UNIDADES DE CORPOS ABELIANOS

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pelo Sr. TRAJANO PIRES DA NÓBREGA NETO e aprovada pela Comissão Julgadora.

Campinas, 18 de julho de 1.991.

Prof. Dr. Francisco Thaine Prada
Orientador

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

AGRADECIMENTOS

Ao Professor Francisco Thaine, que me fez aprender e gostar de Teoria dos Números,

A minha esposa e aos meus filhos, pela paciência e pela compreensão,

Aos professores do IMECC, pela minha formação e pelo estímulo,

Ao CNPq e à CAPES, pelo auxílio financeiro,

Ao Departamento de Matemática de São José do Rio Preto, que além do incentivo, me concedeu condições adequadas para a realização deste trabalho,

Aos colegas da pós-graduação, pelo apoio e pela amizade,

A Deus, pela vida.

Dedico à

Marion,
Juliano,
Luciano,
Daniela e
Adriana.

ÍNDICE

INTRODUÇÃO

Este trabalho foi motivado pelo nosso interesse em responder a duas questões colocadas em artigos diferentes, por autores diferentes.

A primeira questão aparece em [4], onde Thaine define um certo grupo de unidades circulares de um corpo abeliano K, que neste trabalho será denotado por $C_T(K)$. Este conceito já havia sido utilizado por Sinnott em [6], quando este introduziu o grupo das unidades circulares de um corpo abeliano K e que aqui será denotado por $C_S(K)$.

O objetivo de Sinnott, ao definir as unidades circulares, era o de calcular o índice de $C_S(K)$ em $\mathfrak{O}_K^*$, o grupo das unidades do anel dos inteiros de K, motivado por um recente e bem sucedido resultado seu, ver [12], sobre este mesmo índice quando K é um corpo ciclotômico.

Por outro lado, o objetivo de Thaine ao definir $C_T(K)$ era o de obter anuladores para o grupo das classes de ideais de K, a partir de anuladores de W, onde W é o cociente das unidades de K por $C_T(K)$ e K é um corpo real abeliano.

A questão posta por Thaine em [4] era no sentido de se conhecer o índice de $C_S(K)$ em $C_T(K)$, pois a inclusão $C_S(K) \leq C_T(K)$ era evidente.

Resolvemos esta questão mostrando que $C_T(K) = C_S(K)$, para todo corpo abeliano K (Teorema 2.3.5). Ressaltamos que este resultado foi obtido, simultaneamente, por Günter Letl, ver [13], com técnicas completamente distintas daquelas usadas neste trabalho.

A segunda questão aparece em [7], onde Rubin introduz o conceito de unidade especial de um corpo abeliano K. O objetivo de Rubin com este novo grupo, aqui denotado por S(K), era o de estender resultados obtidos por Thaine em [4].

No Teorema 2.1 de [7], Rubin prova que quando K é o subcorpo real maximal de um corpo ciclotômico então S(K) contém um certo grupo de unidades de K (o grupo das unidades ciclotômicas de K definido por norma), que denotaremos por $C_N(K)$. Em seguida ele manifesta interesse em saber quando a inclusão acima citada é uma igualdade.

Respondemos esta questão provando que quando K é o subcorpo real maximal de um corpo ciclotômico, existe um outro grupo de unidades de K (o grupo das unidades ciclotômicas de K definido por intersecção), que denotaremos por $C_I(K)$, tal que $C_I(K) \leq S(K)$ (Teorema 3.1.4) e que $C_N(K)$ é um subgrupo próprio de $C_I(K)$ (Teorema 3.1.7).

Evidentemente que este tipo de resposta suscita um série de outras questões tais como: Seria agora S(K) igual a $C_I(K)$? Ou ainda, a inclusão acima citada não seria válida para qualquer corpo abeliano ?

Na tentativa de responder estas questões, nos deparamos com o problema de caracterizar as soluções da equação

$$\alpha = \xi_n^t \cdot \prod_{i=1}^{n-1} (1-\xi_n^i)^{a_i} = 1, \qquad (*)$$

onde ξ_n é uma raiz primitiva n-ésima da unidade.

Milnor havia conjecturado que as relações entre os expoentes

a_i de uma solução de (*) eram obtidas a partir das identidades

$1-\xi_n^i = -\xi_n^i.(1-\xi_n^{-i})$ e $\prod_{\substack{i=1 \\ i\equiv x(\mathrm{mod}\ b)}}^{n-1} (1-\xi_n^i) = 1-\xi_b^x$, quando b divide n.

Posteriormente H. Bass disse ter provado a veracidade desta afirmação; entretanto, em [10], V. Ennola encontrou um contra exemplo para a conjectura de Milnor e caracterizou as soluções de (*).

Usando esta caracterização dada por Ennola, podemos provar que se K é um corpo abeliano, cujo condutor é uma potência de primo, digamos q^a, e se $\varepsilon \in K$ é uma unidade ciclotômica de $\mathbb{Q}(\xi_{q^a})$, então ε é uma unidade especial de K (Teorema 3.1.11).

Há ainda uma outra definição de unidade especial, introduzida por Thaine em [8], com o objetivo de obter expressões exatas para as ordens de classes de ideais de corpos p-ciclotômicos em termos destas unidades. Uma nova caracterização destas unidades será dada no Capítulo 3 (Teorema 3.2.5).

Tendo como objetivo descrever as respostas para os problemas acima citados, este trabalho será dividido em três capítulos.

No primeiro Capítulo introduzimos parte da notação e alguns resultados básicos, com ênfase para os corpos ciclotômicos.

O objetivo deste Capítulo é dar uma introdução gradual aos fatos que serão utilizados no decorrer deste trabalho.

No segundo Capítulo dedicamos o primeiro parágrafo a estudar caracteres sobre grupos abelianos finitos. O segundo parágrafo destina-se ao estudo das relações entre unidades ciclotômicas, ou seja, damos uma descrição conveniente das soluções de (*). No parágrafo 3 respondemos a questão posta por Thaine em [4], ou seja, provamos que $C_T(K) = C_S(K)$.

No Capítulo 3 falamos de unidades especiais. No primeiro parágrafo introduzimos as unidades especiais definidas por Rubin e

respondemos a questão por ele proposta em [7]. Ainda no primeiro parágrafo provamos outros resultados; dentre os quais mostramos que se K é um corpo abeliano de condutor potência de primo então as unidades ciclotômicas de K definidas por intersecção são unidades especiais. No segundo parágrafo falamos sobres as unidades especiais definidas por Thaine, em [8]. Neste parágrafo conseguimos uma definição mais simples destas unidades.

Com o propósito de fixar notação e de evitar ao leitor frequentes consultas às referências, mostramos, ao longo deste trabalho, as provas de alguns resultados conhecidos.

