobre L-séries, bem como relacionar as L-séries com o número de classes h de corpos ciclotômicos.

DEFINIÇÃO II.2.1. Seja χ um caráter de condutor f_χ. A L-série determinada por χ é definida por

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad s > 1, \ s \text{ real.}$$

TEOREMA II.2.1. Para $s > 1$, $L(s,\chi)$ pode ser representada como produto de Euler convergente

$$L(s,\chi) = \prod_{p} (1-\chi(p)p^{-s})^{-1}$$

onde p percorre todos os números primos.

DEMONSTRAÇÃO:

Temos

$$\prod_{p<A} (1-\chi(p)p^{-s})^{-1} = \prod_{p<A} \sum_{k=0}^{\infty} \left(\frac{\chi(p)}{p^s}\right)^k = \sum_{n}' \frac{\chi(n)}{n^s}$$

onde, na soma $\sum'$, n percorre os inteiros que não excedem A.

Logo,

$$\left| \prod_{p<A} (1-\chi(p)p^{-s})^{-1} - \sum_{n} \frac{\chi(n)}{n^s} \right| \leq \sum_{n \geq A} \frac{1}{n^s}$$

Como $s > 1$, a série $\sum_n \frac{1}{n^s}$ converge e, então,

$$\sum_{n \geq A} \frac{1}{n^s} \longrightarrow 0 \text{ quando } A \longrightarrow \infty . \quad \blacksquare$$

As funções $L(s,\chi)$ podem ser estendidas analiticamente a todo o plano complexo, exceto por um polo simples em $s = 1$ quando $\chi = 1$.

Nosso objetivo, agora, é calcular $\prod_{\chi \neq 1} L(1,\chi)$. Para isso, faremos uma série de considerações.

DEFINIÇÃO II.2.2. Se K é um corpo numérico, então a função zeta de Dedekind $\zeta_K(s)$ é definida por

$$\zeta_K(s) = \sum_{\mathcal{A}} \frac{1}{N(\mathcal{A})^s} \qquad (1)$$

onde $\mathcal{A}$ percorre todos os ideais inteiros do corpo K.

A função zeta de Dedekind para $\mathbb{Q}$ coincide com a função zeta de Riemann $\zeta(s)$,

$$\zeta_{\mathbb{Q}}(s) = \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

A série acima converge para $s > 1$. De fato, como a função $\frac{1}{x^s}$ é decrescente para $x > 0$, então

$$\int_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{dx}{x^s},$$

onde a primeira desigualdade vale para $n \geq 1$ e a segunda para $n \geq 2$. Então para $N > 1$ temos

$$\int_1^N \frac{dx}{x^s} < \sum_{n=1}^{N-1} \frac{1}{n^s} < 1 + \int_1^{N-1} \frac{dx}{x^s}.$$

Logo a série $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converge para $s > 1$, pois a integral $\int_1^{\infty} \frac{dx}{x^s}$ converge para $s > 1$.

Além disso, para $s > 1$ temos

$\lim_{N\to\infty} \int_1^N \frac{dx}{x^s} = \frac{1}{s-1}$ e, então $\frac{1}{s-1} < \sum_{n=1}^{\infty} \frac{1}{n^s} < 1 + \frac{1}{s-1}$, ou seja,

$$1 < (s-1)\zeta(s) < s.$$

Portanto, $\lim_{s\to 1^+} (s-1)\zeta(s) = 1$ (2)

TEOREMA II.2.2. Para $s > 1$, a função $\zeta_K(s)$ pode ser representada como um produto infinito convergente

$$\zeta_K(s) = \prod_{\mathcal{P}} \frac{1}{1-[1/N(\mathcal{P})^s]},$$

onde $\mathcal{P}$ percorre todos os ideais primos do corpo K.

DEMONSTRAÇÃO:

Para todo ideal primo $\mathcal{P}$ temos

$$\frac{1}{1-[1/N(\mathcal{P})^s]} = 1 + \frac{1}{N(\mathcal{P})^s} + \frac{1}{N(\mathcal{P})^{2s}} + \cdots \qquad (3)$$

Dado $N \in \mathbb{N}$, sejam $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r$ todos os ideais primos de K tais que $N(\mathcal{P}_i) \leq N$. Assim,

$$\prod_{N(\mathcal{P})\leq N}\left(1 - \frac{1}{N(\mathcal{P})^s}\right)^{-1} = \sum_{k_1,\ldots,k_r=0}^{\infty} \frac{1}{N(\mathcal{P}_1^{k_1}\cdots\mathcal{P}_r^{k_r})^s} = \sum_{\mathcal{A}}{}' \frac{1}{N(\mathcal{A})^s}$$

onde $\mathcal{A}$ percorre todos os ideais inteiros de K que não são divisíveis por um ideal primo com norma maior que N. Então,

$$\left|\prod_{N(\mathcal{P})\leq N}\left(1 - \frac{1}{N(\mathcal{P})^s}\right)^{-1} - \zeta_K(s)\right| < \sum_{N(\mathcal{A})>N} \frac{1}{N(\mathcal{A})^s}$$

Como para $s > 1$ a série (1) converge (ver Teorema II.2.8), então

$$\sum_{N(\mathcal{A})>N} \frac{1}{N(\mathcal{A})^s} \longrightarrow 0 \text{ quando } N \longrightarrow \infty$$

e o teorema está provado. ∎

Obteremos adiante, a fórmula

$$\lim_{s\to 1^+} (s-1)\zeta_K(s) = h\varkappa, \qquad (4)$$

onde h é o número das classes de ideais de K e $\varkappa$ é uma constante que depende do corpo K.

Quebremos as séries (4) na soma de h séries

$$\zeta_K(s) = \sum_{C}\left(\sum_{\mathcal{A}\in C} \frac{1}{N(\mathcal{A})^s}\right),$$

onde $\mathcal{A}$ percorre todos os inteiros de uma classe de ideais C e a soma externa é tomada sobre todas as h classes C.

Para provarmos que as séries (1) convergem é suficiente mostrarmos que cada uma das séries

$$f_C(s) = \sum_{\mathscr{A}\in C} \frac{1}{N(\mathscr{A})^s} \qquad (5)$$

converge para $s > 1$. Mais ainda, mostraremos que para cada classe C, o limite

$$\lim_{s\to 1^+} (s-1) f_C(s)$$

existe e tem o mesmo valor w para cada classe de ideais C e, então, obteremos a fórmula (4).

Vamos, agora, transformar as séries (5) em séries sobre certos inteiros de K. Na classe inversa C^{-1} escolhamos um ideal inteiro $\mathscr{A}'$. Então, dado $\mathscr{A} \in C$ o produto $\mathscr{A}\mathscr{A}'$ será um ideal principal $\mathscr{A}\mathscr{A}' = (\omega)$, $(\alpha \in K)$.

É evidente que a aplicação

$$\mathscr{A} \mapsto (\omega) \quad (\mathscr{A} \in C)$$

é injetora. Uma vez que

$$N(\mathscr{A})N(\mathscr{A}') = |N(\alpha)|,$$

então $\frac{1}{N(\mathscr{A})} = \frac{N(\mathscr{A}')}{|N(\alpha)|}$ e, conseqüentemente,

$$f_C(s) = \sum_{\substack{\mathscr{A}\in C \\ \mathscr{A} \text{ inteiro}}} \frac{1}{N(\mathscr{A})} = N(\mathscr{A}')^s \sum_{\substack{(\omega) \\ \alpha\equiv 0 (\mathrm{mod}\ \mathscr{A}')}} \frac{1}{|N(\alpha)|^s}, \qquad (6)$$

onde a soma é sobre todos os ideais principais de K que são divisíveis por $\mathscr{A}$. Como dois ideais principais (α_1) e (α_2) são iguais se, e somente se α_1 e α_2 são associados, então podemos considerar que a soma acima é tomada sobre um conjunto completo de números não-nulos dois a dois não associados de K que são divisíveis por $\mathscr{A}'$.

Coloquemos as séries (6) numa forma mais conveniente.

Utilizaremos a notação do Teorema I.3.6. Seja $\mathcal{L}^{r_1,r_2}$ o espaço dos vetores dados por

$$x = (x_1,\ldots,x_{r_1},x_{r_1+1},\ldots,x_{r_1+r_2}),$$

onde os r_1 primeiros componentes são reais e o restante são complexos.

Definamos as seguintes aplicações:

$$\begin{aligned} x\colon K &\longrightarrow \mathcal{L}^{r_1,r_2} \\ \alpha &\longmapsto (\sigma_1(\alpha),\ldots,\sigma_{r_1+r_2}(\alpha)) \end{aligned}$$

$$\begin{aligned} l\colon \mathcal{L}^{r_1,r_2}-(0) &\longrightarrow \mathbb{R}^{r_1+r_2} \\ x &\longmapsto (l_1(x),\ldots,l_{r_1+r_2}(x)) \end{aligned}$$

onde $\begin{cases} l_k(x) = \ln|x_k| & k = 1,\ldots,r_1 \\ l_{r_1+j}(x) = 2\ln|x_{r_1+j}| & j = 1,\ldots,r_2 \end{cases}$

Se $\alpha \in K$, $\alpha \neq 0$, então escrevemos $l(\alpha) = l(x(\alpha))$.

É evidente que se $x,y \in \mathcal{L}^{r_1,r_2}-(0)$, então $l(xy) = l(x)+l(y)$.

Seja $(\varepsilon_1,\ldots,\varepsilon_r)$ um sistema fundamental de unidades de K, onde $r = r_1+r_2-1$. Os vetores $l(\varepsilon_1),\ldots,l(\varepsilon_r) \in \mathbb{R}^{r_1+r_2}$ são linearmente independentes. Como $1^* = (\underbrace{1,\ldots,1}_{r_1},\underbrace{2,\ldots,2}_{r_2}) \notin \langle l(\varepsilon_i)\rangle$, então

$$1^*, l(\varepsilon_1),\ldots,l(\varepsilon_r)$$

formam uma base para $\mathbb{R}^{r_1+r_2}$.

Assim, qualquer vetor $l(x) \in \mathbb{R}^{r_1+r_2}$ $(x \in \mathbb{R}^n,\ N(x) \neq 0)$ pode ser representado na forma

$$l(x) = \xi 1^* + \xi_1 l(\varepsilon_1) + \cdots + \xi_r l(\varepsilon_r) \qquad (7)$$

onde $\xi,\xi_1,\ldots,\xi_r$ são números reais.

Seja W o grupo das raízes da unidade contidas em K e $m = \#W$.

DEFINIÇÃO II.2.3. Um subconjunto X de $\mathbb{R}^n$ é dito um domínio fundamental para K se consiste de todos os pontos x que satisfazem:

i) $N(x) \neq 0$

ii) $l(x)$ é tal que os ξ_i satisfazem $0 \leq \xi_i < 1$, $i = 1,\ldots,r$.

iii) $0 \leq \arg x_1 < \frac{2\pi}{m}$, onde x_1 é o primeiro componente de x.

DEFINIÇÃO II.2.4. Um subconjunto Z de $\mathbb{R}^n$ é dito um cone se para qualquer $x \in Z$, $x \neq 0$ tivermos $\xi x \in Z$, onde $0 < \xi < \infty$.

LEMA II.2.3. Um domínio fundamental X é um cone.

DEMONSTRAÇÃO:

Sejam $x \in X$ e ξ um número real positivo. Afirmo que $\xi x \in X$, provando com isso que X é cone. De fato:

i) $N(\xi x) = \xi^n N(x) \neq 0$.

ii) $l(\xi x) = l(\xi)+l(x) = (\underbrace{\ln\xi,\ldots,\ln\xi}_{r_1},\underbrace{2\ln\xi,\ldots,2\ln\xi}_{r_2})+l(x)$

$= \ln\xi \cdot 1^* + l(x)$.

Assim, se $l(x) = \gamma 1^* + \sum_{i=1}^{r} \gamma_i l(\varepsilon_i)$, $0 \leq \gamma_i < 1$, então

$$l(\xi x) = (\gamma+\ln\xi)1^* + \sum_{i=1}^{r} \gamma_i l(\varepsilon_i), \quad 0 \leq \gamma_i < 1.$$

iii) $\arg(\xi x_1) = \arg x_1$. ∎

LEMA II.2.4. Se $y \in \mathbb{R}^n$ e $N(y) \neq 0$, então y tem uma representação única na forma

$$y = xx(\varepsilon), \tag{8}$$

onde x é um ponto do domúnio fundamental X e ε é uma unidade de K.

DEMONSTRAÇÃO:

Seja $l(y) = \gamma l^{*} + \sum_{i=1}^{r} \gamma_i l(\varepsilon_i)$ e para $j = 1,\ldots,r$ seja

$$\gamma_j = k_j + \xi_j$$

onde k_j é inteiro e $0 \leq \xi_j < 1$. Seja $\eta = \prod_{i=1}^{r} \varepsilon_i^{k_i}$ uma unidade de A^{*} e considere $z = yx(\eta^{-1}) \in \mathbb{R}^n$. Temos

$$\begin{aligned} l(z) &= l(y) - l(\eta) \\ &= \gamma l^{*} + \sum_{i=1}^{r} \gamma_i l(\varepsilon_i) - \sum_{i=1}^{r} k_i l(\varepsilon_i) \\ &= \gamma l^{*} + \sum_{i=1}^{r} (\gamma_i - k_i) l(\varepsilon_i) \\ &= \gamma l^{*} + \sum_{i=1}^{r} \xi_i l(\varepsilon_i). \end{aligned}$$

Seja $\varphi = \arg z_1$. Para algum inteiro k,

$$0 \leq \varphi - \frac{2\pi k}{m} < \frac{2\pi}{m}.$$

Denotemos por ζ a raiz m-ésima da unidade para o qual

$$\sigma_1(\zeta) = \cos\frac{2\pi}{m} + i \operatorname{sen}\frac{2\pi}{m}.$$

Afirmo que $x = zx(\zeta^{-k})$ pertence aó domínio fundamental X. De fato:

$$l(x) = l(z) - kl(\zeta) = l(z) = \gamma l^{*} + \sum_{i=1}^{r} \xi_i l(\varepsilon_i),$$

onde $0 \leq \xi_i < 1$. Logo as condições (i) e (ii) estão satisfeitas. Além disso, $x_1 = z_1 x(\zeta^{-k})_1 = z_1 \sigma_1(\zeta)^{-k}$ e, então

$$\arg x_1 = \arg z_1 - k\frac{2\pi}{m} = \varphi - k\frac{2\pi}{m}.$$

Logo, $0 \leq \arg x_1 < \frac{2\pi}{m}$ e, portanto, $x \in X$.

Conseguimos, então, escrever y como

$$y = zx(\eta) = xx(\zeta^{k})x(\eta) = xx(\varepsilon),$$

onde $x \in X$ e $\varepsilon = \zeta^{k}\eta$ é uma unidade de K.

Mostremos a unicidade. Suponhamos que $y = x'x(\varepsilon')$, onde $x' \in X$ e ε' é uma unidade de K. Como $xx(\varepsilon) = x'x(\varepsilon')$, então

$l(x)+l(\varepsilon) = l(x')+l(\varepsilon')$, ou seja, $l(x)-l(x') = l(\varepsilon')-l(\varepsilon)$.

Se $\varepsilon = \zeta_1 \prod_{i=1}^{r} e_i^{k_i}$ e $\varepsilon' = \zeta_2 \prod_{i=1}^{r} e_i^{m_i}$, com $k_i, m_i \in \mathbb{Z}$, então $l(\varepsilon')-l(\varepsilon) \in \sum_{i=1}^{r} \mathbb{Z}\, l(\varepsilon_i)$. Mas, se $l(x') = \gamma' 1^* + \sum_{i=1}^{r} \xi'_i\, l(\varepsilon_i)$, então $l(x')-l(x) = (\gamma'-\gamma)1^* + \sum_{i=1}^{r} (\xi'_i-\xi_i)\, l(\varepsilon_i)$. Logo,

$$l(\varepsilon')-l(\varepsilon) = (\gamma'-\gamma)1^* + \sum_{i=1}^{r} (\xi'_i-\xi_i)\, l(\varepsilon_i)$$

e, como $0 \leq \xi'_i, \xi_i < 1$, então $\gamma' = \gamma$ e $\xi'_i = \xi_i$. Assim, $l(\varepsilon') = l(\varepsilon)$. Logo $\varepsilon' = \varepsilon\zeta_0$, onde ζ_0 é uma raiz m-ésima da unidade. Conseqüentemente, $x(\varepsilon') = x(\varepsilon)x(\zeta_0)$ e, então $xx(\varepsilon) = x'x(\varepsilon') = x'x(\varepsilon)x(\zeta_0)$. Logo, $x = x'x(\zeta_0)$ e, assim, $x_1 = x'_1\sigma_1(\zeta_0)$.

Temos, por hipótese,

$$0 \leq \arg x_1 < \frac{2\pi}{m} \text{ e } 0 \leq \arg x'_1 < \frac{2\pi}{m}.$$

Então, $0 \leq |\arg \sigma_1(\zeta_0)| < \frac{2\pi}{m}$, ou seja, $\arg \sigma_1(\zeta_0) = 0$. Logo, $\sigma_1(\zeta_0) = 1$ e $\zeta_0 = 1$.

Portanto, $x = x'$ e $\varepsilon = \varepsilon'$ e lema está provado. ■

TEOREMA II.2.5. Em toda classe de inteiros ($\neq 0$) associados do corpo K existe um único número cuja representação geométrica no espaço $\mathbb{R}^n$ pertence ao domínio fundamental X.

DEMONSTRAÇÃO:

Seja $\beta \in K$, $\beta \neq 0$. Pelo lema anterior, podemos escrever $x(\beta) = xx(\varepsilon)$, onde $x \in X$ e ε é uma unidade. O número $\alpha = \beta\varepsilon^{-1}$ é associado com β e $x(\alpha) = x \in X$. Como a representação é única, o número α que satisfaz $\beta = \alpha\varepsilon$ e $x(\alpha) \in X$ é unicamente determinado. ■

Voltemos à série (6). Se denotarmos por $\mathcal{M}$ à rede n-dimensional em $\mathbb{R}^n$ que consiste de todas as imagens $x(\alpha)$, onde α é um inteiro de K divisível por $\mathcal{A}$, então como $|N(\alpha)| = |N(x(\alpha))|$, podemos escrever (6) na forma

$$f_C(s) = N(\mathcal{A})^s \sum_{x \in \mathcal{M} \cap X} \frac{1}{|N(x)|^s}, \qquad (9)$$

onde a soma é sobre todos os pontos $x = x(\alpha)$ na rede $\mathcal{M}$ contidos em X.

LEMA II.2.6. Se T é o conjunto definido por

$$T = \left\{ x \in X;\ |N(x)| \leq 1 \right\},$$

então T é limitado.

DEMONSTRAÇÃO:

Em todo raio contido no cone X existe um único ponto x para o qual $|N(x)| = 1$. Denotemos por S ao conjunto de todos os pontos de X com tais características. É claro que podemos escrever

$$T = \left\{ \xi x \in X;\ x \in S,\ 0 < \xi \leq 1 \right\}.$$

Seja $x \in \mathbb{R}^n$ um ponto com norma não-nula. Temos

$$l(x) = \xi l^* + \xi_1 l(\varepsilon_1) + \cdots + \xi_r l(\varepsilon_r).$$

Calculemos a soma dos componentes desse vetor. Do lado esquerdo temos $l(x) = (l_1(x), \ldots, l_{r_1+r_2}(x))$. Logo, a soma é igual a $\sum_{i=1}^{r_1+r_2} l_i(x) = \sum_{i=1}^{r_1} \ln|x_i| + \sum_{i=1}^{r_2} \ln|x_{r_1+i}|^2 = \ln |N(x)|$.

Do lado direito temos

$$\xi l^* + \xi_1 l(\varepsilon_1) + \cdots + \xi_r l(\varepsilon_r) = \xi(1, \ldots, 1, 2, \ldots, 2) +$$

$$+ \zeta_1(l_1(\varepsilon_1), \ldots, l_{r_1+r_2}(\varepsilon_1)) + \cdots + \zeta_r(l_1(\varepsilon_r), \ldots, l_{r_1+r_2}(\varepsilon_r)).$$

Temos $|N(\varepsilon_i)| = 1$ $\forall i = 1, \ldots, r$ e, logo, $\ln|N(\varepsilon_i)| = 0$. Então,

$\sum_{k=1}^{r_1+r_2} l_k(\varepsilon_i) = \ln |N(\varepsilon_i)| = 0$ $\forall i = 1,\ldots,r$ e a soma do lado direito é igual a $\xi(r_1+2r_2) = n\xi$.

Logo, $\ln |N(x)| = n\xi$, ou seja, $\xi = \frac{1}{n} \ln |N(x)|$. Então temos

$$l(x) = \frac{1}{n} \ln |N(x)| \, 1^* + \sum_{i=1}^{r} \xi_i l(\varepsilon_i). \qquad (10)$$

Se $x \in S$, então $\ln |N(x)| = 0$. Logo,

$$l(x) = (l_1(x),\ldots,l_{r_1+r_2}(x)) \in \mathbb{R}^{r_1+r_2}$$

é representado na forma $l(x) = \sum_{i=1}^{r} \xi_i l(\varepsilon_i)$, onde $0 \leq \xi_i < 1$. Assim, existe uma constante ρ tal que $l_j(x) < \rho$ $\forall j = 1,\ldots,r_1+r_2$, ou seja ρ tal que

$$\begin{cases} \ln |x_k| < \rho & k = 1,\ldots,r_1 \\ \ln |x_{r_1+j}|^2 < \rho & j = 1,\ldots,r_2 \end{cases}$$

Então, $|x_k| < e^{\rho}$ para $1 \leq k \leq r_1$ e $|x_{r_1+j}| < e^{\rho/2}$ para $1 \leq j \leq r_2$, para todo $x \in S$.

Portanto S e, conseqüentemente T, é limitado. ∎

Assumiremos dois resultados:

- Em qualquer transformação linear não-singular, o volume de um conjunto é multiplicado pelo valor absoluto do determinante da matriz de transformação.

- Se ε é uma unidade do corpo K, então a transformação linear do espaço $\mathbb{R}^n$ dado por $x \longrightarrow x\sigma(\varepsilon)$ preserva o volume.

Seja ζ uma raiz m-ésima da unidade com $\sigma_1(\zeta) = \cos\frac{2\pi}{m} + i \operatorname{sen}\frac{2\pi}{m}$. Consideremos os conjuntos T_k $(k = 0,\ldots,m-1)$ obtidos de T pelas transformações lineares $x \longrightarrow x\sigma(\zeta^k)$ $(T_0 = T)$. Temos, então $v(T_k) = v(T)$. Como

$$|N(x\times(\zeta^k))| = |N(x)N(\zeta^k)| = |N(x)|,$$

$$l(x\times(\zeta^k)) = l(x) + l(\zeta^k) = l(x),$$

$$\arg (x\times(\zeta^k))_1 = \arg x_1 + \frac{2\pi}{m} k,$$

então (pela definição do domínio fundamental X) o conjunto T_k consiste de todos os pontos $x \in \mathbb{R}^n$ para os quais:

i) $0 < |N(x)| \leq 1$.

ii) $l(x) = \frac{1}{n} \ln|N(x)| \, 1^* + \sum_{i=1}^{r} \xi_i l(\varepsilon_i)$ com $0 \leq \xi_i < 1$.

iii) $\frac{2\pi}{m} k \leq \arg x_1 < \frac{2\pi}{m} (k+1)$.

Então, T_0, T_1,..., T_{m-1} são disjuntos dois a dois e sua união $\bigcup_{k=0}^{m-1} T_k$ é definida pelas ocndições (i) e (ii). Seja $\bar{T}$ o conjunto de todos os pontos $x \in \bigcup_{k=0}^{m-1} T_k$ tais que $x_1 > 0, \ldots, x_{r_1} > 0$. Fixemos um conjunto de r_1 sinais $\delta_1, \ldots, \delta_{r_1}$ ($\delta_i = \pm 1$). Se multiplicarmos todos os pontos de $\mathbb{R}^n$ por $(\delta_1, \ldots, \delta_{r_1}, 1, \ldots, 1) \in \mathscr{L}^{r_1, r_2}$, obtemos uma transformação linear de $\mathbb{R}^n$ que preserva o volume. Se aplicarmos as 2^{r_1} transformações lineares possíveis a $\bar{T}$, obtemos 2^{r_1} conjuntos disjuntos dois a dois cuja união coincide com $\bigcup_{k=0}^{m-1} T_k$. Se $\bar{T}$ tem volume não-nulo $\bar{v}$, então

$$v(T) = \frac{2^{r_1}}{m} \bar{v}. \qquad (11)$$

Temos $l(x) = \frac{1}{n} \ln|N(x)| \, 1^* + \sum_{i=1}^{r} \xi_i l(\varepsilon_i)$, ou seja,

$$(l_1(x), \ldots, l_{r_1+r_2}(x)) = \frac{1}{n} \ln|N(x)| \, (\underbrace{1, \ldots, 1}_{r_1}, \underbrace{2, \ldots, 2}_{r_2}) +$$

$$+ \left(\sum_{k=1}^{r} \xi_k \, l_1(\varepsilon_k), \ldots, \sum_{k=1}^{r} \xi_k \, l_{r_1+r_2}(\varepsilon_k) \right), \text{ ou seja,}$$

$$l_j(x) = \frac{e_j}{n} \ln|N(x)| + \sum_{k=1}^{r} \xi_k \, l_j(\varepsilon_k) \quad (j = 1, \ldots, r_1+r_2)$$

onde $e_j = \begin{cases} 1 \text{ se } 1 \le j \le r_1 \\ 2 \text{ se } r_1+1 \le j \le r_1+r_2 \end{cases}$

Façamos uma mudança de variáveis pelas fórmulas:

$$x_k = \rho_k . \qquad (k = 1,\ldots,r_1)$$

$$x_{r_1+j} = y_j + iz_j \quad (j = 1,\ldots,r_2)$$

onde $y_j = \rho_{r_1+j}\cos\varphi_j$

$z_j = \rho_{r_1+j}\operatorname{sen}\varphi_j$.

O jacobiano dessa transformação é dado por

$$\begin{vmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & \cos\varphi_1 & -\rho_{r_1+1}\operatorname{sen}\varphi_1 & & \\ & & & & \operatorname{sen}\varphi_1 & \rho_{r_1+1}\cos\varphi_1 & & \\ & & & & & & \ddots & \\ & & & & & & \cos\varphi_{r_2} & -\rho_{r_1+r_2}\operatorname{sen}\varphi_{r_2} \\ & & & & & & \operatorname{sen}\varphi_{r_2} & \rho_{r_1+r_2}\cos\rho_{r_2} \end{vmatrix} =$$

$$= \rho_{r_1+1}\cdots\rho_{r_1+r_2}$$

onde, no determinante, os outros elementos são nulos.

Temos $l_j(x) = \ln \rho_j^{e_j}$ e

$$N(x) = \rho_1\cdots\rho_{r_1}\cdot\left[\rho_{r_1+1}^2\cos^2\varphi_1+\rho_{r_1+1}^2\operatorname{sen}^2\varphi_1\right]\times\cdots\times$$

$$\times\left[\rho_{r_1+r_2}^2\cos^2\varphi_{r_2}+\rho_{r_1+r_2}^2\operatorname{sen}^2\varphi_{r_2}\right]$$

$$= \prod_{j=1}^{r_1+r_2}\rho_j^{e_j} .$$

Então em termos das variáveis $\rho_1,\ldots,\rho_{r_1+r_2},\varphi_1,\ldots,\varphi_{r_2}$, o conjunto $\bar{T}$ é dado pelas condições:

i) $\rho_1 > 0, \ldots, \rho_{r_1+r_2} > 0$, $\prod_{j=1}^{r_1+r_2} \rho_j^{e_j} \leq 1$.

ii) Nas equações

$$\ln \rho_j^{e_j} = \frac{e_j}{n} \ln \left(\prod_{j=1}^{r_1+r_2} \rho_j^{e_j} \right) + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_j) \quad (j = 1, \ldots, r_1+r_2)$$

os coeficientes ξ_k satisfazem $0 \leq \xi_k < 1$ $(k = 1, \ldots, r)$.

Uma vez que não impusemos nenhuma condição sobre as variáveis $\varphi_1, \ldots, \varphi_{r_2}$, elas tomam todos os valores em $[0, 2\pi)$. Troquemos $\rho_1, \ldots, \rho_{r_1+r_2}$ por novas variáveis $\xi, \xi_1, \ldots, \xi_r$ pelas fórmulas

$$\ln \rho_j^{e_j} = \frac{e_j}{n} \ln \xi + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_j) \quad (j = 1, \ldots, r_1+r_2). \tag{12}$$

Logo,
$$\xi = \prod_{j=1}^{r_1+r_2} \rho_j^{e_j} \tag{13}$$

pois $\sum_{j=1}^{r_1+r_2} e_j = n$ e $\sum_{j=1}^{r_1+r_2} l_j(\varepsilon_k) = 0$. (14)

O conjunto $\tilde{T}$ é determinado pelas condições

$$0 < \xi \leq 1, \quad 0 \leq \xi_k < 1 \quad (k = 1, \ldots, r).$$

Temos $\frac{\partial \rho_j}{\partial \xi} = \frac{\rho_j}{n\xi}$ e $\frac{\partial \rho_j}{\partial \xi_k} = \frac{\rho_j}{e_j} l_j(\varepsilon_j)$.

Então, o jacobiano da transformação acima é igual a

$$J = \begin{vmatrix} \frac{\rho_1}{n\xi} & \frac{\rho_1}{e_1} l_1(\varepsilon_1) & \cdots & \frac{\rho_1}{e_1} l_1(\varepsilon_r) \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\rho_{r_1+r_2}}{n\xi} & \frac{\rho_{r_1+r_2}}{e_{r_1+r_2}} l_{r_1+r_2}(\varepsilon_1) & \cdots & \frac{\rho_{r_1+r_2}}{e_{r_1+r_2}} l_{r_1+r_2}(\varepsilon_r) \end{vmatrix}$$

$$= \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n\xi 2^{r_2}} \begin{vmatrix} e_1 & l_1(\varepsilon_1) & \cdots & l_1(\varepsilon_r) \\ \cdots & \cdots & \cdots & \cdots \\ e_{r_1+r_2} & l_{r_1+r_2}(\varepsilon_1) & \cdots & l_{r_1+r_2}(\varepsilon_r) \end{vmatrix}$$

Somando todas as linhas à primeira, temos

$$J = \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n\xi 2^{r_2}} \begin{vmatrix} \sum_{j=1}^{r_1+r_2} e_j & \sum_{j=1}^{r_1+r_2} l_j(\varepsilon_1) & \cdots & \sum_{j=1}^{r_1+r_2} l_j(\varepsilon_r) \\ e_2 & l_2(\varepsilon_1) & \cdots & l_2(\varepsilon_r) \\ \cdots & \cdots & \cdots & \cdots \\ e_{r_1+r_2} & l_{r_1+r_2}(\varepsilon_1) & \cdots & l_{r_1+r_2}(\varepsilon_r) \end{vmatrix}$$

$$= \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n\xi 2^{r_2}} \begin{vmatrix} n & 0 & \cdots & 0 \\ e_2 & l_2(\varepsilon_1) & \cdots & l_2(\varepsilon_r) \\ \cdots & \cdots & \cdots & \cdots \\ e_{r_1+r_2} & l_{r_1+r_2}(\varepsilon_1) & \cdots & l_{r_1+r_2}(\varepsilon_r) \end{vmatrix} .$$

Portanto, $|J| = \dfrac{R}{2^{r_2}\rho_{r_1+1}\rho_{r_1+r_2}}$.