CAPÍTULO 1

CORPOS CICLOTÔMICOS

Este capítulo tem como objetivo a introdução do leitor à notação usada neste trabalho e uma breve revisão de resultados básicos da Teoria dos Números Algébricos, com ênfase para os corpos ciclotômicos.

A maioria dos resultados aqui citados podem ser encontrados na bibliografia, especialmente [1] e [11].

Optamos por fazer algumas demonstrações por acharmos que estas contribuem para uma melhor compreensão do presente texto.

1.1 NOTAÇÃO

Sejam $a_1,\ldots,a_n$ números inteiros. Denotaremos por $[a_1,\ldots,a_n]$, (resp. $(a_1,\ldots,a_n)$) o menor múltiplo comum (resp. o maior divisor comum) de $a_1,\ldots,a_n$. Estaremos sempre supondo que $[a_1,\ldots,a_n]$ (resp. $(a_1,\ldots,a_n)$) é positivo.

É sabido que dados os números inteiros $a_1,\ldots,a_n$ existem números $r_1,\ldots,r_n \in \mathbb{Z}$ tais que $a_1.r_1+\ldots+a_n.r_n = (a_1,\ldots,a_n)$. Em particular, se $a_1,\ldots,a_n$ são números inteiros primos entre si então existem números inteiros $r_1,\ldots,r_n$ tais que

$$a_1.r_1+\ldots+a_n.r_n = 1. \qquad (1.1)$$

Tal fato será usado com alguma frequência sem maiores justificativas.

Sejam n e m números inteiros, $n \neq 0$. Se existir um número inteiro r tal que $m = n.r$ dizemos que n divide m e denotaremos por

$n|m$. Sejam n , m e a números inteiros, $n \neq 0$, a não negativo. Se n^a divide m mas n^{a+1} não divide m, escrevemos $n^a || m$.

Consideramos a função:

$$\phi : \mathbb{N} \longrightarrow \mathbb{N}$$

tal que $\phi(1) = 1$ e se $P_1,\ldots,P_s$ são primos distintos e $a_i > 0$ então

$$\phi(P_1^{a_1}.....P_s^{a_s}) = (P_1-1)P_1^{a_1-1}.....(P_s-1)P_s^{a_s-1} .$$

A função acima descrita é conhecida como a função ϕ de Euler e algumas de suas propriedades serão aqui listadas.

Dados n e m números inteiros maiores que 1 temos:

P.1- $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$.

P.2- Se $n|m$ então $\phi(n)|\phi(m)$.

P.3- Se $(n,m) = 1$ então $\phi(n.m) = \phi(n).\phi(m)$.

Lema 1.1.1: Sejam n e m números inteiros positivos. Então $\phi(n).\phi(m) = \phi((n,m)).\phi([n,m])$.

Demonstração: Suponhamos

$$n = P_1^{a_1} \ldots P_s^{a_s}.\ P'_1{}^{b_1} \ldots P'_r{}^{b_r} \qquad e$$

$$m = P_1^{c_1} \ldots P_s^{c_s}\ P''_1{}^{d_1} \ldots P''_t{}^{d_t}$$

com a_i, b_i , c_i , d_i números inteiros positivos, P_i, P'_j e P''_k números primos distintos.

Se $e_i = \min\{ a_i, c_i \}$ e $f_i = \max\{ a_i, c_i \}$ temos:

$$\phi((n,m)) = (P_1 - 1).P_1^{e_1-1} \ldots (P_s - 1).P_s^{e_s-1} \qquad e$$

$$\phi([n,m]) = (P_1 - 1)\,P_1^{f_1-1} \ldots (P_s - 1)\,P_s^{f_s-1}\,(P'_1 - 1)\,P'_1{}^{b_1-1} \ldots$$

$$(P'_r - 1).P'_r{}^{b_r-1}.(P''_1 - 1).P''_1{}^{d_1-1} \ldots (P''_t - 1).P''_t{}^{d_t-1} .$$

Logo $\phi((n,m)).\phi([n,m]) = \phi(n).\phi(m)$, pois $e_i + f_i = a_i + c_i$ e o lema está provado.

Sejam n e m números inteiros maiores que 1. Suponhamos que $(n,m) = 1$. Se r e s são inteiros tais que $(r,m) = (s,n) = 1$ então $(r.n + s.m,\ n.m) = 1$. Além disso, dados r' e s' inteiros, com $(r', m) = (s',n) = 1$; se $r.n + s.m \equiv r'.n + s'.m \pmod{n.m}$ então $(r - r').n + (s - s').m \equiv 0 \pmod{n.m}$. Logo n divide $(s- s')$ e m divide $(r-r')$, ou seja, $r \equiv r' \pmod{m}$ e $s \equiv s' \pmod{n}$. Posto isso, seja R (resp S) um subconjunto de $\mathbb{Z}$ cujos elementos são primos com m (resp. n) com $\phi(m)$ (resp. $\phi(n)$) elementos tal que dois elementos distintos quaisquer de R (resp. S) não são congruentes mod m (resp. mod n)). (Isto é, sejam R um sistema reduzido de rezíduos mod m e S um sistema reduzido de rezíduos mod n). Se P é o conjunto $\{ a = r.n + s.m : r \in R,\ s \in S \}$, então P tem $\phi(n).\phi(m) = \phi(n.m)$ classes de congruência distintas mod n.m, e todo elemento de P é primo com n.m. Com isso temos provado o

Lema 1.1.2 : Sejam n e m números inteiros maiores que 1. Suponhamos que $(n,m) = 1$. Seja R (resp. S e T) um subconjunto de $\mathbb{Z}$, cujos elementos são primos com m (resp. n e n.m), com $\phi(m)$ (resp. $\phi(n)$ e $\phi(n.m)$) elementos tais que dois elementos quaisquer distintos de R (resp. S e T) não são congruentes mod m (resp. mod n e mod n.m). Então os conjuntos T e $U = \{ r.n + s.m : r \in R,\ s \in S \}$ são iguais mod n.m, isto é, dado $u \in U$ existe um único $t \in T$ tal que $t \equiv u \pmod{n.m}$; e vice-versa, dado $t \in T$ existe um único $u \in U$ tal que $u \equiv t \pmod{n.m}$.

1.2 CORPOS DE NÚMEROS

Definição 1.2.1 : Chamamos de corpo de números a toda extensão

finita K dos racionais. Se $K/\mathbb{Q}$ é uma extensão galoisiana e $Gal(K/\mathbb{Q})$ é abeliano então dizemos que K é um corpo de números abeliano ou simplesmente K é um corpo abeliano.

Sendo K uma extensão finita de $\mathbb{Q}$, todo elemento x de K é raiz de um polinômio não nulo a coeficientes inteiros. Se um polinômio não nulo de $\mathbb{Z}[X]$ que tem x como raiz for mônico então dizemos que x é integral sobre $\mathbb{Z}$. O subconjunto de K formado pelos elementos integrais sobre $\mathbb{Z}$ é um anel de Dedekind, (ver [11], Teorema 1 pg. 59) o qual denotaremos por $\mathfrak{O}_K$ e chamaremos de anel dos inteiros de K.