Calculemos, então, $\bar{v}$:

$$\bar{v} = \int_{(T)} \cdots \int dx_1 \cdots dx_{r_1} dy_1 dz_1 \cdots dy_{r_2} dz_{r_2}$$

$$= \int_{(T)} \cdots \int \rho_{r_1+1} \cdots \rho_{r_1+r_2} d\rho_1 \cdots d\rho_{r_1+r_2} d\varphi_1 \cdots d\varphi_{r_2}$$

$$= \int_0^{2\pi} d\varphi_1 \cdots \int_0^{2\pi} d\varphi_{r_2} \int \cdots \int \rho_{r_1+1} \cdots \rho_{r_1+r_2} d\rho_1 \cdots d\rho_{r_1+r_2}$$

$$= 2^{r_2} \pi^{r_2} \int \cdots \int |J| \rho_{r_1+1} \cdots \rho_{r_1+r_2} d\xi \, d\xi_1 \cdots d\xi_r$$

$$= \pi^{r/2} R \int_0^1 d\xi \int_0^1 d\xi_1 \cdots \int_0^1 d\xi_r = \pi^{r/2} R.$$

Portanto, pela equação (11),

$$v(T) = \frac{2^r \pi^{r/2} R}{m} . \qquad (15)$$

Seja $X \subset \mathbb{R}^n$ um cone e suponhamos $F: X \to \mathbb{R}^*_+$ tal que:

i) se $\xi > 0$ é um número real, então $F(\xi x) = \xi^n F(x)$, $x \in X$.

ii) o conjunto $T = \{x \in X;\ F(x) \leq 1\}$ é limitado e tem um volume n-dimensional $v = v(T) \neq 0$.

Seja $\mathcal{M}$ uma rede n-dimensional em $\mathbb{R}^n$ com volume do paralelepípedo fundamental dado por Δ. Consideremos a série

$$\zeta(s) = \sum_{x \in \mathcal{M} \cap X} \frac{1}{F(x)^s} \quad (s > 1) . \qquad (16)$$

TEOREMA II.2.7. A série $\zeta(s)$ acima converge para todo $s > 1$ e

$$\lim_{s \to 1^+} (s-1)\zeta(s) = \frac{v}{\Delta} . \qquad (17)$$

DEMONSTRAÇÃO:

Para todo real $r > 0$, designaremos por $\mathcal{M}_r$ à rede

$$\mathcal{M}_r = \left\{ \frac{x}{r};\ x \in \mathcal{M} \right\}.$$

Assim, $v(\mathcal{M}_r) = \frac{\Delta}{r^n}$. Se $N(r)$ é o número de pontos de $\mathcal{M}_r$ contidos em T, então

$$v = v(T) = \lim_{r \to \infty} N(r) \frac{\Delta}{r^n} = \Delta \lim_{r \to \infty} \frac{N(r)}{r^n} . \qquad (18)$$

Consideremos o conjunto rT. É claro que

$$N(r) = \#\{rT \cap \mathcal{M}\} = \#\{x \in X \cap \mathcal{M};\ F(x) \leq r^n\}.$$

Podemos ordenar os pontos de $\mathcal{M} \cap X$ em uma seqüência (x_k) de modo que $0 < F(x_1) \leq F(x_2) \leq \cdots \leq F(x_k) \leq \cdots \leq 1$. Seja $r_k = \sqrt[n]{F(x_k)}$. Então, $F(x_k) = r_k^n$ e, logo, $x_1, \ldots, x_k$ pertencem a $r_k T$, ou seja, $N(r_k) \geq k$. Mas, para qualquer $\varepsilon > 0$, $x_k \notin (r_k - \varepsilon)T$

e, então, $N(r_k-\varepsilon) < k$. Assim, $N(r_k-\varepsilon) < k \leq N(r_k)$.

Logo, $\dfrac{N(r_k-\varepsilon)}{r_k^n} < \dfrac{k}{r_k^n} \leq \dfrac{N(r_k)}{r_k^n}$ e, então

$$\frac{N(r_k-\varepsilon)}{(r_k^n-\varepsilon)^n}\,\frac{(r_k^n-\varepsilon)^n}{r_k^n} < \frac{k}{r_k^n} \leq \frac{N(r_k)}{r_k^n}\,.$$

Assim,

$$\lim_{k\to\infty}\frac{N(r_k-\varepsilon)}{(r_k^n-\varepsilon)^n}\left(1-\frac{\varepsilon}{r_k}\right)^h \leq \lim_{k\to\infty}\frac{k}{r_k^n} \leq \lim_{k\to\infty}\frac{N(r_k)}{r_k^n}$$

e, conseqüentemente, usando a fórmula (18), $\dfrac{v}{\Delta} \leq \lim\limits_{k\to\infty}\dfrac{k}{r_k^n} \leq \dfrac{v}{\Delta}$, ou seja,

$$\lim_{k\to\infty}\frac{k}{F(x_k)} = \frac{v}{\Delta}\,. \qquad (19)$$

Logo, dado $\varepsilon > 0$, $\exists\, k_o \in \mathbb{N}$ tal que se $k \geq k_o$ temos

$$\left(\frac{v}{\Delta} - \varepsilon\right) < \frac{k}{F(x_k)} < \left(\frac{v}{\Delta} + \varepsilon\right).$$

Então, $\left(\dfrac{v}{\Delta} - \varepsilon\right)^s\dfrac{1}{k^s} < \dfrac{1}{F(x_k)^s} < \left(\dfrac{v}{\Delta} + \varepsilon\right)^s\dfrac{1}{k^s}$ $\forall s > 1$ e, assim,

$$\left(\frac{v}{\Delta} - \varepsilon\right)^s\sum_{k=k_o}^{\infty}\frac{1}{k^s} < \sum_{k=k_o}^{\infty}\frac{1}{F(x_k)^s} < \left(\frac{v}{\Delta} + \varepsilon\right)^s\sum_{k=k_o}^{\infty}\frac{1}{k^s}\,.$$

Multiplicaremos essas inequações por s-1 e faremos tender a 1 pela direita. Como $\lim\limits_{s\to1}(s-1)\sum\limits_{k=1}^{k_o-1}\dfrac{1}{k^s} = 0$, então por (2), $\lim\limits_{s\to1^+}(s-1)\sum\limits_{k=k_o}^{\infty}\dfrac{1}{k^s} = 1$. Como também $\lim\limits_{s\to1}(s-1)\sum\limits_{k=1}^{k_o-1}\dfrac{1}{F(x_k)^s} = 0$, obtemos $\dfrac{v}{\Delta} - \varepsilon \leq \lim\limits_{s\to1^+}(s-1)\sum\limits_{k=k_o}^{\infty}\dfrac{1}{F(x_k)^s} \leq \dfrac{v}{\Delta} + \varepsilon$.

Portanto, $\lim\limits_{s\to1^+}(s-1)\zeta(s) = \dfrac{v}{\Delta}$. ■

Pelo teorema acima, as séries (9) convergem para $s > 1$ e

$$\lim_{s\to 1^+} (s-1) \sum_{x\in\mathcal{A}\cap X} \frac{1}{|N(x)|^s} = \frac{V}{\Delta}. \qquad (20)$$

Mas, pelo Lema I.3.7 enunciado no teorema I.3.6,

$$\Delta = 2^{-r_2}|D|^{1/2}N(\mathcal{A}), \qquad (21)$$

onde D é o discriminante do corpo K.

Usando as equações (9), (15), (20) e (21) obtemos

$$\lim_{s\to 1^+} (s-1)f_C(s) = \frac{2^{r_1+r_2}\pi^{r_2}R}{m\sqrt{|D|}}.$$

Como $\zeta_K(s) = \sum_C f_C(s)$, provamos o seguinte resultado:

TEOREMA II.2.8. Se K é um corpo numérico algébrico de grau $n = r_1+2r_2$, então as séries

$$\zeta_K(s) = \sum_{\mathcal{A}} \frac{1}{N(\mathcal{A})^s}$$

convergem para todo $s > 1$. Além disso, temos a fórmula

$$\lim_{s\to 1^+} (s-1)\zeta_k(s) = \frac{2^{r_1+r_2}\pi^{r_2}R}{m\sqrt{|D|}}\, h,$$

onde h, D e R denotam o número das classes de ideais, o discriminante e o regulador de um corpo K, respectivamente, e m é o número de raízes da unidade contidas em K. ■

Seja $\zeta_K(s)$ a função ζ do m-ésimo corpo ciclotômico $K = \mathbb{Q}(\zeta)$, $\zeta^m = 1$. Podemos escrever

$$\zeta_K(s) = \prod_{\mathcal{P}} \frac{1}{1-[1/N(\mathcal{P})^s]} = \prod_p \prod_{\mathcal{P}|p} \frac{1}{1-[1/N(\mathcal{P})^s]}.$$

onde o produto é tomado sobre todos os primos racionais p. Seja

$$G(s) = \prod_{\mathcal{P}|m} \left(1 - \frac{1}{N(\mathcal{P})^s}\right)^{-1}. \qquad (22)$$

Se $(p, m) = 1$ e $\mathcal{P}$ é um ideal primo qualquer de p, então $N(\mathcal{P}) = p^{f_p}$,

onde f_p é a ordem de p módulo m. Como o número de distintos $\mathfrak{P}$ que dividem p é $\varphi(m)/f_p$, então

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \left(1 - \frac{1}{p^{f_p s}}\right)^{-\varphi(m)/f_p}. \qquad (23)$$

Mas,

$$1 - \left(\frac{1}{p^s}\right)^{f_p} = \prod_{k=0}^{f_p-1} \left(1 - \frac{\varepsilon^k}{p^s}\right), \qquad (24)$$

onde $\varepsilon = \varepsilon_p = \cos(2\pi/f_p) + i\,\mathrm{sen}(2\pi/f_p)$.

Assim,

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \prod_{k=0}^{f_p-1} \left(1 - \frac{\varepsilon_{f_p}^k}{p^s}\right)^{-\varphi(m)/f_p}$$

$$= G(s) \prod_{(p,m)=1} \prod_{\chi \bmod m} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \qquad (25)$$

pois: i) para cada caráter $\chi: \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \to \mathbb{C}^*$, temos $\chi(p) = \varepsilon_{f_p}^k$ para algum k;

ii) reciprocamente, dado ε^k, $k = 0,..,f_p-1$, existe caráter χ com $\chi(p) = \varepsilon^k$ e tais χ são exatamente em número de $\varphi(m)/f_p$.

No lugar de caracteres do grupo $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$, podemos considerar caracteres numéricos módulo m. Logo, se p é um primo que divide m, então $\chi(p) = 0$ e (25) toma a forma

$$\zeta_K(s) = G(s) \prod_{p} \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

onde p percorre todos os primos e χ percorre todos os caracteres numéricos módulo m. Se trocarmos a ordem da multiplicação obtemos

$$\zeta_K(s) = G(s) \prod_{\chi} L(s,\chi). \qquad (26)$$

Agora, $\zeta_K(s) = G(s)\, L(s,1) \prod_{\chi \neq 1} L(s,\chi)$. Mas,

$$L(s,1) = \prod_{(p,m)=1} \frac{1}{1-(1/p^s)}$$

$$= \left(\prod_{p|m} \frac{1}{1-(1/p^s)} \right)^{-1} \prod_{p} \frac{1}{1-(1/p^s)}$$

$$= \left(\prod_{p|m} \frac{1}{1-(1/p^s)} \right)^{-1} \zeta(s),$$

onde $\zeta(s)$ foi obtido pela aplicação do Teorema II.2.2 ao corpo $\mathbb{Q}$.

Portanto,

$$\zeta_K(s) = F(s)\, \zeta(s) \prod_{\chi \neq 1} L(s,\chi) \quad (s > 1), \tag{27}$$

onde

$$F(s) = \prod_{\mathcal{P}|m} \left(1 - \frac{1}{N(\mathcal{P})^s}\right)^{-1} \prod_{p|m} \left(1 - \frac{1}{p^s}\right).$$

LEMA II.2.9. Seja (a_n) $(n = 1,2,\ldots)$ seqüência de números complexos tal que as somas $A_n = \sum_{k=1}^{n} a_n$ são limitadas, isto é, $|A_n| \leq C$ para todo $n \geq 1$. Então as séries

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

convergem para todo real $s > 0$. Para todo $\sigma > 0$, a convergência é uniforme em $[\sigma,\infty)$ e $f(s)$ é contínua em s.

DEMONSTRAÇÃO:

Fixemos $\sigma > 0$. Dado $\varepsilon > 0$, seja n_o tal que $1/n^\sigma < \varepsilon$ $\forall$ $n > n_o$. Para tais inteiros $n > n_o$, temos $1/n^s < \varepsilon$, $\forall$ $s \geq \sigma$. Seja, agora, $M > N > n_o$. Então

$$\sum_{k=N}^{M} \frac{a_k}{k^s} = \sum_{k=N}^{M} \frac{A_k - A_{k-1}}{k^s} = \sum_{k=N}^{M} \frac{A_k}{k^s} - \sum_{k=N-1}^{M-1} \frac{A_k}{(k+1)^s}$$

$$= -\frac{A_{N-1}}{N^s} + \sum_{k=N}^{M-1} A_k \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) + \frac{A_M}{M^s},$$

e, logo,

$$\left| \sum_{k=N}^{M} \frac{a_k}{k^s} \right| \leq \frac{C}{N^\sigma} + C \sum_{k=N}^{M-1} \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) + \frac{C}{M^\sigma} = \frac{2C}{N^\sigma} < 2C\varepsilon$$

para todo s em $]\alpha,\omega[$. ∎

COROLÁRIO II.2.10. Para todo caráter $\chi \neq 1$, as séries $L(s,\chi)$ convergem para $s > 0$ e são funções contínuas em $(0,\infty)$. ∎

Voltando à função $\zeta_K(s)$, multipliquemos (27) por s-1 e tomemos o limite quando $s \to 1$ pela direita. Por (2),

$$\lim_{s\to 1^+} (s-1)\zeta_K(s) = F(1) \prod_{\chi\neq 1} L(1,\chi), \tag{28}$$

onde

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}. \tag{29}$$

Comparando (28) com o Teorema II.2.8, obtemos a seguinte fórmula:

$$\prod_{\chi\neq 1} L(1,\chi) = \frac{2^{r_1+r_2}\,\pi^{r_2}\,h\,R}{w\sqrt{|D|}\,F(1)}. \tag{30}$$

COROLÁRIO II.2.11. Se $K = \mathbb{Q}(\zeta_f)^+$, então

$$\prod_{\substack{\chi\neq 1\\ \chi \text{ par}}} L(1,\chi) = \frac{2^{\frac{\varphi(f)}{2}}\,h^+\,R^+}{2\sqrt{D}},$$

onde ζ_f é uma raiz primitiva f-ésima da unidade, $f \not\equiv 2 \pmod 4$, h^+ é o número de classes de K, R^+ é o regulador de K e $D = d(K)$ é o discriminante de K. ∎

LEMA II.2.12. Sejam χ um caráter de condutor f e $\tau(\chi) = \sum_{a=1}^{f} \chi(a)e^{2\pi i a/f}$ uma soma de Gauss. Então, para todo inteiro b,

$$\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi iab/f} = \chi(b)\tau(\overline{\chi}).$$

Em particular,

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

DEMONSTRAÇÃO:

Se $(b,f) = 1$, então façamos a mudança de variável $c \equiv ab \pmod f$. Logo,

$$\begin{aligned}
\chi(b)\tau(\overline{\chi}) &= \chi(b)\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi ia/f} \\
&= \chi(b)\sum_{a=1}^{f} \overline{\chi}(ab)e^{2\pi iab/f} \\
&= \chi(b)\overline{\chi}(b)\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi iab/f} \\
&= \sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi iab/f}.
\end{aligned}$$

Se $(b,f) = d > 1$, então o resultado é válido uma vez que ambos os lados se anulam. De fato:

Obviamente, $\chi(b)\tau(\overline{\chi}) = 0$.

Se para todo $c \equiv 1 \pmod{f/d}$, $(c,f) = 1$ tivermos $\chi(c) = 1$, então o condutor de χ dividiria f/d, uma contradição. Logo, existe $c \equiv 1 \pmod{f/d}$, $(c,f) = 1$ tal que $\chi(c) \neq 1$. Se $b = b'd$, então

$$\begin{aligned}
\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi iab/f} &= \sum_{a=1}^{f} \overline{\chi}(ac)e^{2\pi iabc/f} \\
&= \overline{\chi}(c)\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi iab'dc/f}.
\end{aligned}$$

Como $dc \equiv d \pmod f$, então

$$\begin{aligned}
\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi iab/f} &= \overline{\chi}(c)\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi iab'd/f} \\
&= \overline{\chi}(c)\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi iab/f}.
\end{aligned}$$

O resultado se segue, uma vez que $\overline{\chi}(c) \neq 1$. ∎

LEMA II.2.13. Usando a notação do lema acima,

$$|\tau(\chi)| = \sqrt{f}\ .$$

DEMONSTRAÇÃO:

$$\varphi(f)|\tau(\chi)|^2 = \sum_{b=1}^{f} |\chi(b)\tau(\chi)|^2 \quad \text{(apenas } \varphi(f) \text{ termos são não nulos)}$$

$$= \sum_{b=1}^{f} \overline{\chi(b)}\ \overline{\tau(\chi)}\ \chi(b)\tau(\chi)$$

$$= \sum_{b=1}^{f} \left(\overline{\chi(b)} \sum_{a=1}^{f} \bar{\chi}(a)\ e^{-2\pi i a/f}\right)\left(\chi(b) \sum_{c=1}^{f} \chi(c)\ e^{2\pi i c/f}\right)$$

$$= \sum_{b=1}^{f} \left(\sum_{a=1}^{f} \bar{\chi}(ab)\ e^{-2\pi i a/f}\right)\left(\sum_{c=1}^{f} \chi(bc)\ e^{2\pi i c/f}\right)$$

$$= \sum_{b=1}^{f} \left(\sum_{d=1}^{f} \bar{\chi}(d)\ e^{-2\pi i d b^{-1}/f}\right)\left(\sum_{g=1}^{f} \chi(g)\ e^{2\pi i b^{-1} g/f}\right)$$

$$= \sum_{d=1}^{f} \sum_{g=1}^{f} \bar{\chi}(d)\chi(g) \sum_{b=1}^{f} e^{2\pi i b^{-1}(g-d)/f}.$$

Temos

$$\sum_{b=1}^{f} e^{2\pi i b^{-1}(g-d)/f} = \sum_{b=0}^{f-1} \left(e^{2\pi i(g-d)/f}\right)^b \quad \text{pois } b^{-1} \equiv b \pmod f$$

$$= 1+\zeta+\cdots+\zeta^{f-1}\ , \text{ onde } \zeta = e^{2\pi i(g-d)/f}$$

$$= \begin{cases} f & , \text{ se } \zeta = 1 \Leftrightarrow g = d \\ \dfrac{\zeta^f - 1}{\zeta - 1} = 0 & , \text{ se } \zeta \neq 1 \end{cases}$$

Portanto

$$\varphi(f)|\tau(\chi)|^2 = \sum_{a} \chi(a)\bar{\chi}(a) f = f\varphi(f),$$

pois $\chi(a)\bar{\chi}(a) = 1$ se $(a,f) = 1$ e 0 caso contrário. ∎

LEMA II.2.14. Seja ζ uma raiz primitiva n-ésima da unidade. Então,

$$\prod_{\substack{\chi \neq 1 \\ \chi \text{ par}}} f_\chi = |d(\mathbb{Q}(\zeta)^+)| \ , \qquad (31)$$

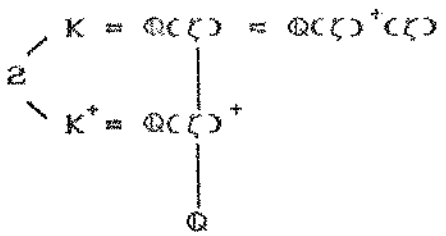
onde χ percorre os caracteres pares não triviais mod n.

DEMONSTRAÇÃO:

Vamos nos ater somente ao caso $n = p^a$, $p \neq 2$ primo. Os outros casos são demonstrados de maneira semelhante.

Demonstraremos que ambos os lados são iguais a $\frac{1}{2} p^{\frac{1}{2}(ap^a - ap^{a-1} - p^{a-1} - 1)}$.

Calculemos o lado direito de (31):



Temos $d(K) = d(K^+)^{[K:K^+]} N_{K^+|\mathbb{Q}}(D_1)$, onde $D_1 = \det(Tr_{K|K^+}(x_i x_j))$.

Uma vez que $\{1, \zeta\}$ é base integral de K sobre K^+, temos que

$$D_1 = \begin{vmatrix} Tr(1) & Tr(\zeta) \\ Tr(\zeta) & Tr(\zeta^2) \end{vmatrix} = \begin{vmatrix} 2 & \zeta+\zeta^{-1} \\ \zeta+\zeta^{-1} & \zeta^2+\zeta^{-2} \end{vmatrix}$$

$$= 2\zeta^2+2\zeta^{-2}-(\zeta^2+1+1+\zeta^{-2}) = \zeta^2+\zeta^{-2}-2$$

$$= (\zeta-\zeta^{-1})^2, \text{ onde } Tr = Tr_{K|K^+} .$$

Temos $N_{K^+|\mathbb{Q}}(\zeta-\zeta^{-1})^2 = N_{K|\mathbb{Q}}(\zeta-\zeta^{-1}) = N_{K|\mathbb{Q}}(\zeta(1-\zeta^{-2})) = N_{K|\mathbb{Q}}(1-\zeta^{-2})$. Também

$$\Phi_{p^a}(X) = X^{p^{a-1}(p-1)} + X^{p^{a-1}(p-2)} + \cdots + X^{p^{a-1}} + 1 = \prod_{\substack{i=1 \\ (i,p)=1}}^{p} (X - \zeta_{p^a}^{\,i}).$$

Se $X = Y+1$, então

$$\Phi_{p^a}(Y+1) = (Y+1)^{p^{a-1}(p-1)} + \cdots + (Y+1)^{p^{a-1}} + 1 = \prod_{(d,p^a)=1} (Y - (\zeta_{p^a}^{d} - 1)).$$

Colocando $Y = 0$, temos

$$p = \Phi_{p^a}(1) = \prod_{(d,p)=1} (1 - \zeta_{p^a}^{d}) = N_{K|\mathbb{Q}}(1 - \zeta^{-2}) .$$

Portanto, $|d(K^+)|^2 = d(K)\, p^{-1}$, ou seja

$$|d(K^+)| = p^{\frac{1}{2}(ap^a - ap^{a-1} - p^{a-1} - 1)}.$$

Calculemos, agora, o lado esquerdo de (31):

Temos que

- o número de caracteres pares de condutor 1 é 1.
- o número de caracteres pares de condutor p, $\chi: \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \to \mathbb{C}^*$, é

  $$\frac{\varphi(p)}{2} - 1 = \frac{p-3}{2} .$$

- o número de caracteres pares de condutor p^2, $\chi: \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^* \to \mathbb{C}^*$, é

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

- o número de caracteres pares de condutor p^i, $\chi: \left(\frac{\mathbb{Z}}{p^i\mathbb{Z}}\right)^* \to \mathbb{C}^*$, $(2 \le i \le a)$, é $\frac{\varphi(p^i)}{2} - \frac{\varphi(p^{i-1})}{2} = \frac{1}{2} p^{i-2}(p-1)^2$.

Portanto, $\prod_{\substack{\chi \neq 1 \\ \chi \text{ par}}} f_\chi = p^y$ onde

$$y = \frac{p-3}{2} + \frac{(p-1)^2}{2}(2 + 3p + 4p^2 + \cdots + ap^{a-2})$$

$$= \frac{p-3}{2} + \frac{(p-1)^2}{2p}(2p + 3p^2 + 4p^3 + \cdots + ap^{a-1}).$$

Seja $F(X) = 1 + X + X^2 + \cdots + X^a = \frac{X^{a+1}-1}{X-1}$. Logo,

$$F'(X) = 1 + 2X + 3X^2 + \cdots + aX^{a-1} = \frac{(a+1)X^a(X-1) - (X^{a+1}-1)}{(X-1)^2} .$$

Então, para $X = p$,

$$1 + 2p + 3p^2 + \cdots + ap^{a-1} = \frac{(a+1)p^a(p-1)-(p^{a+1}-1)}{(p-1)^2}\ , \text{ ou seja,}$$

$$2p + 3p^2 + \cdots + ap^{a-1} = \frac{ap^{a+1}-ap^a+p^{a+1}-p^a-p^{a+1}+1-(p-1)^2}{(p-1)^2}$$

$$= \frac{ap^{a+1}-ap^a-p^a-p^2+2p}{(p-1)^2}\ .$$

Conseqüentemente, $y = \frac{p-3}{2} + \frac{1}{2}(ap^a-ap^{a-1}-p^{a-1}-p+2)$

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

e a igualdade está provada. ∎

TEOREMA II.2.15. Usando a notação dos lemas anteriores,

$$\prod_{\substack{\chi\neq 1\\ \chi \text{ par}}} \tau(\chi) = \sqrt{|d(\mathbb{Q}(\zeta)^+)|}\ . \qquad (32)$$

DEMONSTRAÇÃO:

A equação (32) é equivalente a

$$\left(\prod_{\substack{\chi\neq 1\\ \chi \text{ par}}} \tau(\chi) \right)^2 = |d(\mathbb{Q}(\zeta)^+)|\ .$$

Pelo lema II.2.12, $\overline{\tau(\chi)} = \tau(\bar{\chi})$ se χ é par. Logo,

$$\left(\prod_{\substack{\chi\neq 1\\ \chi \text{ par}}} \tau(\chi) \right)^2 = \prod_{\substack{\chi\neq 1\\ \chi \text{ par}}} \tau(\chi)\overline{\tau(\chi)} = \prod_{\substack{\chi\neq 1\\ \chi \text{ par}}} |\tau(\chi)|^2 = \prod_{\substack{\chi\neq 1\\ \chi \text{ par}}} f\ ,$$

onde a última igualdade é justificada pelo Lema II.2.13.

Portanto, a equação (32) é equivalente a

$$\prod_{\substack{\chi\neq 1\\ \chi \text{ par}}} f = |d(\mathbb{Q}(\zeta)^+)| \qquad (33)$$

e o teorema está demonstrado, pois a equação (33) acima foi demonstrada no Lema II.2.14. ∎

TEOREMA II.2.16. Sejam $K = \mathbb{Q}(\zeta)$, ζ uma raiz primitiva n-ésima da unidade e E o seu grupo das unidades. Se E^+ é o grupo das unidades de $K^+ = \mathbb{Q}(\zeta)^+$ e W o grupo das raizes da unidade em K, então

$$[E:WE^+] = \begin{cases} 1 \text{ se n é uma potência de primo} \\ 2 \text{ se n não é uma potência de primo} \end{cases}$$

DEMONSTRAÇÃO:

Definamos ϕ: $E \longrightarrow W$ por $\phi(\varepsilon) = \frac{\varepsilon}{\overline{\varepsilon}}$.

Temos, para $\forall\ \sigma \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$,

$|\sigma(\phi(\varepsilon))|^2 = \left|\sigma\left(\frac{\varepsilon}{\overline{\varepsilon}}\right)\right|^2 = \left|\frac{\sigma(\varepsilon)}{\sigma(\overline{\varepsilon})}\right|^2 = \frac{\sigma(\varepsilon)}{\overline{\sigma(\varepsilon)}}\,\overline{\frac{\sigma(\varepsilon)}{\sigma(\varepsilon)}} = 1$ e, portanto, $|\sigma(\phi(\varepsilon))| = 1$, $\forall\ \sigma \in Gal(\mathbb{Q}(\zeta)\setminus\mathbb{Q})$. Logo, pelo lema I.3.5, $\phi(\varepsilon) \in W$.

Seja ψ: $E \longrightarrow W/W^2$ a aplicação induzida por ϕ.

Suponhamos $\varepsilon = \zeta\varepsilon_1$, onde $\zeta \in W$ e $\varepsilon_1 \in E^+$. Então, $\phi(\varepsilon) = \frac{\varepsilon}{\overline{\varepsilon}} = \frac{\zeta\varepsilon_1}{\overline{\zeta\varepsilon_1}} = \frac{\zeta}{\overline{\zeta}} = \zeta^2 \in W^2$ e, conseqüentemente $\varepsilon \in \ker(\psi)$, ou seja, $WE^+ \subseteq \ker(\psi)$. Reciprocamente, seja $\varepsilon \in \ker(\psi)$. Então $\phi(\varepsilon) = \zeta^2 \in W^2$ e, logo, $\frac{\varepsilon}{\overline{\varepsilon}} = \zeta^2$, ou seja, $\varepsilon = \overline{\varepsilon}\zeta^2 = \overline{\varepsilon\zeta}\zeta$. Afirmo que $\overline{\varepsilon\zeta}$ é unidade real. De fato, $\overline{\varepsilon\zeta}$ é unidade pois ε é unidade e ζ é raiz da unidade e é real pois $\overline{\overline{\varepsilon\zeta}} = \varepsilon\zeta^{-1} = \overline{\varepsilon}\zeta^2\zeta^{-1} = \overline{\varepsilon\zeta}$. Assim, $\varepsilon \in WE^+$ e, então $\ker(\psi) = WE^+$. Como $\left|\frac{W}{W^2}\right| = 2$, então $[E:WE^+] = 1$ ou 2. Notemos que se $\phi(E) = W$, então $[E:WE^+] = 2$ e se $\phi(E) = W^2$, então $[E:WE^+] = 1$.

Olhando a demonstração do Teorema I.2.11 podemos afirmar que se n é potência de um primo ímpar, então $\frac{\varepsilon}{\overline{\varepsilon}} \in W^2$, $\varepsilon \in E$ e, portanto, $[E:WE^+] = 1$.

Suponhamos, então, que n seja uma potência de 2 e que ε seja uma unidade em $\mathbb{Q}(\zeta_{2^m})$ tal que $\frac{\varepsilon}{\overline{\varepsilon}} \notin W^2$. Logo, $\frac{\varepsilon}{\overline{\varepsilon}} = \zeta$, ζ uma raiz primitiva 2^m-ésima da unidade. Se $N = N_{\mathbb{Q}(\zeta_{2^m})|\mathbb{Q}(i)}$, então $N(\zeta) = \zeta^a$, onde

$$a = \sum_{\substack{0<b<2^m \\ b\equiv 1 (4)}} b = \sum_{j=0}^{2^{m-2}-1} (1+4j) = (1+4\cdot 0)+(1+4\cdot 1)+\cdots+(1+4(2^{m-2}-1))$$

$$= 2^{m-2} + 4[1+2+\cdots+(2^{m-2}-1)] = 2^{m-2} + 2^{m-1}(2^{m-2}+1)$$

$$\equiv 2^{m-2} \pmod{2^{m-1}}.$$

Logo, ζ^a é uma raiz primitiva quarta da unidade: $\zeta^a = \pm i$. Segue que $\frac{N(\varepsilon)}{N(\varepsilon)} = N(\frac{\varepsilon}{\varepsilon}) = N(\zeta) = \pm i$. Mas, $N(\varepsilon)$ é uma unidade de $Q(i)$, ou seja, $N(\varepsilon) = \pm 1$ ou $\pm i$, uma contradição. Portanto, $\frac{\varepsilon}{\varepsilon} \in W^2$ e $[E:WE^+] = 1$.