O maior interesse deste trabalho concentra-se no conjunto dos elementos inversíveis de $\mathfrak{O}_K$, que denotaremos por $\mathfrak{O}_K^*$ e chamaremos de grupo das unidades de K.

Dado um corpo de números K, sabe-se que existem n imersões de K em $\mathbb{C}$, onde $n = [K:\mathbb{Q}]$ (ver [11], Teorema 1, pg. 40). Destas imersões r_1 são reais, isto é, K é imerso no corpo dos números reais, e $2.r_2$ são complexas. Introduzidos estes números, podemos enunciar o Teorema de Dirichlet sobre a estrutura de $\mathfrak{O}_K^*$. Sua demonstração pode ser encontrada em [11], pg. 72.

Teorema 1.2.2 : Sejam K um corpo de números e $n = [K:\mathbb{Q}] = r_1 + 2.r_2$, onde r_1 e r_2 são os números inteiros acima definidos. Então $\mathfrak{O}_K^*$ é o produto de um grupo cíclico finito, o grupo das raízes da unidade contidas em K, por um $\mathbb{Z}$-módulo livre de posto $r = r_1 + r_2 - 1$.

Sejam $K \subseteq L$ corpos de números e $G_{L/K}$ o conjunto de todas as K-imersões de L em $\mathbb{C}$.

Definição 1.2.3 : Com a notação acima, se $x \in L$, chamamos de norma

(resp. traço) de L sobre K de x, e denotamos por $N_{L/K}(x)$ (resp. $T_{L/K}(x)$), ao elemento $\prod_{\tau \in G_{L/K}} \tau(x)$ (resp. $\sum_{\tau \in G_{L/K}} \tau(x)$).

A demonstração do seguinte fato pode ser encontrada em [11], pg. 45.

Proposição 1.2.4 : Sejam $K \subseteq L$ corpos de números e $x \in L$. Então $N_{L/K}(x)$, $T_{L/K}(x) \in K$.

Como consequência da Proposição 1.2.4 podemos deduzir que se $x \in \mathfrak{O}_L$ então $N_{L/K}(x)$, $T_{L/K}(x) \in \mathfrak{O}_K$. Mais ainda, se $x \in \mathfrak{O}_L^*$ então $N_{L/K}(x) \in \mathfrak{O}_K^*$.

Teorema 1.2.5 : Sejam K um corpo de números e $x \in K$. Então $x \in \mathfrak{O}_K^*$ se e somente se $x \in \mathfrak{O}_K$ e $N_{K/\mathbb{Q}}(x) = \pm 1$.

Este teorema dá uma breve caracterização do grupo das unidades de um corpo de números K e sua demonstração pode ser encontrada em [11], pg.72. Mais geralmente, sabemos que se $K \subseteq L \subseteq M$ são corpos de números então:

$$T_{M/K} = T_{L/K} \circ T_{M/L} \quad e \quad N_{M/K} = N_{L/K} \circ N_{M/L}.$$

(ver [11], pg. 111).

Corolário 1.2.6 : Sejam $K \subseteq L$ corpos de números e $x \in L$. Então $x \in \mathfrak{O}_L^*$ se e somente se $x \in \mathfrak{O}_L$ e $N_{L/K}(x) \in \mathfrak{O}_K^*$.

Demonstração : Se $x \in \mathfrak{O}_L^*$ então $N_{L/K}(x) \in \mathfrak{O}_K^*$ pela observação anterior ao Teorema 1.2.5. Reciprocamente, se $x \in \mathfrak{O}_L$ e se $N_{L/K}(x) \in \mathfrak{O}_K^*$ então $N_{L/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(N_{L/K}(x)) = \pm 1$. Com isto temos $x \in \mathfrak{O}_L$ e $N_{L/\mathbb{Q}}(x) = \pm 1$ no que implica em $x \in \mathfrak{O}_L^*$.

A seguir faremos um breve resumo dos principais resultados envolvendo o automorfismo de Frobenius para um primo $\mathfrak{p}$ de um corpo de números K. As respectivas demonstrações podem ser encontradas em [11], Capítulo 5.

Sejam K um corpo de números e $\mathfrak{O}_K$ o seu anel de inteiros. Sendo $\mathfrak{O}_K$ um domínio de Dedekind, todo ideal de $\mathfrak{O}_K$ se fatora de modo único como um produto de ideais primos de $\mathfrak{O}_K$. Se L é um corpo de números, $K \subseteq L$ e $\mathfrak{a}$ é um ideal de K, então $\mathfrak{a}\mathfrak{O}_L$ será o ideal de $\mathfrak{O}_L$ gerado pelos elementos de $\mathfrak{a}$. O ideal $\mathfrak{a}\mathfrak{O}_L$ é dito o levantamento de $\mathfrak{a}$ em $\mathfrak{O}_L$.

Seja $\mathfrak{p}$ um ideal primo de $\mathfrak{O}_K$. Então existem inteiros positivos s, e_i; $i = 1,\ldots,s$ tais que

$$\mathfrak{p}\mathfrak{O}_L = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i} \qquad (1.2)$$

onde os $\mathfrak{q}_i$ são os ideais primos $\mathfrak{q}$ de $\mathfrak{O}_L$ tais que $\mathfrak{q} \cap \mathfrak{O}_K = \mathfrak{p}$. Neste caso dizemos que $\mathfrak{q}_i$ divide $\mathfrak{p}$ ou que $\mathfrak{q}_i$ é um ideal de L que está acima de $\mathfrak{p}$. Além disto temos

$$\sum_{i=1}^{s} e_i . [\ \mathfrak{O}_L/\mathfrak{q}_i : \mathfrak{O}_K/\mathfrak{p}\ ] = [\ L : K\ ]. \qquad (1.3)$$

A equação (1.3) é conhecida como igualdade fundamental do ideal primo $\mathfrak{p}$ na extensão L/K.

Para $1 \leq i \leq s$, o número inteiro e_i que aparece na equação (1.2) é dito índice de ramificação de $\mathfrak{q}_i$ na extensão L/K. Se pelo menos um destes números é maior que 1 dizemos que o ideal primo $\mathfrak{p}$ se ramifica na extensão L/K. Além disto se $e_i = [L:K]$, para algum i, então $s = 1$ e, neste caso, diz-se que o ideal primo $\mathfrak{p}$ se ramifica completamente em L. Por outro lado, se $s = [L:K]$, então $e_i = 1$, para todo $i = 1,\ldots,s$ e dizemos que o ideal primo $\mathfrak{p}$ se decompõe completamente em L.