Assumamos, agora, que n não é uma poténcia de primo. Logo, $1-\zeta$ é uma unidade. Mas, $\frac{1-\zeta}{1-\zeta} = -\zeta$. Suponhamos que $-\zeta \in W^2$. Então, $-\zeta = (\pm\zeta^r)^2 = \zeta^{2r}$ e, logo, $-1 = \zeta^{2r-1}$. Logo, n deve ser par, ou seja $n\equiv 0 \pmod 4$. Como $-1 = \zeta^{n/2}$, temos $\frac{n}{2}\equiv 2r-1 \pmod n$ e, portanto $\frac{n}{2}\equiv -1 \pmod 2$, uma contradição.

Segue que $-\zeta \notin W^2$ e, conseqüentemente, $[E:WE^+] = 2$. ∎

PROPOSIÇÃO II.2.17. Sejam $\varepsilon_1,\ldots,\varepsilon_r$ unidades independentes de um corpo numérico K que geram um subgrupo A de unidades de K módulo raízes da unidade e $\eta_1,\ldots,\eta_r$ geradores de um subgrupo B. Se $A \subseteq B$ é de índice finito, então

$$[B:A] = \frac{R_K(\varepsilon_1,\ldots,\varepsilon_r)}{R_K(\eta_1,\ldots,\eta_r)}.$$

DEMONSTRAÇÃO:

Podemos escrever

$$\varepsilon_i = \left(\prod_l \eta_l^{a_{il}}\right)\cdot(\text{raiz da unidade}), \text{ com } a_{il} \in \mathbb{Z}.$$

Portanto, $\delta_j \log|\sigma_j(\varepsilon_i)| = \sum_l a_{il}\delta_j \log|\sigma_j(\eta_l)|$ e,

conseqüentemente, $\dfrac{R_K(\varepsilon_1,\ldots,\varepsilon_r)}{R_K(\eta_1,\ldots,\eta_r)} = |\det(a_{il})|$.

Sejam $v_i = \log|\varepsilon_i|$ e $u_i = \log|\eta_i|$, com $v_i = \sum_l a_{il}u_l$.

Consideremos a transformação

$$\begin{aligned} T:\ B &\longrightarrow B \\ u_i &\mapsto v_i \end{aligned}.$$

Existem mudanças de bases (u_i) para (y_i) e (v_i) para (x_i) tais que, se M e N representam as matrizes de mudança de base de A e B, então $M(a_{il})N = \mathrm{diag}(d_1,\ldots,d_r)$. Ou seja, $\det(a_{il}) = \pm\prod_i d_i$ e $T(y_i) = x_i$. Logo, $x_i = d_i y_i$ e, portanto,

$$B/A \simeq \frac{\mathbb{Z}_{y_1}\oplus\cdots\oplus\mathbb{Z}_{y_r}}{\mathbb{Z}_{x_1}\oplus\cdots\oplus\mathbb{Z}_{x_r}} \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \text{ e } [B:A] = \left|\prod_i d_i\right|. \quad \blacksquare$$

TEOREMA II.2.18. Sejam G um grupo abeliano finito e f uma função em G com valores em um corpo C de característica zero. Então

$$\det(f(\sigma\tau^{-1})-f(\sigma))_{\sigma,\tau\neq 1} = \prod_{\chi\neq 1}\sum_{\sigma\in G}\chi(\sigma)f(\sigma).$$

DEMONSTRAÇÃO:

Consideremos o espaço vetorial finito-dimensional V de todas as funções em G, $V = \{h;\ h: G \longrightarrow C\}$ e seja ϕ_τ: $G \longrightarrow C$ a função característica de G, isto é,

$$\phi_\tau(\sigma) = \begin{cases} 1 \text{ se } \sigma = \tau \\ 0 \text{ se } \sigma \neq \tau \end{cases}.$$

Então $(\phi_\tau)_{\tau\in G}$ forma uma base de V. Seja W o subespaço de V dado por $W = \left\{h \in V;\ \sum_{\sigma\in G} h(\sigma) = 0\right\}$ e ψ_τ: $G \longrightarrow C$ definida por $\psi_\tau(X) = \phi_\tau(X) - \frac{1}{|G|}$. Como $\sum_{\sigma\in G}\psi_\tau(\sigma) = \sum_{\sigma\in G}\left[\phi_\tau(\sigma) - \frac{1}{|G|}\right] = 0$, então

$\psi_\tau \in W$, $\tau \in G$. Afirmo que $\{\psi_\tau;\ \tau \neq 1\}$ forma uma base de W. De fato:

Suponhamos que $\sum_{\tau\neq 1} a_\tau \psi_\tau = 0$.

Logo, $\sum_{\tau\neq 1} a_\tau \psi_\tau(\sigma) = = \sum_{\tau\neq 1} a_\tau(\phi_\tau(\sigma) - \frac{1}{|G|}) = 0 \quad \forall\ \sigma \in G$, ou seja, $\sum_{\tau\neq 1} a_\tau \phi_\tau(\sigma) = \sum_{\tau\neq 1} \frac{a_\tau}{|G|}$, $\forall\ \sigma \in G$. Então, $a_\sigma = \sum_{\tau\neq 1} \frac{a_\tau}{|G|}$, $\forall\ \sigma \in G$.

Portanto, $\sum_{\tau\neq 1} a_\tau \psi_\tau = 0$ implica em $a_\tau = 0$, ou seja, $\{\psi_\tau;\ \tau \neq 1\}$ são l.i.

Seja, agora, $h \in W$. Então

$$h = \sum_{\tau\neq 1} a_\tau \psi_\tau \Leftrightarrow h = \sum_{\tau\neq 1} a_\tau(\phi_\tau - \frac{1}{|G|})$$

$$\Leftrightarrow h(\sigma) = \sum_{\tau\neq 1} a_\tau(\phi_\tau(\sigma) - \frac{1}{|G|})$$

$$\Leftrightarrow \sum_{\sigma\in G} h(\sigma) = \sum_{\sigma\in G}\sum_{\tau\neq 1} a_\tau \phi_\tau(\sigma) - \sum_{\sigma\in G}\sum_{\tau\neq 1} a_\tau \frac{1}{|G|}$$

$$\Leftrightarrow \sum_{\sigma\in G} h(\sigma) = \sum_{\sigma\neq 1} a_\sigma - \sum_{\sigma\neq 1} a_\sigma \frac{1}{|G|}\ |G|$$

$$\Leftrightarrow \sum_{\sigma\in G} h(\sigma) = 0.$$

Mas, essa última igualdade é válida pois $h \in W$ e, portanto, $\{\psi_\tau;\ \tau \neq 1\}$ geram W.

Definamos a transformação linear $T = \sum_\sigma f(\sigma)\ \sigma$, $T: V \to V$.

Afirmo que $T(W) \subseteq W$. De fato,

$$T(\psi_\tau) = \sum_{\sigma\in G} f(\sigma)\sigma\psi_\tau$$

e, então,

$$\sum_{X\in G}\left[\sum_{\sigma\in G} f(\sigma)\sigma\psi_\tau(X)\right] = \sum_{X\in G}\left[\sum_{\sigma\in G} f(\sigma)\psi_\tau(\sigma X)\right]$$

$$= \sum_{\sigma\in G} f(\sigma) \sum_{X\in G} \psi_\tau(\sigma X)$$

$$= \sum_{\sigma\in G} f(\sigma) \sum_{X\in G} \psi_\tau(X)$$

$$= 0.$$

Temos

$$T(\psi_\tau) = \sum_{\sigma\in G} f(\sigma)\sigma\psi_\tau = \sum_{\sigma\in G} f(\sigma)\psi_{\sigma^{-1}\tau}$$

$$= \sum_{\theta} f(\tau\theta^{-1})\psi_\theta = \sum_{\theta\neq 1} f(\tau\theta^{-1})\psi_\theta + f(\tau)\psi_1.$$

Como $\sum_{\tau\in G} \psi_\tau(\sigma) = \sum_{\tau\in G} \phi_\tau(\sigma) - \sum_{\tau\in G} \frac{1}{|G|} = 0 \quad \forall\, \sigma \in G$, então

$$\psi_1(\sigma) = -\sum_{\tau\neq 1} \psi_\tau(\sigma)$$

e, logo,

$$T(\psi_\tau) = \sum_{\theta\neq 1} f(\tau\theta^{-1})\psi_\theta - \sum_{\theta\neq 1} f(\tau)\psi_\theta$$

$$= \sum_{\theta\neq 1} (f(\tau\theta^{-1}) - f(\tau))\psi_\theta.$$

Assim, $(f(\tau\theta^{-1}) - f(\tau))_{\tau,\theta\neq 1}$ é a matriz de T restrito a W para a base $\{\psi_\tau;\ \tau \neq 1\}$.

Denotemos por $\hat{G}$ o grupo de caracteres de G. Seja $\chi \in \hat{G}$, $\chi\colon G \longrightarrow \mathbb{C}^*$. Como

$$\sum_{g\in G} \chi(g) = \begin{cases} |G|, \text{ se } \chi = 1 \\ 0, \text{ caso contrário} \end{cases},$$

então $\chi \in W$, $\chi \neq 1$.

Afirmo que $(\chi_i \in \hat{G};\ \chi_i \neq 1)$ forma uma base de W. De fato, como $\#(\chi_i \in \hat{G};\ \chi_i \neq 1) = |G|-1$, resta mostrarmos que os χ_i são linearmente independentes. Suponhamos, então, que os χ_i são linearmente dependentes e consideremos $\sum_i u_i\chi_i = 0$ $(u_i \in \mathbb{C})$ tal que o número q de u_i's que são não-nulos é mínimo. Depois de reordenarmos, suponhamos que

$$u_1\chi_1(g)+\cdots+u_q\chi_q(g) = 0 \quad \forall\ g \in G. \tag{33}$$

Temos $q \geq 2$, uma vez que os χ_i são não-nulos. Para h e g arbitrários,

$$u_1\chi_1(hg)+\cdots+u_q\chi_q(hg) = u_1\chi_1(h)\chi_1(g)+\cdots+u_q\chi_q(h)\chi_q(g) = 0.$$

Multiplicando (33) por $\chi_1(h)$ e subtraindo, temos

$$u_2(\chi_1(h)-\chi_2(h))\chi_2(g)+\cdots+u_q(\chi_1(h)-\chi_q(h))\chi_q(g) = 0.$$

Como isso ocorre $\forall\ g \in G$ e como q foi escolhido o menor possível, segue que $u_2(\chi_1(h)-\chi_2(h)) = 0$. Então $\chi_1(h) = \chi_2(h)$, uma contradição.

Portanto, $(\chi_i \in \hat{G};\ \chi_i \neq 1)$ forma uma base de W.

Temos

$$T\chi(g) = \sum_\sigma f(\sigma)\sigma\chi(g) = \sum_\sigma f(\sigma)\chi(g\sigma) = \sum_\sigma f(\sigma)\chi(\sigma)\chi(g)$$

$$= \left(\sum_\sigma f(\sigma)\chi(\sigma)\right)\chi(g).$$

Logo, χ é um auto-vetor com auto-valor $\sum_\sigma f(\sigma)\chi(\sigma)$. Então, T restrito a W é diagonal com respeito à essa base e o determinante é o produto desses auto-valores.

Portanto, $\det(f(\tau\theta^{-1}) - f(\tau))_{\tau,\theta\neq 1} = \prod_{\chi\neq 1}\sum_\sigma f(\sigma)\chi(\sigma)$. ∎

DEFINIÇÃO II.3.1. Sejam m e n inteiros positivos. A soma de Ramanujan é definida por

$$C_m(n) = \sum_{\substack{\alpha \bmod m \\ (\alpha,m)=1}} e^{2\pi i n\alpha/m}.$$

É imediato que se $(a,b) = 1$, então $C_{ab}(n) = C_a(n)C_b(n)$.

TEOREMA II.3.1. Se p é primo e a e n são inteiros positivos, então

$$C_{p^a}(n) = \begin{cases} 0 & \text{se } (p^a,n) < p^{a-1} \\ -p^{a-1} & \text{se } (p^a,n) = p^{a-1} \\ \varphi(p^a) & \text{se } (p^a,n) = p^a \end{cases}$$

DEMONSTRAÇÃO:

Se $(p^a,n) = p^a$, então $p^a \mid n$ e, logo,

$$C_{p^a}(n) = \sum_{\substack{\alpha=1 \\ (\alpha,p)=1}}^{p^a} 1 = \varphi(p^a).$$

Suponhamos, então, que $p^a \nmid n$. Se ζ é uma raiz primitiva p^a-ésima da unidade, podemos escrever

$$C_{p^a}(n) = \sum_{\substack{\alpha=1 \\ (\alpha,p)=1}}^{p^a} e^{2\pi i n\alpha/p^a} = \sum_{\substack{\alpha=1 \\ (\alpha,p)=1}}^{p^a} (\zeta^n)^\alpha$$

$$= \sum_{\alpha=1}^{p^a} (\zeta^n)^\alpha - \sum_{\beta=1}^{p^{a-1}} (\zeta^n)^{p\beta},$$

pois os múltiplos de p contidos em $\sum_{\alpha=1}^{p^a} (\zeta^n)^\alpha$ são $p, 2p, \ldots, p^a = p(p^{a-1})$. Como $p^a \nmid n$, então

$$\sum_{\alpha=1}^{p^a} (\zeta^n)^\alpha = \frac{(\zeta^n)^{p^a} - 1}{\zeta^n - 1} = 0.$$

Logo,

$$C_{p^a}(n) = -\sum_{\beta=1}^{p^{a-1}} (\zeta^n)^{p\beta} = -\sum_{\beta=1}^{p^{a-1}} (\zeta^{pn})^{\beta}.$$

Se $p^a | pn$, isto é, se $(p^a, n) = p^{a-1}$, então $\zeta^{pn} = 1$ e, portanto, $C_{p^a}(n) = -\sum_{\beta=1}^{p^{a-1}} 1 = -p^{a-1}$.

Se $p^a \nmid pn$, isto é, se $(p^a, n) < p^{a-1}$, então

$$C_{p^a}(n) = \frac{(\zeta^{pn})^{p^{a-1}} - 1}{\zeta^{pn} - 1} = 0$$

e o teorema está provado. ∎

III.1. UNIDADES CICLOTÔMICAS

Neste parágrafo, definimos um grupo de unidades chamado unidades ciclotômicas. O resultado fundamental é dado pelo Teorema III.11, onde é demonstrado que o grupo das unidades ciclotômicas é de índice finito no grupo das unidades. Antes, porém, são efetuadas uma série de cálculos para chegarmos ao regulador das unidades de Ramachandra.

DEFINIÇÃO III.1. Sejam f um número natural com $\varphi(f) > 2$ e

$$f = \prod_{j=1}^{k} p_j^{a_j} \qquad (k \geq 1,\ a_j > 0;\ j = 1,\ldots,k) \tag{1}$$

sua fatoração em primos.

Sejam $\chi: \mathcal{R}_f \longrightarrow \mathbb{C}^*$ um caráter não principal e $\chi_0: \mathcal{R}_{f_\chi} \longrightarrow \mathbb{C}^*$ o caráter primitivo módulo o seu condutor f_χ.

Escrevamos $f_\chi = \prod_{j=1}^{l} p_j^{r_j}$ $(1 \leq j \leq k,\ 0 < r_j \leq a_j;\ j = 1,\ldots,l)$ (2)

Seja g um divisor de f. Após uma reordenação, podemos escrever

$$g = g_1 g_2 g_3$$

onde

$$g_1 = \prod_{j=1}^{l} p_j^{t_j}\ ,\quad g_2 = \prod_{\substack{j=l+1 \\ t_j = a_j}}^{l+u} p_j^{t_j} \quad e \quad g_3 = \prod_{\substack{j=l+u+1 \\ t_j < a_j}}^{k} p_j^{t_j} \tag{3}$$

$$(\ 0 \leq t_j \leq a_j;\ j = 1,\ldots,l\ )$$

Sejam $$h = \prod_{j=1}^{l} p_j^{a_j}\ , \tag{4}$$

$$h_1 = \prod_{j=l+u+1}^{k} p_j^{a_j} = \frac{f}{hg_2} \quad e \tag{5}$$

$$T_{f,g}(\chi,n) = \sum_{r \bmod f} \overline{\chi}(r)\ e^{2\pi i n g r/f} \qquad (\ n=1,2,\dots\ )$$

Notemos que $f_\chi \mid h$.

As quantidades aqui estabelecidas (k, l, u, a_j, t_j, r_j) serão mantidas até o final desse capitulo.

LEMA III.1. Se $C_{f/h}(ng)$ é a soma de Ramanujan definida no §3 do Capitulo II, então $T_{f,g}(\chi,n)$ é dado por

$$T_{f,g}(\chi,n) = \overline{\chi}\left(\frac{f}{h}\right) C_{f/h}(ng) \left\{ \sum_{\beta_i \bmod f_\chi} \overline{\chi}(\beta_i)\, e^{2\pi i n g \beta_i/h} \right\} \left\{ \sum_{t=0}^{\left(\frac{h}{f}\right)-1} {}^{\chi}\, e^{2\pi i n g t f_\chi/h} \right\}$$

DEMONSTRAÇÃO:

Se α e β percorrem um sistema completo de resíduos módulo $\frac{f}{h}$ e h, respectivamente, então $r = \alpha h + \beta\frac{f}{h}$ percorre um sistema completo de resíduos módulo f.

Temos, então

$$\begin{aligned}
T_{f,g}(\chi,n) &= \sum_{r \bmod f} \overline{\chi}(r)\ e^{2\pi i n g r/f} \qquad (\ n=1,2,\dots\ ) \\
&= \sum_{\substack{\alpha \bmod f/h \\ \beta \bmod h}} \overline{\chi}\left(\alpha h + \beta\frac{f}{h}\right)\ e^{2\pi i n g(\alpha h + \beta\frac{f}{h})/f} \\
&= \sum_{\substack{\alpha \bmod f/h \\ \beta \bmod h}} \overline{\chi}\left(\beta\frac{f}{h}\right)\ e^{2\pi i n g \alpha h/f}\ e^{2\pi i n g \beta/h} \\
&= \overline{\chi}\left(\frac{f}{h}\right) \sum_{\beta \bmod h} \left[\ \overline{\chi}(\beta)\ e^{2\pi i n g \beta/h}\ \right] \sum_{\alpha \bmod f/h} e^{2\pi i n g \alpha h/f} \\
&= \overline{\chi}\left(\frac{f}{h}\right) \left\{ \sum_{\alpha \bmod f/h} e^{2\pi i n g \alpha h/f} \right\} \sum_{\beta \bmod h} \overline{\chi}(\beta)\ e^{2\pi i n g \beta/h}
\end{aligned}$$

Como $\overline{\chi}(\beta_i + t f_\chi) = \overline{\chi}(\beta_i)$ $(\ t=1,\dots,\frac{h}{f_\chi}-1\ )$, temos

$$T_{f,g}(\chi,n) = \overline{\chi}(-\frac{f}{h})\left\{\sum_{\alpha \bmod f/h} e^{2\pi i n g \alpha h/f}\right\}\left\{\sum_{\beta_i \bmod f_\chi}\overline{\chi}(\beta_i)\sum_{t=0}^{\chi(\frac{h}{f})-1} e^{2\pi i n g(\beta_i+tf_\chi)/h}\right\}$$

$$= \overline{\chi}(\frac{f}{h})C_{f/h}(ng)\left\{\sum_{\beta_i \bmod f_\chi}\overline{\chi}(\beta_i)\sum_{t=0}^{\chi(\frac{h}{f})-1} e^{2\pi i n g\beta_i/h}\, e^{2\pi i n g t f_\chi/h}\right\}$$

$$= \overline{\chi}(\frac{f}{h})C_{f/h}(ng)\left\{\sum_{\beta_i \bmod f_\chi}\overline{\chi}(\beta_i)e^{2\pi i n g\beta_i/h}\right\}\left\{\sum_{t=0}^{\chi(\frac{h}{f})-1} e^{2\pi i n g t f_\chi/h}\right\}$$

■

LEMA III.2. Se τ é uma soma de Gauss, então

$$T_{f,g}(\chi,n) = \begin{cases} 0 & \text{se } (h,ng) \neq h/f_\chi \\ \dfrac{h}{f_\chi}\,\tau(\overline{\chi})\chi(\dfrac{ngf_\chi}{f})C_{f/h}(ng) & \text{se } (h,ng) = \dfrac{h}{f_\chi} \end{cases}$$

DEMONSTRAÇÃO:

Consideremos o fator $\displaystyle\sum_{t=0}^{\chi(\frac{h}{f})-1} e^{2\pi i n g t f_\chi/h} = \sum_{t=0}^{\chi(\frac{h}{f})-1}\left(\zeta_{h/f_\chi}^{ng}\right)^t$.

Se $\dfrac{h}{f_\chi}\mid ng$, então $\zeta_{h/f_\chi}^{ng} = 1$ e, portanto, $\displaystyle\sum_{t=0}^{\chi(\frac{h}{f})-1} e^{2\pi i n g t f_\chi/h} = \frac{h}{f_\chi}$.

Se $\dfrac{h}{f_\chi}\nmid ng$, então $\displaystyle\sum_{t=0}^{\chi(\frac{h}{f})-1} e^{2\pi i n g t f_\chi/h} = 1+\left(\zeta_{h/f_\chi}^{ng}\right)+\cdots+\left(\zeta_{h/f_\chi}^{ng}\right)^{\left[\chi(\frac{h}{f})-1\right]}$

$$= \frac{\left(\zeta_{h/f_\chi}^{ng}\right)^{\frac{h}{f_\chi}} - 1}{\zeta_{h/f_\chi}^{ng} - 1} = 0.$$

Agora, sabemos, pelo Lema II.2.12 que

$$\sum_{\beta_i \bmod f_\chi} \overline{\chi}(\beta_i) e^{2\pi i n g \beta_i / h} = \sum_{\beta_i \bmod f_\chi} \overline{\chi}(\beta_i) e^{2\pi i \beta_i \frac{ngf_\chi}{h}/f_\chi} \chi\left(\frac{ngf_\chi}{h}\right) \tau(\overline{\chi})$$

e que o resultado se anula quando $\left(\frac{ngf_\chi}{h}, f_\chi\right) \neq 1$

Logo,

$$T_{f,g}(\chi, n) = \begin{cases} 0 & \text{se } \frac{h}{f_\chi} \nmid ng \text{ ou } \frac{h}{f_\chi} \mid ng \text{ e } (ngf_\chi/h, f_\chi) \neq 1 \\ \overline{\chi}\left(\frac{f}{h}\right) \chi\left(\frac{\chi_{ngf}}{h}\right) \tau(\overline{\chi}) C_{f/h}(ng) \frac{h}{f_\chi} & \text{caso contrário} \end{cases}$$

Se $(h, ng) = \frac{h}{f_\chi}$, então $\frac{h}{f_\chi} \mid ng$. Afirmo que $\left(\frac{ngf_\chi}{h}, f_\chi\right) = 1$.

De fato, se $\left(\frac{ngf_\chi}{h}, f_\chi\right) = d > 1$, então

$$\frac{ngf_\chi}{h} = k_1 d \quad \text{e} \quad f_\chi = k_2 d, \quad k_1 \text{ e } k_2 \text{ naturais, } k_2 < f_\chi.$$

Logo, $ng = \frac{k_1}{k_2} h$, uma contradição, pois $\frac{h}{f_\chi} \mid ng$.

Seja, então $(h, ng) \neq \frac{h}{f_\chi}$. Se $\frac{h}{f_\chi} \nmid ng$, então $T_{f,g}(\chi, n) = 0$. Se $\frac{h}{f_\chi} \mid ng$, então existe primo p tal que $p \frac{h}{f_\chi} \mid (h, ng)$. Logo, $\left(\frac{ngf_\chi}{h}, f_\chi\right) \geq p \neq 1$ e, então $T_{f,g}(\chi, n) = 0$.

Uma vez que

$$\overline{\chi}\left(\frac{f}{h}\right) \chi\left(\frac{ngf_\chi}{h}\right) = \chi\left(\frac{h}{f} \frac{ngf_\chi}{h}\right) = \chi\left(\frac{ngf_\chi}{f}\right),$$

o resultado se segue. ∎

DEFINIÇÃO III.2. Definimos a aplicação $\varphi_{f,g}$ por

$$\begin{aligned} \varphi_{f,g}: \mathcal{R}_f &\longrightarrow \mathbb{R} \\ R &\longmapsto \log|1 - e^{2\pi i g r / f}| \end{aligned}$$

onde r é um representante da classe R de $\mathcal{R}_f$.

Afirmo que $\varphi_{f,g}$ está bem definida. De fato:

Se r e r' são dois representantes de R e r-r'=tf, então

$$\log|1-e^{2\pi igr/f}| = \log|1-e^{2\pi igr'+tf)/f}|$$

$$= \log|1-e^{2\pi igr'/f}\, e^{2\pi igt}|$$

$$= \log|1-e^{2\pi igr'/f}|$$

Analogamente se r+r'=tf.

Vamos agora definir $V_{f,g}$ que terá papel importante no cálculo do regulador das unidades de Ramachandra.

DEFINIÇÃO III.3. Fixado o caráter χ, definimos $V_{f,g}$ por

$$V_{f,g} = \sum_{R\in\mathcal{R}_f} \overline{\chi}(R)\ \varphi_{f,g}(R).$$

O lema seguinte relaciona $V_{f,g}$ definido acima com $T_{f,g}(\chi,n)$.

LEMA III.3. $\quad V_{f,g} = -\frac{1}{2}\sum_{n=1}^{\infty}\frac{1}{n}\ T_{f,g}(\chi,n).$

DEMONSTRAÇÃO:

Temos

$$V_{f,g} = \sum_{R\in\mathcal{R}_f} \overline{\chi}(R)\ \log|1-e^{2\pi igr/f}|$$

$$= \frac{1}{2}\sum_{R\in\mathcal{R}_f} \overline{\chi}(R)\ \log|1-e^{2\pi igr/f}|^2$$

$$= \frac{1}{2}\sum_{\substack{r=1\\(r,f)=1}}^{f-1} \overline{\chi}(r)\ \log|1-e^{2\pi igr/f}|^2$$

$$= \frac{1}{2}\sum_{\substack{r=1\\(r,f)=1}}^{f-1} \overline{\chi}(r)\ \left\{\log(1-e^{2\pi igr/f}) + \log(1-e^{-2\pi igr/f})\right\}$$

$$= \frac{1}{2}\sum_{\substack{r=1\\(r,f)=1}}^{f-1} \overline{\chi}(r)\log(1-e^{2\pi igr/f}) + \frac{1}{2}\sum_{\substack{r=1\\(r,f)=1}}^{f-1} \overline{\chi}(r)\log(1-e^{-2\pi igr/f})$$

$$= \frac{1}{2}\sum_{\substack{1\le r<f/2\\(r,f)=1}} \overline{\chi}(r)\log(1-e^{2\pi igr/f}) + \frac{1}{2}\sum_{\substack{f/2<r<f\\(r,f)=1}} \overline{\chi}(r)\log(1-e^{2\pi igr/f})$$

$$= \frac{1}{2}\sum_{r\in \frac{\mathbb{Z}}{f\mathbb{Z}}} \overline{\chi}(r)\ \log(1-e^{2\pi igr/f}).$$

Como $\log(1-X) = -\sum_{n=1}^{\infty}\frac{X^n}{n}$, então, pondo $X = e^{2\pi igr/f}$, temos

$$V_{f,g} = -\frac{1}{2}\sum_{r \bmod f} \overline{\chi}(r)\ \left\{\sum_{n=1}^{\infty}\frac{e^{2\pi ingr/f}}{n}\right\}$$

$$= -\frac{1}{2}\sum_{n=1}^{\infty}\frac{1}{n}\left\{\sum_{r \bmod f} \overline{\chi}(r)\ e^{2\pi ingr/f}\right\}$$

$$= -\frac{1}{2}\sum_{n=1}^{\infty}\frac{1}{n}\ T_{f,g}(\chi,n).$$

As séries são convergentes pelo teste de Dirichlet ([1] Apostol, Theorem 12.28, p.365). ∎

Vamos, agora, usar o Lema III.2 para caracterizar melhor $V_{f,g}$.

LEMA III.4.

$$V_{f,g} = \begin{cases} 0\ , \text{ se } g\nmid (f/f_\chi) \\ -\frac{1}{2}\ \frac{h}{f_\chi}\ \tau(\widetilde{\chi})\ \sum_{n=1}^{\infty}\frac{1}{n}\left\{\ \chi(\frac{ngf_\chi}{f})\ C_{f/h}(ng)\ \right\}, \text{ se } g\mid \frac{f}{f_\chi} \end{cases}$$

onde $\sum_{n=1}^{\infty}$ denota a soma sobre os inteiros n dados por

$$n = \frac{h}{g_1 f_\chi}\ m_1 \text{ com } (m_1,h) = 1.$$

DEMONSTRAÇÃO:

Usando as equações (1), (2), (3) e (4), podemos escrever que

$$\frac{h}{f_\chi} = \prod_{j=1}^{l} p_j^{a_j-r_j} \quad \text{e} \quad \frac{f}{f_\chi} = \prod_{j=1}^{l} p_j^{a_j-r_j}\prod_{j=l+1}^{k} p_j^{a_j}\ .$$

Afirmo que se $g\nmid \frac{f}{f_\chi}$, então $(h,ng) \neq \frac{h}{f_\chi}$. De fato, se $\frac{h}{f_\chi}\mid ng$,

então $(h,ng) \neq \frac{h}{f_\chi}$. Se $\frac{h}{f_\chi} \mid ng$, então $\prod_{j=1}^{l} p_j^{a_j-r_j} \mid ng$. Mas, como $g \nmid \frac{f}{f_\chi}$, existe i, $1 \leq i \leq l$, tal que $t_i \geq a_i - r_i + 1$. Logo, $p_i^{a_i-r_i+1} \mid ng$ e, portanto, $(h,ng) \geq \frac{h}{f_\chi} p_i \neq \frac{h}{f_\chi}$. Então, $V_{f,g} = 0$ se $g \nmid \frac{f}{f_\chi}$.

Estudemos, agora o caso $g \mid \frac{f}{f_\chi}$ e $(h,ng) = \frac{h}{f_\chi}$. Temos

$$V_{f,g} = -\frac{1}{2} \sum_{n=1}^{\infty} \frac{1}{n} T_{f,g}(\chi,n)$$

$$= -\frac{1}{2} \frac{h}{f_\chi} \tau(\bar{\chi}) \sum_{n=1}^{\infty} \frac{1}{n} \left\{ \chi\left(\frac{ngf}{f}\right) C_{f/h}(ng) \right\}.$$

Como $(h,ng) = \frac{h}{f_\chi}$, então $\frac{h}{f_\chi} t = ng$ com $(t,h)=1$, t inteiro. Ou seja, $n = \frac{ht}{f_\chi g}$.

Logo, $n = \prod_{j=1}^{l} p_j^{a_j-t_j-r_j} m_1 = \frac{h}{g_1 f_\chi} m_1$, com $(m_1,h) = 1$ e está provado o lema. ■

Antes de prosseguirmos com o cálculo de $V_{f,g}$, vamos restringir ainda mais os inteiros n considerados na soma $\sum_{n=1}^{\infty}$ do lema anterior.