Se L/K é uma extensão galoisiana e $\mathfrak{q}_1$ e $\mathfrak{q}_2$ são dois ideais primos de L tais que $\mathfrak{q}_1 \cap \mathfrak{O}_K = \mathfrak{q}_2 \cap \mathfrak{O}_K$ então existe um

K-automorfismo de L que leva q_1 em q_2 e consequentemente os índices de ramificação de q_1 e q_2 são iguais e $\mathfrak{O}_L/q_1 \simeq \mathfrak{O}_L/q_2$. Portanto, neste caso, a igualdade fundamental para o primo p de K fica:

$$[\ L\ :\ K\ ] = e.f.g \qquad (1.4)$$

onde e é o índice de ramificação de q e $f = [\mathfrak{O}_L/q\ :\ \mathfrak{O}_K/p]$, onde q é qualquer ideal primo de L acima de p e g é o número de ideais primos de L acima de p.

Sejam L/K um extensão galoisiana , p um ideal primo de K que não se ramifica em L e p' um ideal primo de L que está acima de p. Sabe-se que existe um único K-automorfismo γ de L, que tem a seguinte propriedade:

$$\gamma(x) \equiv x^p \pmod{p'} \quad \forall\ x \in \mathfrak{O}_L \qquad (1.5)$$

onde $p = \#(\mathfrak{O}_K/p)$.

O K-automorfismo acima descrito é denominado de automorfismo de Frobenius para o primo p' na extensão L/K. Quando a extensão L/K é abeliana então tal automorfismo só depende do ideal primo p e, neste caso, costumamos nos referir apenas ao automorfismo de Frobenius do primo p, quando não há ambiguidade quanto à extensão L/K.

Sabe-se também que, no caso L/K abeliano, o automorfismo de Frobenius para um ideal primo p de K que não se ramifica em L é a identidade de Gal(L/K) se e somente se o ideal primo p se decompõe completamente em L.

1.3 CORPOS CICLOTÔMICOS

Dado um número inteiro positivo n, seja $\xi_n = e^{2\pi i/n} \in \mathbb{C}$. É fácil ver que ξ_n é uma raiz primitiva n-ésima da unidade, isto é, $\xi_n^m = 1$ se e somente se n divide m. Além disto, se r é um número

inteiro então ξ_n^r é uma raiz primitiva n-ésima da unidade se e somente se $(r,n) = 1$. Mais geralmente, visto que $\xi_n^r = \xi_{n'}^{r'}$, onde $r' = r/(r,n)$ e $n' = n/(r,n)$, segue-se que ξ_n^r é uma raiz primitiva n'-ésima da unidade, onde n' é como acima.

Definição 1.3.1 : Dado um número inteiro positivo n, chamamos de n-ésimo corpo ciclotômico, e denotamos por K_n, o corpo $\mathbb{Q}(\xi_n)$ e K_n^+ denotará o subcorpo real maximal de K_n, ou seja, $K_n^+ = K_n \cap \mathbb{R}$.

É um fato conhecido (ver [1]) que K_n (resp. K_n^+) é um corpo de números abeliano cujo grupo de Galois, aqui denotado por G_n (resp. G_n^+) é isomorfo ao grupo $(\mathbb{Z}/n\mathbb{Z})^*$ (resp. $(\mathbb{Z}/n\mathbb{Z})^*/(\pm 1)$) e portanto $[K_n:\mathbb{Q}] = \phi(n)$ (resp. $[K_n^+:\mathbb{Q}] = \phi(n)/2$), onde ϕ é a função de Euler.

Teorema 1.3.2 : (Kronecker-Weber) Seja K um corpo de números. Se K é abeliano então existe um número inteiro positivo n tal que $K \subseteq K_n$.

Uma demonstração deste teorema pode-se encontrar em [1].

Definição 1.3.3 : Seja K um corpo abeliano. Ao menor número inteiro positivo n tal que $K \subseteq K_n$, daremos o nome de condutor de K.

Seja n um número inteiro positivo e suponhamos que $n \equiv 2 \pmod 4$. Então $\xi_n^2 = \xi_{n/2}$, e n/2 é ímpar. Visto que a ordem de -1 é 2, a ordem de $\xi_{n/2}$ é n/2 e $(2, n/2) = 1$ segue que a ordem de $-\xi_{n/2}$ é n, ou seja,

Lema 1.3.4: Seja n um número inteiro positivo. Se $n \equiv 2 \pmod 4$ então $-\xi_{n/2}$ é uma raiz primitiva n-ésima da unidade.

Visto que $\mathbb{Q}(-\xi_{n/2}) = \mathbb{Q}(\xi_{n/2}) = K_{n/2}$, pelo lema acima, concluimos que se n é um número inteiro positivo, $n \equiv 2 \pmod 4$,

então $K_n = K_{n/2}$. Tendo em vista esta igualdade, toda vez que nos referimos a um corpo ciclotômico K_n podemos supor que $n \not\equiv 2 \pmod 4$.

Lema 1.3.5 : Sejam n e m números inteiros positivos. Então $K_n.K_m = K_{[n,m]}$.

Demonstração : O produto $K_n.K_m$ é, por definição, o menor corpo que contém K_n e K_m, ou seja, o menor corpo que contém $\mathbb{Q}$, ξ_n e ξ_m. Visto que $\xi_n = \xi_{[n,m]}^{[n,m]/n}$ e $\xi_m = \xi_{[n,m]}^{[n,m]/m}$ segue-se que ξ_n , $\xi_m \in K_{[n,m]}$, ou seja, $K_n.K_m \subseteq K_{[n,m]}$. Sejam r e s números inteiros tais que $r.m + s.n = (n,m)$. É evidente que ξ_n^r, $\xi_m^s \in K_n.K_m$ e $\xi_n^r.\xi_m^s = \xi_{n.m}^{r.m}.\xi_{n.m}^{s.n} = \xi_{n.m.}^{r.m+s.n} = \xi_{n.m}^{(n,m)} = \xi_{n.m/(n,m)} = \xi_{[n,m]}$, pois dados dois números inteiros n e m tem-se $n.m = (n,m).[n,m]$. Com isto temos visto que $\xi_{[n,m]} \in K_n.K_m$, logo $K_{[n,m]} \subseteq K_n.K_m$ e consequentemente $K_{[n,m]} = K_n.K_m$ e o lema está provado.

O nosso próximo passo é provar que $K_n \cap K_m = K_{(n,m)}$; para tanto precisamos de um teorema da teoria de Galois cuja demonstração será omitida neste texto, mas pode ser encontrada em [5], pg. 196.

Teorema 1.3.6 : Sejam K uma extensão galoisiana de k e F uma extensão de k. Supondo K e F subcorpos de um mesmo corpo, tem-se K.F galoisiana sobre F, com $Gal(K.F/F) \cong Gal(K/ K \cap F)$.

Teorema 1.3.7 : Sejam n e m números inteiros positivos. Então $K_n.K_m = K_{[n,m]}$, $K_n \cap K_m = K_{(n,m)}$ e $Gal\,(K_{[n,m]}/K_m) \cong Gal\,(K_n/K_{(n,m)})$.

Demonstração: A igualdade $K_n.K_m = K_{[n,m]}$ consiste do Lema 1.3.5. Se mostrarmos que $K_n \cap K_m = K_{(n,m)}$ então o isomorfismo $Gal(K_{[n,m]}/K_m)$

$\cong Gal(K_n/K_{(n,m)})$ é consequência do Teorema 1.3.6, tomando $K = K_n$, $F = K_m$ e $k = K_{(n,m)}$.

Visto que para todo número inteiro positivo n, $[K_n : \mathbb{Q}] = \phi(n)$ tem-se $[K_{[n,m]} : K_m] = \phi([n,m])/\phi(m)$. Do Lema 1.1.1 temos $\frac{\phi([n,m])}{\phi(m)}$ $= \frac{\phi(n)}{\phi((n,m))}$ e portanto $[K_{[n,m]} : K_m] = [K_n : K_{(n,m)}]$. Por outro lado a igualdade $[K_{[n,m]} : K_m] = [K_n : K_n \cap K_m]$ decorre do Teorema 1.3.6, ou seja, $[K_n : K_n \cap K_m] = [K_n : K_{(n,m)}]$. Visto que $K_{(n,m)} \subseteq K_n \cap K_m$, pois $\xi_{(n,m)} = \xi_n^{n/(n,m)} = \xi_m^{m/(n,m)}$; obtemos a igualdade desejada.

É resultado conhecido (ver [1]) que o anel dos inteiros $\mathfrak{O}_{K_n}$ de K_n é $\mathbb{Z}[\xi_n]$. Pelo Teorema 1.2.2, o grupo das unidades $\mathfrak{O}_{K_n}^*$ de K_n é isomorfo ao produto de um grupo cíclico finito por um $\mathbb{Z}$-módulo livre de posto $\frac{\phi(n)}{2} - 1$. O grupo cíclico finito é constituido pelas raizes da unidade contidas em K_n e pode-se provar que tal grupo é $\langle \pm \xi_n^i,\ i = 0,1,\ldots,n-1 \rangle$. Quanto a parte livre pouco se sabe.

Todavia se conhecem subgrupos de $\mathfrak{O}_{K_n}^*$ que, a menos da parte de torção, são isomorfos a $\mathfrak{O}_{K_n}^*$. Evidentemente um subgrupo E de $\mathfrak{O}_{K_n}^*$ satisfaz a condição acima se e somente se o índice $[\mathfrak{O}_{K_n}^* : E]$ é finito.

Seja V_n o subgrupo de K_n^* gerado pelos elementos $\langle -1,\ \xi_n,\ 1-\xi_n^i,$ $i = 1,2,\ldots,n-1 \rangle$.

Definição 1.3.8: Sejam n um número inteiro positivo e V_n o subgrupo

de K_n^* acima definido. Definimos o grupo das unidades ciclotômicas de K_n, e denotamos por C_n, como sendo a intersecção $V_n \cap \mathcal{O}_{K_n}^*$.

Visto que ξ_n^i , $i=0,\ldots,n-1$, são todas as raizes do polinômio $X^n - 1$, temos

$$\frac{X^n - 1}{X - 1} = 1 + X + \ldots + X^{n-1} = \prod_{i=1}^{n-1}(X-\xi_n^i).$$

Fazendo $X = 1$, temos a identidade:

$$n = \prod_{i=1}^{n-1}(1-\xi_n^i). \qquad (1.6)$$

Lema 1.3.9 : Se n é uma potência de primo, digamos $n = p^a$, p um número primo e a um número inteiro positivo então $N_{K_n/\mathbb{Q}}(1-\xi_n^i) = p^{(n,i)}$, se $i \not\equiv 0 \pmod n$. Em particular $1-\xi_n^i$ não é uma unidade de K_n.

Demonstração : Se $a = 1$, pela identidade (1.6) temos:

$$p = \prod_{i=1}^{p-1}(1-\xi_p^i) = N_{K_p/\mathbb{Q}}(1-\xi_p^j), \ \forall\ j = 1,2,\ldots,p-1.$$

Se $a > 1$, ainda pela identidade (1.6) , temos:

$$p^a = \prod_{i=1}^{p^a-1}(1-\xi_{p^a}^i) = \prod_{\substack{i=1 \\ (i,p)=1}}^{p^a-1}(1-\xi_{p^a}^i).\prod_{i=1}^{p^{a-1}-1}(1-\xi_{p^a}^{pi}) = N_{K_{p^a}/\mathbb{Q}}(1-\xi_{p^a}^j).p^{a-1},$$

$\forall\ j = 1,2,\ldots,p^{a-1}$; $(j,p) = 1$, e portanto, se $(j,n) = 1$ então $N_{K_n/\mathbb{Q}}(1-\xi_n^j) = p$. Se $j = j'.p^b$, com $(j',p) = 1$, $0 < b < a$, então $1-\xi_{p^a}^j = 1-\xi_{p^{a-b}}^{j'}$ é consequentemente, pelo caso anterior,

$$N_{K_p{}^a / \mathbb{Q}}(1-\xi_p{}^j{}^a) = \left[N_{K_p{}^{a-b} / \mathbb{Q}}\left(1-\xi_p{}^{j'}{}^{a-b}\right)\right]^{p^b} = p^{p^b}. \qquad (1.7)$$

A não invertibilidade de $1-\xi_n^j$ em $\mathcal{O}_{K_n}$ decorre do Teorema 1.2.5 e o lema está provado.

Observação 1.3.10: Seja $n = q_1^{a_1}.....q_s^{a_s}$ um número inteiro positivo. Se $1 \leq i \leq q_1^{a_1}-1$ e $1 \leq j \leq q_2^{a_2}-1$ (estamos supondo $s \geq 2$), então os números

$$\left[n / q_1^{a_1} \right].i \quad \text{e} \quad \left[n / q_2^{a_2} \right].j \quad \text{são distintos.}$$

Seja S o conjunto

$$\left\{ j = 1,2,...., n-1 \ : \ n/(j,n) \text{ é uma potência de primo} \right\}.$$

Lema 1.3.11: Preservando a notação acima, $1-\xi_n^j$ é uma unidade de K_n se e somente se $j \notin S$.

Demonstração: Visto que $1-\xi_n^j = 1-\xi_{n/(n,j)}^{j/(n,j)}$ segue do Lema 1.3.9 que se $1-\xi_n^j$ é uma unidade então $n/(j,n)$ não é uma potência de primo, ou seja, $j \notin S$. Pela identidade (1.6) tem-se:

$$n = \prod_{i=1}^{n-1}(1-\xi_n^i) \quad \text{e} \quad q_i^{a_i} = \prod_{t=1}^{q_i^{a_i}-1}\left(1-\xi_n^{(n/q_i^{a_i}).t}\right).$$

Logo $1 = \prod_{j \notin S}(1-\xi_n^j)$. Visto que $1-\xi_n^j \in \mathcal{O}_{K_n}$, segue-se que para os números inteiros $j = 1,...,n-1$, $j \notin S$, $1-\xi_n^j \in \mathcal{O}_{K_n}^*$, o que completa a demonstração do lema.