Já vimos no §3 do Capítulo II que

$$C_{f/h}(ng) = \prod_{j=l+1}^{k} C_{p_j^{a_j}}(ng) \text{ e que}$$

$$C_{p_j^{a_j}}(ng) = \begin{cases} 0 & \text{se } (p_j^{a_j}, ng) < p_j^{a_j-1} \\ -p_j^{a_j-1} & \text{se } (p_j^{a_j}, ng) = p_j^{a_j-1} \\ \varphi(p_j^{a_j}) & \text{se } (p_j^{a_j}, ng) = p_j^{a_j} \end{cases}$$

Logo, vamos nos restringir aos n tais que $p_j^{a_j-1} \mid ng$ ($j = l+1,\ldots,k$). Mas, isto é equivalente a dizer que

$$(ng, \frac{f}{h}) = \prod_{j=l+1}^{k} p_j^{a_j - e_j} \quad (e_j = 0 \text{ ou } 1).$$

Logo, podemos restringir a soma aos n tais que

$$n = \frac{h}{g_1 f_\chi} m_1 \ , \ (m_1, h) = 1 \text{ e } (ng, \frac{f}{h}) = \prod_{j=l+1}^{k} p_j^{a_j - e_j}.$$

Mas, se $(ng, \frac{f}{h}) = \prod_{j=l+1}^{k} p_j^{a_j - e_j}$, então $p_j^{a_j - e_j} | ng$, ou seja, $p_j^{a_j - e_j} | \frac{h}{g_1 f_\chi} m_1 g_1 g_2 g_3$, $j = l+1, \ldots, k$. Uma vez que $p_j \nmid \frac{h}{f_\chi}$, então $p_j^{a_j - e_j} | m_1 g_2 g_3$. Se $p_j | g_2$, então $e_j = 0$ e nada se pode concluir. Se $p_j \nmid g_2$, então $p_j^{a_j - e_j} | m_1 g_3$ e, logo, $p_j^{a_j - e_j - t_j} | m_1$. Assim, $m_1 = \prod_{j=l+u+1}^{k} p_j^{a_j - e_j - t_j} m$.

Afirmo que $(m, f_\chi \prod_{j=l+u+1}^{k} p_j^{e_j}) = 1$. De fato, uma vez que $(m, f_\chi) = 1$, resta, então, mostrarmos que $(m, \prod_{j=l+u+1}^{k} p_j^{e_j}) = 1$.

Se $(m, p_i^{e_i}) \neq 1$ para algum i, $l+u+1 \leq i \leq k$, então, uma vez que $(ng, \frac{f}{h}) = \prod_{j=l+1}^{k} p_j^{a_j - e_j}$, $e_i = 0$, uma contradição.

Provamos, então, o seguinte lema:

LEMA III.5.

$$V_{f,g} = \begin{cases} 0 \ , \text{ se } g \nmid (f / f_\chi) \\ -\frac{1}{2} \frac{h}{f_\chi} \tau(\overline{\chi}) \sum_{n=1}^{\infty} \frac{1}{n} \left\{ \chi(\frac{ngf}{f}) \ C_{f/h}(ng) \right\} \ , \text{ se } g | (\frac{f}{f_\chi}) \end{cases}$$

onde $\sum_{n=1}^{\infty}$ denota a soma sobre os inteiros n dados por

$$n = \left(\prod_{p_j | h_1} p_j^{a_j - t_j - e_j} \right) \frac{mh}{g_1 f_\chi} \text{ com } (m, f_\chi \prod_{p_j | h_1} p_j^{e_j}) = 1 \qquad (6)$$

■

Cada k-l-u-upla $(e_{l+u+1},\ldots,e_k)$ $(e_i=0$ ou $1,\ \ i=l+u+1,..,k)$ determina um conjunto de inteiros n dados por (6). Os conjuntos dos inteiros n determinados por duas k-l-u-uplas distintas são disjuntos. Logo, a soma $\sum_{n=1}^{\infty}{}'$ pode ser partida em 2^{k-l-u} parcelas, cada parcela definida por uma escolha dos números e_j, $j\geq l+u+1$.

Agora vamos expressar $V_{f,g}$ em termos de L-séries.

LEMA III.6.

$$V_{f,g}=\begin{cases} 0\ , & \text{se } g\nmid(f/f_\chi) \\ -\frac{1}{2}\,\tau(\bar\chi)L(1,\chi)\ g\prod_{\substack{p\mid f\\ p\nmid f/g}}(1-p^{-1})\prod_{p\mid f/g}(1-\bar\chi(p)), & \text{se } g\mid(\frac{f}{f_\chi}) \end{cases}$$

DEMONSTRAÇÃO:

Temos

$$C_{f/h}(ng)=\prod_{j=l+1}^{k}C_{p_j^{a_j}}(ng)=\prod_{j=l+1}^{l+u}C_{p_j^{a_j}}(ng)\cdot\prod_{j=l+u+1}^{k}C_{p_j^{a_j}}(ng)\quad e$$

$$ng=\left(\prod_{p_j\mid h_1}p_j^{a_j-t_j-e_j}\right)\frac{mh}{g_1f_\chi}\,g_1g_2g_3=\left(\prod_{p_j\mid h_1}p_j^{a_j-t_j-e_j}\right)\frac{mhg_2g_3}{f_\chi}\ .$$

Se $j=l+1,\ldots,l+u$, então $p_j\nmid h_1$ e, logo, $(p_j^{a_j},ng)=p_j^{a_j}$.

Então, $\prod_{j=l+1}^{l+u}C_{p_j^{a_j}}(ng)=\prod_{j=l+1}^{l+u}\varphi(p_j^{a_j})$.

Se $j=l+u+1,\ldots,k$, então $p_j\mid h_1$ e, logo, $(p_j^{a_j},ng)=p_j^{a_j-e_j}$.

Então,
$$\prod_{j=l+u+1}^{k}C_{p_j^{a_j}}(ng)=\prod_{\substack{j=l+u+1\\ e_j=0}}^{k}\varphi(p_j^{a_j})\cdot\prod_{\substack{j=l+u+1\\ e_j=1}}^{k}(-p_j^{a_j-1})$$

$$=\prod_{j=l+u+1}^{k}\left[\varphi(p_j^{a_j})\right]^{1-e_j}\cdot(-p_j^{a_j-1})^{e_j}$$

$$=\prod_{j=l+u+1}^{k}\varphi(p_j^{a_j})\cdot\prod_{j=l+u+1}^{k}\left[\frac{-p_j^{a_j-1}}{\varphi(p_j^{a_j})}\right]^{e_j}$$

$$= \prod_{j=l+u+1}^{k} \varphi(p_j^{a_j}) \cdot \prod_{j=l+u+1}^{k} \left[\frac{-p_j^{a_j-1}}{p_j^{a_j-1}(p_j-1)} \right]^{e_j}$$

$$= \prod_{j=l+u+1}^{k} \varphi(p_j^{a_j}) \cdot \prod_{j=l+u+1}^{k} (1-p_j)^{-e_j} .$$

Portanto,

$$C_{f/h}(ng) = \prod_{j=l+1}^{l+u} \varphi(p_j^{a_j}) \cdot \prod_{j=l+u+1}^{k} \varphi(p_j^{a_j}) \cdot \prod_{j=l+u+1}^{k} (1-p_j)^{-e_j}$$

$$= \prod_{j=l+1}^{k} \varphi(p_j^{a_j}) \cdot \prod_{j=l+u+1}^{k} (1-p_j)^{-e_j}$$

$$= \varphi\left(\frac{f}{h}\right) \prod_{j=l+u+1}^{k} (1-p_j)^{-e_j} .$$

Temos

$$n = \left(\prod_{p_j | h_1} p_j^{a_j - t_j - e_j} \right) \frac{mh}{g_1 f \chi} = \left(\prod_{p_j | h_1} p_j^{a_j - t_j} \prod_{p_j | h_1} p_j^{-e_j} \right) \frac{mh}{g_1 f \chi}$$

$$= \frac{h_1}{g_3} \frac{mh}{g_1 f \chi} \prod_{p_j | h_1} p_j^{-e_j} .$$

Logo,

$$\chi\left(\frac{ngf}{f}\chi\right) = \chi(m)\ \chi\left(\frac{h_1 hgf}{g_3 g_1 f \chi^f}\chi\right) \prod_{p_j | h_1} \chi(p_j^{-e_j})$$

$$= \chi(m) \prod_{p_j | h_1} \chi(p_j^{-e_j}) \text{ , pois } h_1 hg = g_3 g_1 f.$$

Assim, se $g | f/f_\chi$,

$$V_{f,g} = -\frac{1}{2} \frac{h}{f_\chi} \tau(\bar{\chi}) \sum_{n=1}^{\infty} \frac{1}{n} \left\{ \chi\left(\frac{ngf}{f}\chi\right) C_{f/h}(ng) \right\}$$

$$= -\frac{1}{2} \frac{h}{f_\chi} \tau(\bar{\chi})\ \varphi\left(\frac{f}{h}\right) \frac{g_3 g_1 f \chi}{h_1 h} \times$$

$$\times \sum_{n=1}^{\infty} \frac{\chi(m)}{m} \prod_{p_j | h_1} \chi(p_j^{-e_j})(1-p_j)^{-e_j} p_j^{e_j}$$

$$= -\frac{1}{2}\,\tau(\bar{\chi})\;\varphi(\frac{f}{h})\;\frac{g_2 g_1}{h_1}\sum_{e_j}\Big[\prod_{p_j\mid h_1}\Big\{-\bar{\chi}(p_j)p_j(p_j-1)^{-1}\Big\}^{e_j}\sum_{(m,\,f_{g,e})=1}\frac{\chi(m)}{m}\Big]$$

onde $f_{g,e} = f_\chi \prod_{p_j\mid h_1} p_j^{e_j}$.

Mas,

$$\sum_{(m,\,f_{g,e})=1}\frac{\chi(m)}{m} = \prod_{\substack{p\nmid f_\chi \\ p\neq p_j \text{ se } e_j=1}}(1-\chi(p)p^{-1})^{-1}$$

$$= \prod_{p}(1-\chi(p)p^{-1})^{-1}\prod_{\substack{p\mid f_\chi \\ p\neq p_j \text{ se } e_j=1}}(1-\chi(p)p^{-1})$$

$$= L(1,\chi)\;\Big[(1-\chi(p_1)p_1^{-1})\cdots(1-\chi(p_l)p_l^{-1})\;\times$$

$$\times\prod_{p_j\mid h_1}(1-\chi(p_j)p_j^{-1})^{e_j}\Big]$$

$$= L(1,\chi)\prod_{p_j\mid h_1}(1-\chi(p_j)p_j^{-1})^{e_j}.$$

Logo,

$$V_{f,g} = -\frac{1}{2}\,\tau(\bar{\chi})\;\varphi(\frac{f}{h})\;\frac{g_2 g_1}{h_1}\,L(1,\chi)\;\times$$

$$\times\sum_{e_j}\Big[\prod_{p_j\mid h_1}\Big\{-\bar{\chi}(p_j)(1-\chi(p_j)p_j^{-1})\Big\}^{e_j}(p_j(p_j-1)^{-1})^{e_j}\Big].$$

Como

$$\prod_{p_j\mid h_1}(p_j(p_j-1)^{-1})^{e_j} = \prod_{p_j\mid h_1}\Big(\frac{p_j}{p_j-1}\Big)^{e_j} = \prod_{p_j\mid h_1}\Big(\frac{1}{1-\frac{1}{p_j}}\Big)^{e_j}$$

$$= \prod_{p_j\mid h_1}(1-p_j^{-1})^{-e_j}$$

$$= \prod_{p_j\mid h_1}(1-p_j^{-1})^{-1}\prod_{p_j\mid h_1}(1-p_j^{-1})^{1-e_j}$$

$$= \prod_{p_j | h_1} \frac{p_j}{p_j - 1} \prod_{p_j | h_1} (1-p_j^{-1})^{1-e_j}$$

$$V_{f,g} = -\frac{1}{2}\, \tau(\bar{\chi})\, \varphi\left(\frac{f}{h}\right) \frac{g_3 g_1}{h_1}\, L(1,\chi) \prod_{p_j | h_1} \frac{p_j}{p_j - 1} \times$$

$$\times \sum_{e_j} \left[\prod_{p_j | h_1} \left\{ -\bar{\chi}(p_j)(1-\chi(p_j)p_j^{-1}) \right\}^{e_j} (1-p_j^{-1})^{1-e_j} \right].$$

Mas,

$$\varphi\left(\frac{f}{h}\right) \frac{1}{h_1} \prod_{p_j | h_1} \frac{p_j}{p_j - 1} = \varphi\left(\prod_{j=l+1}^{k} p_j^{a_j} \right) \frac{1}{\prod_{j=l+u+1}^{k} p_j^{a_j}} \frac{1}{\prod_{j=l+u+1}^{k} p_j^{-1}(p_j-1)}$$

$$= \frac{\prod_{j=l+1}^{k} p_j^{a_j - 1}(p_j-1)}{\prod_{j=l+u+1}^{k} p_j^{a_j - 1}(p_j-1)} = \prod_{j=l+1}^{l+u} p_j^{a_j - 1}(p_j-1)$$

$$= \prod_{j=l+1}^{l+u} \varphi(p_j^{a_j}) = \varphi\left(\prod_{j=l+1}^{l+u} p_j^{a_j} \right) = \varphi(g_2).$$

Logo,

$$V_{f,g} = -\frac{1}{2}\, \tau(\bar{\chi})\, L(1,\chi)\, g_3 g_1\, \varphi(g_2) \times$$

$$\times \sum_{e_j} \left[\prod_{p_j | h_1} \left\{ -\bar{\chi}(p_j)(1-\chi(p_j)p_j^{-1}) \right\}^{e_j} (1-p_j^{-1})^{1-e_j} \right].$$

Temos que

$$g_3 g_1 \varphi(g_2) = \frac{g}{g_2} \varphi(g_2) = g\, \frac{\prod_{j=l+1}^{l+u} p_j^{a_j - 1}(p_j-1)}{\prod_{j=l+1}^{l+u} p_j^{a_j}} = g \prod_{j=l+1}^{l+u} \frac{p_j - 1}{p_j}$$

$$= g \prod_{j=l+1}^{l+u} \left(1 - \frac{1}{p_j} \right) = g \prod_{\substack{p | f \\ p \nmid f/g}} (1-p^{-1}).$$

Podemos facilmente provar, por indução, que

$$\sum_{e_j=0,1} \left[\prod_{j=1}^{n} a_j^{e_j} b_j^{1-e_j} \right] = \prod_{j=1}^{n} (a_j+b_j) . \qquad (6)$$

Então,

$$\sum_{e_j} \left[\prod_{p_j | h_1} \left\{ - \bar{\chi}(p_j)(1-\chi(p_j)p_j^{-1}) \right\}^{e_j} (1-p_j^{-1})^{1-e_j} \right] =$$

$$= \prod_{p_j | h_1} \left[- \bar{\chi}(p_j)(1-\chi(p_j)p_j^{-1}) + (1-p_j^{-1}) \right]$$

$$= \prod_{p_j | h_1} (- \bar{\chi}(p_j)+p_j^{-1}+1-p_j^{-1}) = \prod_{p_j | h_1} (1-\bar{\chi}(p_j))$$

$$= \prod_{p | \frac{f}{g}} (1-\bar{\chi}(p))$$

pois $\bar{\chi}(p_j) = 0$ se $j = 1,\ldots,l$, e o lema está provado. ∎

Introduzemos, agora, os dois subgrupos de unidades de índice finito e caminharemos na direção da prova do principal resultado deste trabalho (Teorema III.11).

DEFINIÇÃO III.4. Sejam ζ uma raiz primitiva f-ésima da unidade, $f \not\equiv 2 \pmod 4$ e E o grupo das unidades de $\mathbb{Q}(\zeta)$. Então

$$C = \left\{ \pm \zeta^j \prod_{i=1}^{f-1} (1-\zeta^i)^{r_i} \in E : j, r_i \in \mathbb{Z} \right\}$$

é chamado grupo das unidades ciclotômicas de $\mathbb{Q}(\zeta)$.

Faz-se a restrição $f \not\equiv 2 \pmod 4$ pois se $f \equiv 2 \pmod 4$, então $\mathbb{Q}(\zeta_f) = \mathbb{Q}(\zeta_{f/2})$. Note, também, que nem sempre $(1-\zeta^i) \in E$, mas comparecem no produto da definição acima só aqueles que pertencem ao grupo E.

DEFINIÇÃO III.5. Sejam $f \not\equiv 2 \pmod 4$ e $f = \prod_{j=1}^{k} p_j^{a_j}$ sua decomposição

em primos. Para $1 < s < \frac{f}{2}$, com $(s,f) = 1$, definamos

$$\xi_s = \zeta^{d_s} \prod_{e_j}{}' \frac{1-\zeta^{sf_J}}{1-\zeta^{f_J}}, \quad d_s = \frac{1}{2}(1-s)\sum_{e_j}{}' f_J$$

onde $f_J = \prod_{j=1}^{k} p_j^{a_j e_j}$, ζ é uma raiz primitiva f-ésima da unidade e o produto é estendido sobre todos os $e_j = 0$ ou 1, $j = 1,\ldots,k$, excelo $e_1 = e_2 = \cdots = e_k = 1$.

LEMA III.7. Os ξ_s acima definidos são unidades reais e $\xi_s \in C^+$, onde $C^+ = C \cap E^+$, sendo E^+ o grupo das unidades de $\mathbb{Q}(\zeta)^+$.

DEMONSTRAÇÃO:

Uma vez que $\frac{1-\zeta^{sf_J}}{1-\zeta^{f_J}} = \frac{1-\zeta_{f/f_J}^{s}}{1-\zeta_{f/f_J}}$ são unidades de $\mathbb{Q}(\zeta_{f/f_J})$ ([11] Washington, Lemma 1.3, p.2 e Proposition 2.8, p.12) e, portanto de $\mathbb{Q}(\zeta)$, os ξ_s são unidades de $\mathbb{Q}(\zeta)$.

São reais pois

$$\overline{\xi}_s = \zeta^{-d_s} \prod_{e_j}{}' \frac{1-\zeta^{-sf_J}}{1-\zeta^{-f_J}} = \zeta^{-d_s} \prod_{e_j}{}' \frac{-\zeta^{-sf_J}(1-\zeta^{sf_J})}{-\zeta^{-f_J}(1-\zeta^{f_J})}$$

$$= \zeta^{-d_s} \prod_{e_j}{}' \zeta^{(1-s)f_J} \prod_{e_j}{}' \frac{1-\zeta^{sf_J}}{1-\zeta^{f_J}}$$

$$= \zeta^{-d_s+(1-s)\sum_{e_j}{}' f_J} \prod_{e_j}{}' \frac{1-\zeta^{sf_J}}{1-\zeta^{f_J}} = \zeta^{d_s} \prod_{e_j}{}' \frac{1-\zeta^{sf_J}}{1-\zeta^{f_J}}$$

$$= \xi_s .$$

Claramente $\xi_s \in C^+$. ∎

As unidades ξ_s definidas acima são chamadas de unidades de Ramachandra.

LEMA III.8. $R(\xi_s) = \pm \prod_{\chi \neq 1} \frac{1}{2} \tau(\bar{\chi})\, L(1,\chi) \prod_{p_j \mid \frac{f}{h}} \left\{ \chi(p_j^2) - \bar{\chi}(p_j) \right\}$

onde χ percorre os caracteres pares não triviais módulo f.

DEMONSTRAÇÃO:

Sejam $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ e $G^+ = Gal(\mathbb{Q}(\zeta)^+/\mathbb{Q})$, onde ζ é uma raiz primitiva f-ésima da unidade e $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta+\zeta^{-1})$ é o maior subcorpo real de $\mathbb{Q}(\zeta)$.

$\mathbb{Q}(\zeta)$
|
$\mathbb{Q}(\zeta)^+$
|
$\mathbb{Q}$

Seja $\psi: G^+ \longrightarrow \mathbb{C}$

$\sigma_k \mapsto \log \left| \prod_{e_j}' (1-\zeta^{kf_j}) \right|$

Cabe observar que, como $G^+ \simeq \mathcal{R}_f$, k é fixado pelo isomorfismo $\sigma_k \mapsto \bar{k}$.

Temos que

$$\psi(\sigma_k\sigma_s) - \psi(\sigma_k) = \log|\sigma_k(\xi_s)|$$

pois

$$\psi(\sigma_k\sigma_s) - \psi(\sigma_k) = \log \left| \prod_{e_j}' (1-\zeta^{ksf_j}) \right| - \log \left| \prod_{e_j}' (1-\zeta^{kf_j}) \right|$$

$$= \log \left| \prod_{e_j}' \frac{1-\zeta^{ksf_j}}{1-\zeta^{kf_j}} \right| \quad e$$

$$\log|\sigma_k(\xi_s)| = \log \left| \sigma_k \left(\zeta^{d_s} \prod_{e_j}' \frac{1-\zeta^{sf_j}}{1-\zeta^{f_j}} \right) \right|$$

$$= \log \left| \zeta^{kd_s} \prod_{e_j}' \frac{1-\zeta^{ksf_j}}{1-\zeta^{kf_j}} \right|$$

$$= \log \left| \prod_{e_j}' \frac{1-\zeta^{ksf_j}}{1-\zeta^{kf_j}} \right| .$$

Então,

$$R(\xi_s) = \pm \det \left(\log|\sigma_k(\xi_s)| \right)_{\sigma_k \neq 1}$$

$$= \pm \det\left(\psi(\sigma_k\sigma_s) - \psi(\sigma_k)\right)_{\sigma_k,\sigma_s \neq 1}$$

$$= \pm \prod_{\chi \neq 1} \sum_{\sigma \in G^+} \chi(\sigma)\psi(\sigma) \quad \text{(cf. Teorema II.2.18)}$$

$$= \pm \prod_{\chi \neq 1} \sum_{R \in \mathcal{R}_f} \chi(R) \log\left|\prod_{e_j}{}' (1-\zeta^{rf_j})\right|$$

$$= \pm \prod_{\chi \neq 1} \sum_{R \in \mathcal{R}_f} \chi(R) \sum_{e_j}{}' \log|1-\zeta^{rf_j}|$$

$$= \pm \prod_{\chi \neq 1} \sum_{R \in \mathcal{R}_f} \chi(R) \sum_{e_j}{}' \log|1-e^{2\pi i r f_j/f}|$$

$$= \pm \prod_{\chi \neq 1} \sum_{e_j}{}' \sum_{R \in \mathcal{R}_f} \chi(R) \log|1-e^{2\pi i r f_j/f}|$$

$$= \pm \prod_{\chi \neq 1} \sum_{e_j}{}' V_{f,f_j}$$

Considerando $g=f_j$ tal que $g\left|\frac{f}{f_\chi}\right.$, temos, pelo Lema III.6 que

$$R((\xi_s)) = \pm \prod_{\chi \neq 1} \frac{1}{2} \tau(\bar{\chi}) L(1,\chi) \left\{ \sum_{e_j}{}' \prod_{j=l+1}^{k} p_j^{a_j e_j} \prod_{p \mid f} (1-p^{-1}) \times \right.$$

$$\left. \times \prod_{p \nmid f / \left\{\prod_{j=l+1}^{k} p_j^{a_j e_j}\right\}} (1-\bar{\chi}(p)) \right\}$$

$$= \pm \prod_{\chi \neq 1} \frac{1}{2} \tau(\bar{\chi}) L(1,\chi) \left\{ \sum_{e_j}{}' \left[\prod_{j=l+1}^{k} p_j^{a_j e_j} (1-p_j^{-1})^{e_j} \times \right. \right.$$

$$\times \left(1-\bar{\chi}(p_j)\right)^{1-e_j} \Bigg]\Bigg\}$$

$$= \pm\prod_{\chi\neq 1} \frac{1}{2}\,\tau(\bar{\chi})\; L(1,\chi)\Bigg\{ \sum_{e_j}{}' \Bigg[\prod_{j=l+1}^{k} \Big[p_j^{a_j}(1-p_j^{-1}) \Big]^{e_j} \times$$

$$\times \left(1-\bar{\chi}(p_j)\right)^{1-e_j} \Bigg]\Bigg\}$$

$$= \pm\prod_{\chi\neq 1} \frac{1}{2}\,\tau(\bar{\chi})\; L(1,\chi)\Bigg\{ \sum_{e_j}{}' \Bigg[\prod_{j=l+1}^{k} \Big[p_j^{a_j-1}(p_j-1) \Big]^{e_j} \times$$

$$\times \left(1-\bar{\chi}(p_j)\right)^{1-e_j} \Bigg]\Bigg\}$$

$$= \pm\prod_{\chi\neq 1} \frac{1}{2}\tau(\bar{\chi})L(1,\chi)\Bigg[\sum_{e_j}{}' \prod_{j=l+1}^{k} \left(\varphi(p_j^{a_j})\right)^{e_j} \left(1-\bar{\chi}(p_j)\right)^{1-e_j}\Bigg]$$

$$= \pm\prod_{\chi\neq 1} \frac{1}{2}\,\tau(\bar{\chi})\; L(1,\chi) \prod_{j=l+1}^{k} \Big\{ \varphi(p_j^{a_j})+1-\bar{\chi}(p_j) \Big\} \quad (\text{cf } (6))$$

$$= \pm\prod_{\chi\neq 1} \frac{1}{2}\,\tau(\bar{\chi})\; L(1,\chi) \prod_{p_j \mid \frac{f}{h}} \Big\{ \varphi(p_j^{a_j})+1-\bar{\chi}(p_j) \Big\} \quad \blacksquare$$

TEOREMA III.9. O grupo de unidades C' gerado por -1 e pelas unidades de Ramachandra ξ_a é de índice finito sobre o grupo E^+ das unidades de $\mathbb{Q}(\zeta)^+$, onde ζ é uma raiz primitiva f-ésima da unidade, $f\not\equiv 2 \pmod 4$.

DEMONSTRAÇÃO:

Temos, pelo Lema III.8, que

$$R(\xi_s) = \pm \prod_{\chi \neq 1} \frac{1}{2} \tau(\bar{\chi})\, L(1,\chi) \prod_{p_j \mid \frac{f}{h}} \left\{ \varphi(p_j^a) + 1 - \bar{\chi}(p_j) \right\}.$$

Mas, pelo Corolário II.2.11 e pelo Teorema II.2.15,

$$\prod_{\substack{\chi \neq 1 \\ \chi \text{ par}}} L(1,\chi) = \frac{2^{\frac{\varphi(f)}{2}}\, h^+ R^+}{2\sqrt{|d(\mathbb{Q}(\zeta)^+)|}} \quad \text{e} \quad \prod_{\substack{\chi \neq 1 \\ \chi \text{ par}}} \tau(\bar{\chi}) = \sqrt{|d(\mathbb{Q}(\zeta)^+)|}$$

onde h^+ é o número de classes de $\mathbb{Q}(\zeta)^+$, R^+ é o regulador de $\mathbb{Q}(\zeta)^+$, $d(\mathbb{Q}(\zeta)^+)$ é o discriminante de $\mathbb{Q}(\zeta)^+$ e χ percorre os caracteres pares não triviais de $\left(\frac{\mathbb{Z}}{f\mathbb{Z}}\right)^*$.

Logo, $R(\xi_s) = h^+ R^+ \prod_{\chi \neq 1} \prod_{p_j \mid \frac{f}{h}} \left\{ \varphi(p_j^a) + 1 - \bar{\chi}(p_j) \right\}$.

Também, pela Proposição II.2.17, $[E^+:C'] = \frac{R(\xi_s)}{R^+}$. Portanto,

$$[E^+:C'] = h^+ \prod_{\chi \neq 1} \prod_{p_j \mid \frac{f}{h}} \left\{ \varphi(p_j^a) + 1 - \bar{\chi}(p_j) \right\} \neq 0$$

e o teorema está provado.

LEMA III.10. Seja ζ uma raiz primitiva f-ésima da unidade, $f \not\equiv 2 \pmod 4$. Então $[E:C] = [E^+:C^+]$.

DEMONSTRAÇÃO:

Denotemos por W o grupo das raízes da unidade de $\mathbb{Q}(\zeta)$.

É claro que $W \subseteq C$ pois

$$-\zeta = \frac{1-\zeta}{1-\zeta^{-1}}$$

Afirmo que $E = E^+C$. De fato:

Se $f = p^a$, então, pelo Teorema II.2.16, $E = E^+W$ e, portanto, $E = E^+W \subseteq E^+C \subseteq E$, o que mostra a igualdade.

Seja, então, $f \neq p^a$. Temos $1-\zeta \in C$. Tomemos $\eta \in E$ e seja

$\beta = \frac{\eta}{\overline{\eta}}$. Logo, $|\beta| = 1$.

Para $\sigma \in G$, temos $\sigma(\beta) = \frac{\sigma(\eta)}{\sigma(\overline{\eta})} = \frac{\sigma(\eta)}{\overline{\sigma(\eta)}}$ e, então, $|\sigma(\beta)| = 1$, $\forall \ \sigma \in G$.

Logo, β é uma raiz da unidade e podemos, então, escrever $\beta = (-\zeta)^a$, $a \in \mathbb{Z}$. Daí, $\overline{\eta}(-\zeta)^a = \eta$.

Considere $\alpha = \eta(1-\zeta)^{-a}$ uma unidade. Temos que α é real, pois

$$\overline{\alpha} = \overline{\eta}(1-\zeta^{-1})^{-a} = (-\zeta^{-1})^{-a}\ \overline{\eta}\ (1-\zeta)^{-a} = \eta(1-\zeta)^{-a} = \alpha .$$

Logo, $\alpha \in E^+$. Vimos portanto que, dado $\eta \in E$, existe $\alpha \in E^+$ e $a \in \mathbb{Z}$ tais que $\eta = \alpha(1-\zeta)^a$, ou seja, $E \subseteq E^+C$. Como é claro que $E^+C \subseteq E$, a igualdade é verificada.

Temos, então

$$\frac{E}{C} \cong \frac{E^+C}{C} \cong \frac{E^+}{E^+ \cap C} \cong \frac{E^+}{C^+}$$

e o lema está provado. ∎

TEOREMA III.11. O grupo das unidades ciclotômicas C é de índice finito sobre o grupo E das unidades de $\mathbb{Q}(\zeta)$, onde ζ é uma raiz primitiva f-ésima da unidade, $f \not\equiv 2 \pmod 4$.

DEMONSTRAÇÃO:

Temos que o índice $[E^+:C^+]$ é finito pois $[E^+:C^+] = [E^+:C^+][C^+:C^+]$ e, pelo Teorema III.9, $[E^+:C^+]$ é finito.

Portanto o teorema está provado, pois pelo lema anterior $[E:C] = [E^+:C^+]$. ∎

[1] - APOSTOL, T.M. Mathematical Analysis, Addison-Wesley, 1958.

[2] - BOREVICH, Z.I.; SHAFAREVICH, I.R. Number Theory, Academic Press, 1973.

[3] - LANG, S. Algebraic Number Theory, Addison-Wesley, 1970.

[4] - LANG, S. Algebra, Addison-Wesley, 1965.

[5] - LONG, R. Algebraic Number Theory, Marcel Dekker, 1977.

[6] - RAMACHANDRA, K. On the units of cyclotomic fields, Acta Arithmetica 12(1966), 165-173.

[7] - RIBEMBOIM, P. Algebraic Numbers, Wiley-Interscience, 1972.

[8] - SAMUEL, P. Algebraic Theory of Numbers, Hermann, 1970.

[9] - SINNOTT, W. On the Stickelberger ideal and the circular units of a cyclotomic field, Annals of Mathematics (2), 108(1978), 107-134.

[10] - THAINE, F. On the ideal class groups of real abelian number fields, Annals of Mathematics 128(1988), 1-18.

[11] - WASHINGTON, L.C. Introduction to Cyclotomic Fields, Springer-Verlag, 1982.

[12] - WEISS, E. Algebraic Number Theory, McGraw-Hill, 1963.