Até aqui temos estabelecido condições necessárias e

suficientes para que $1-\xi_n^i$ seja uma unidade de K_n.

Sejam $n = \prod_{i=1}^{s} q_i^{a_i}$ e $\varepsilon = \prod_{i=1}^{n-1}(1-\xi_n^i)^{b_i} \in K_n$.

Queremos estabelecer condições necessárias e suficientes para que ε seja uma unidade ciclotômica de K_n.

Pelo Lema 1.3.11, ε é uma unidade de K_n se e somente se $\varepsilon' = \prod_{\substack{i=1 \\ i\in S}}^{n-1}(1-\xi_n^i)^{b_i}$ é uma unidade de K_n. Neste caso podemos escrever

$$\varepsilon' = \prod_{j=1}^{s} \varepsilon'_j \text{ , com } \varepsilon'_j = \prod_{\substack{i=1 \\ i\in S_j}}^{n-1}(1-\xi_n^i)^{b_i}, \qquad (1.8)$$

onde

$$S_j = \left\{ i = 1,2,\ldots,n-1 : n/(i,n) \text{ é uma potência do primo } q_j \right\}$$

pois, pela Observação 1.3.10 S é a reunião disjunta dos subconjuntos S_j.

Visto que $N_{K_n/\mathbb{Q}}(\varepsilon'_j)$ é uma potência de q_j, deduzimos que para ε' ter norma, de K_n para $\mathbb{Q}$, igual a 1, devemos ter $N_{K_n/\mathbb{Q}}(\varepsilon'_j) = 1$ e portanto $N_{K_{q'_j}/\mathbb{Q}}(\varepsilon'_j) = 1$, onde $q'_j = q_j^{a_j}$.

Lema 1.3.12 : Sejam n um número inteiro positivo, $\gamma \in G_n$ e i um número inteiro não múltiplo de n. Então $\varepsilon = (1-\xi_n^i)^{\gamma-1}$ é uma unidade de K_n.

Demonstração : Seja $r \in \mathbb{Z}$ tal que $\gamma(\xi_n) = \xi_n^r$, logo $(r,n) = 1$ e portanto existe um número inteiro positivo y tal que $y.r \equiv 1$

(mod n). Para provar que ε é uma unidade de K_n devemos mostrar que ε, $\varepsilon^{-1} \in \mathbb{Z}[\xi_n]$. De fato $(1-\xi_n^{ri})/(1-\xi_n^{i}) = 1 + \xi_n^{i} + \ldots + \xi_n^{(r-1)i} \in \mathbb{Z}[\xi_n]$. Por outro lado $\varepsilon^{-1} = (1-\xi_n^{i})/(1-\xi_n^{r\cdot i}) = (1-\xi_n^{y\cdot r\cdot i})/(1-\xi_n^{r\cdot i})$ e portanto $\varepsilon^{-1} = 1 + \xi_n^{r\cdot i} + \ldots + \xi_n^{(y-1)\cdot r\cdot i} \in \mathbb{Z}[\xi_n]$ e portanto $\varepsilon \in \mathcal{O}_{K_n}^{*}$.

Teorema 1.3.13: Sejam $n = \prod_{i=1}^{s} q_i^{a_i}$ e $\varepsilon = \pm\xi_n^{t}\cdot\prod_{i=1}^{n-1}(1-\xi_n^{i})^{b_i}$ um elemento ciclotômico de K_n. Então ε é uma unidade se e somente se

$$\sum_{j=1}^{q_i'-1} (j,q_i')\cdot b_{(n/q_i')\cdot j} = 0 \quad \forall\ i = 1,\ldots,s$$

onde $q_i' = q_i^{a_i}$.

Demonstração : Sejam ε' e ε_j' como em (1.8). Já sabemos que ε é uma unidade de K_n se e somente se ε_j' é uma unidade de $K_{q_j'}$, $j = 1,\ldots,s$; ou seja, podemos supor que n é uma potência de primo, digamos $n = q^a$, e devemos mostrar que ε é uma unidade de K_n se e somente se $\sum_{j=1}^{n-1} (j,n)\cdot b_j = 0$.

Pela equação (1.7), $N_{K_n/\mathbb{Q}}(1-\xi_n^{j}) = q^{(j,q^a)}$, logo $N_{K_n/\mathbb{Q}}(\varepsilon) = q^{\sum_{j=1}^{n-1}(j,q^a)\cdot b_j}$. Pelo Teorema 1.2.5, se ε é uma unidade então $N_{K_n/\mathbb{Q}}(\varepsilon) = \pm 1$ e portanto $\sum_{j=1}^{n-1}(j,q^a)\cdot b_j = 0$. Agora devemos mostrar que se $\sum_{j=1}^{n-1}(j,q^a)\cdot b_j = 0$ então ε é uma unidade de K_n. Afirmamos

que $(1-\xi_n^j)/(1-\xi_n)^{(j,q^a)}$ é uma unidade de K_n. Se $(j,n) = 1$, isto é, se j é primo com q, isto decorre do Lema 1.3.12. Agora suponhamos que $(j,q^a) = q^b$, com $0 < b < a$. Neste caso podemos escrever $j = q^b.k$, onde $(k,q) = 1$. Agora

$$1-\xi_n^{q^b.k} = 1-\left(\xi_n^k\right)^{q^b} = \prod_{j=1}^{q^b}\left(1-\xi_{q^b}^{j}.\xi_n^k\right) = \prod_{j=1}^{q^b}\left(1-\xi_n^{j.q^{a-b}+k}\right). \qquad (1.9)$$

Visto que $(k,q) = 1$, então $t_j = j.q^{a-b} + k$ é primo com q, logo $(1-\xi_n^{t_j})/(1-\xi_n)$ é uma unidade de K_n, $\forall$ $j = 1,\ldots,q^b$, pelo Lema 1.3.12. Destas considerações deduzimos que $(1-\xi_n^j)/(1-\xi_n)^{(j,n)}$ e $(1-\xi_n^j)^{b_j}/(1-\xi_n)^{(j,n).b_j}$ são unidades de K_n. Logo

$\delta = \prod_{j=1}^{n-1}\left((1-\xi_n^j)^{b_j}/(1-\xi_n)^{(j,n).b_j}\right)$ é uma unidade de K_n. Mas $n = q^a$ e $\sum_{j=1}^{n-1}(j,q^a).b_j = 0$, portanto $\varepsilon = \pm\xi_n^t.\delta$ é uma unidade de K_n e o teorema está provado.

Com isto temos caracterizado quando um elemento ciclotômico de K_n é uma unidade ciclotômica de K_n.

Descrever explicitamente uma base para C_n, a menos das raízes da unidade, sempre foi um desafio fascinante. O primeiro registro que temos deste problema é uma carta de Milnor, enviada a Ramanathan, com data de 6 de fevereiro de 1.964. Nesta carta Milnor observa que os elementos

$$u_s = (1-\xi_n^s)/(1-\xi_n)\ , \quad 1 < s < n/2\ ,\ (s,n) = 1 \qquad (1.10)$$

são unidades ciclotômicas de K_n (nosso Lema 1.3.12). Se $s > n/2$, então $(1-\xi_n^s)/(1-\xi_n) = -\xi_n^s.u_{n-s}$, ou seja, as unidades u_s de (1.10)

geram, a menos de raízes da unidade, o subgrupo C_n' de C_n formado pelas unidades ciclotômicas do tipo

$$\varepsilon = \prod_{\substack{i=1 \\ (i,n)=1}}^{n-1} (1 - \xi_n^i)^{a_i}. \qquad (1.11)$$

Ora, em (1.10) temos $(\phi(n)/2)-1$ unidades ciclotômicas, número este que coincide com o $\mathbb{Z}$-posto de C_n e daí a pergunta de Milnor, se não seria C_n' o grupo de todas as unidades ciclotômicas de K_n.

Quando n é uma potência de número primo a resposta para a questão de Milnor é afirmativa. Entretanto a resposta para o caso geral foi dada em 1.966, ver [9], onde Ramachandra considera o caso em que n é um número inteiro com dois divisores primos ímpares p e q, com $p \equiv 1 \pmod{q}$ e existe um homomorfismo não trivial de $(\mathbb{Z}/q\mathbb{Z})^*$ em $\mathbb{C}^*$ que leva -1 em 1. Para os números inteiros n com estas propriedades, Ramachandra provou, em [9], que o grupo C_n' terá o $\mathbb{Z}$-posto menor que o $\mathbb{Z}$-posto de C_n e portanto a resposta para a questão de Milnor é negativa. Ainda em [9], Ramachandra exibiu, para todo número inteiro positivo n, um conjunto com $(\phi(n)/2)-1$ unidades ciclotômicas, que gera um subgrupo C_n'' cujo índice em C_n é finito. Até então havia duas questões concretas: explicitar uma base para C_n e calcular o índice de C_n em $\mathcal{O}_{K_n}^*$. Esta última questão foi resolvida por Sinnott em [12], onde este provou que $[\mathcal{O}_{K_n}^* : C_n]$ é igual ao número das classes de K_n. Quanto à base para C_n alguns resultados parciais foram obtidos mas o problema não foi resolvido por completo.

Definição 1.3.14 : Seja K um corpo abeliano de condutor n. O grupo das unidades ciclotômicas de K definido por intersecção (resp. por norma) é o conjunto $C_n \cap K$ (resp. $N_{K_n/K}(C_n)$) e será denotado por

$C_J(K)$ (resp. $C_N(K)$).

Lema 1.3.15 : Sejam r e s números inteiros positivos. Se r divide s então

$$Gal(K_s/K_r) = \left\{ \gamma_t \in G_s \text{ tais que } t \equiv 1 \pmod{r}, \text{ onde } \gamma_t(\xi_s) = \xi_s^t \right\}.$$

Demonstração : Dado $\gamma_t \in G_s$, tem-se $\gamma_t(\xi_r) = \gamma_t(\xi_s^{s/r}) = \xi_s^{(s/r).t} = \xi_r^t$. Mas $\gamma_t \in Gal(K_s/K_r)$ se e somente se γ_t fixa o corpo K_r, e isto ocorre se e somente se γ_t fixa ξ_r e isto acontece se e somente se $t \equiv 1 \pmod{r}$ e isto completa a demonstração.

Lema 1.3.16 : Seja K um corpo abeliano de condutor n. Então $C_N(K) \subseteq C_I(K)$.

Demonstração : É claro que $C_N(K) \subseteq K$. Logo só falta provar que $C_N(K) \subseteq C_n$. Mas se $\gamma \in G_n$ então $\gamma(\varepsilon) \in C_n$, $\forall\ \varepsilon \in C_n$, ou seja γ é um automorfismo de C_n, portanto $N_{K_n/K}(\varepsilon) \in C_n$, $\forall\ \varepsilon \in C_n$ e o lema está provado.

CAPÍTULO 2

CARACTERES E UNIDADES CICLOTÔMICAS

O propósito deste capítulo é, inicialmente, demonstrar um resultado nosso sobre caracteres de Dirichlet (Teorema 2.1.7). Para tanto precisamos de alguns resultados intermediários, a maioria dos quais encontrados nas referências.

No parágrafo seguinte desenvolvemos alguns resultados do artigo de V. Ennola [10] para melhor usá-los no Capítulo 3.

No último parágrafo introduzimos as unidades circulares de um corpo abeliano K e provamos que os conceitos de unidades circulares definidos por Sinnott e Thaine, em [6] e [4], respectivamente, coincidem (Teorema 2.3.5).

2.1 CARACTERES

Definição 2.1.1: Um caracter é um homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$, onde G é um grupo abeliano finito.

Dado um grupo abeliano finito G, seja $G^\wedge$ o conjunto de todos os caracteres de G em $\mathbb{C}^*$. Em $G^\wedge$ definimos o produto natural, isto é, se χ_1, $\chi_2 \in G^\wedge$ então $\chi_1 . \chi_2$ será a função de G em $\mathbb{C}^*$ tal que $\chi_1 . \chi_2(g) = \chi_1(g) . \chi_2(g)$ para todo g em G.

Lema 2.1.2: Seja G um grupo abeliano finito. Então $G \cong G^\wedge$.

Demonstração : Inicialmente veremos que se G_1 e G_2 são dois grupos abelianos finitos então $G_1^\wedge \oplus G_2^\wedge \cong (G_1 \oplus G_2)^\wedge$. De fato, se $\chi_1 \in G_1^\wedge$ e $\chi_2 \in G_2^\wedge$ então a função $[\chi_1, \chi_2] : G_1 \oplus G_2 \longrightarrow \mathbb{C}^*$ tal que

$[\chi_1,\chi_2](a,b) = \chi_1(a).\chi_2(b)$ é um caracter de $G_1 \oplus G_2$. Por outro lado se χ é um caracter de $G_1 \oplus G_2$ então $\chi_i = \chi|_{G_i}: G_i \longrightarrow \mathbb{C}^*$, onde $\chi_1(a) = \chi(a,1)$ para todo $a \in G_1$ e $\chi_2(b) = \chi(1,b)$ para todo $b \in G_2$; são caracteres de G_1 e G_2, respectivamente e $\chi = [\chi_1,\chi_2]$. Agora é claro que a aplicação $G_1^\wedge \oplus G_2^\wedge \longrightarrow (G_1 \oplus G_2)^\wedge$ dada por $(\chi_1,\chi_2) \longrightarrow [\chi_1,\chi_2]$ é um isomorfismo.

Sendo G um grupo abeliano finito então G é isomorfo a uma soma direta de grupos cíclicos finitos e, após a observação feita acima, o lema se reduz ao caso em que G é um grupo finito cíclico. Se G é cíclico de ordem m e g é um gerador de G então todo caracter de G fica completamente determinado pelo seu valor em g. Seja χ um caracter de G em $\mathbb{C}^*$ tal que $\chi(g) = \xi_m$. É fácil ver que χ é um gerador de $G^\wedge$ e portanto o lema está provado.

Proposição 2.1.3 : Seja G um grupo abeliano finito. Então o par

$$\begin{array}{ccc} G \times G^\wedge & \longrightarrow & \mathbb{C}^* \\ (g,\chi) & \longmapsto & \chi(g) \end{array}$$

é não degenerado.

Demonstração : De fato se $\chi(g) = 1$ para todo $g \in G$ então χ é o caracter trivial. Por outro lado se $\chi(g) = 1$ para todo $\chi \in G^\wedge$ então podemos considerar os caracteres de G como sendo caracteres de $G/\langle g\rangle$. Assim sendo $\#(G/\langle g\rangle)^\wedge \geq \#(G^\wedge)$. Pelo Lema 2.1.2 segue que $\#(G^\wedge) \geq \#(G^\wedge)$ e isto só é possível se $\#(\langle g\rangle) = 1$, ou seja, g é o $\#(\langle g\rangle)$
elemento neutro de G e a proposição está demonstrada.

Lema 2.1.4 : Sejam G um grupo abeliano finito de ordem n e $G^\wedge$ o grupo dos caracteres de G. Então

i) $$\sum_{\chi \in G^\wedge} \chi(g) = \begin{cases} n & \text{se } g = 1_G \\ 0 & \text{caso contrário.} \end{cases}$$

ii) $\sum_{g\in G} \chi(g) = \begin{cases} n & \text{se } \chi = 1_{G^\wedge} \\ 0 & \text{caso contrário.} \end{cases}$

Demonstração:

i) Temos $\#(G) = \#(G^\wedge) = n$. Se $g = 1_G$ então $\chi(g) = 1$, $\forall \chi \in G^\wedge$ e portanto $\sum_{\chi \in G^\wedge} \chi(g) = n$. Se $g \neq 1_G$ então existe $\chi_r \in G^\wedge$ tal que $\chi_r(g) \neq 1$ (Proposição 2.1.3). Assim sendo, temos $\sum_{\chi \in G^\wedge} \chi(g) = \sum_{\chi \in G^\wedge} \chi_r.\chi(g) = \chi_r(g).\sum_{\chi \in G^\wedge} \chi(g)$, logo $(1-\chi_r(g)).\sum_{\chi \in G} \chi(g) = 0$. Mas $\chi_r(g) \neq 1$; portanto $\sum_{\chi \in G^\wedge} \chi(g) = 0$.

ii) Se $\chi \neq 1_{G^\wedge}$ então existe $g_1 \in G$ tal que $\chi(g_1) \neq 1$. Assim teremos $\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g_1.g) = \chi(g_1).\sum_{g \in G} \chi(g)$. Logo $(1-\chi(g_1)).\sum_{g \in G} \chi(g) = 0$, e o Lema 2.1.4 está provado.

A seguir demonstraremos um teorema que não encontramos na literatura.

Teorema 2.1.5: Sejam G um grupo abeliano finito de ordem n e $G^\wedge$ o grupo dos caracteres de G. Suponhamos $G = \langle g_1, g_2, \ldots, g_n \rangle$ e $G^\wedge = \langle \chi_1, \chi_2, \ldots, \chi_n \rangle$. Se M é a matriz $\left(\chi_i(g_j) \right)_{\substack{i=1,\ldots,n \\ j=1,\ldots,n}}$, então $\det M^2 = \pm n^n$.

Demonstração : Seja $\overline{M}$ a matriz $(\overline{\chi_i(g_j)}) = (\overline{\chi}_i(g_j))$, onde $\overline{\chi}_i$ é o caracter de G que a cada g_j associa o elemento $\overline{\chi_i(g_j)}$, o complexo conjugado de $\chi_i(g_j)$. De fato $\overline{\chi}_i$ é o caracter inverso de χ_i em $G^\wedge$.

Com isto a matriz $\bar{M}$ é obtida de M permutando-se algumas linhas entre si e portanto $\det \bar{M} = \pm \det M$. Por outro lado, $\det \bar{M} = \overline{\det M} = \pm \det M$, logo $\det M$ é um número real ou puramente imaginário. Agora $\det M^2 = \pm \det (M.\bar{M}) = \pm \det(M.\bar{M}^t)$ e a matriz $M.\bar{M}^t$ terá na posição (i,j) o elemento $\sum_{g \in G} \chi_i . \bar{\chi}_j(g)$. Pelo Lema 2.1.4 a matriz $M.\bar{M}^t$ terá entrada igual a n na diagonal principal e 0 nas demais posições e portanto o seu determinante é igual a n^n, ou seja, $\det M^2 = \pm n^n$ e o teorema está provado.

Sejam G um grupo abeliano finito, R um subgrupo de G e S um subgrupo de $G^\wedge$. Definimos o conjunto ortogonal de R (resp. de S), e denotamos por $R^\perp$ (resp. $S^\perp$), como sendo o conjunto

$(\chi \in G^\wedge ; \chi(r) = 1, \forall r \in R)$ (res. $(g \in G; \chi(g) = 1, \forall \chi \in S)$).

A seguir enunciaremos uma proposição cuja demonstração pode ser encontrada em [1], pg. 22.

Proposição 2.1.6 : Sejam G um grupo abeliano finito, R um subgrupo de G e S um subgrupo de $G^\wedge$. Então temos:

i) $R^\wedge \simeq G^\wedge / R^\perp$

ii) $S^\wedge \simeq G / S^\perp$.

Teorema 2.1.7 : Sejam G um grupo abeliano finito, H um subgrupo de $G^\wedge$ e X um conjnunto de representantes de G mod $H^\perp$, vamos assumir que $1 \in X$. Assim $G = \bigcup_{x \in X} x.H^\perp$. Sejam $c, a_g \in \mathbb{C}$, $g \in G$, $C(\chi) = \sum_{g \in G} \chi(g) a_g$, $\chi \in G^\wedge$. Então :

i) Para que $C(\chi) = c$ para todo $\chi \in H$ é necessário e suficiente

que $A_1 = c$ e $A_x = 0$, para todo $x \in X\setminus(1)$, onde $A_x = \sum_{g \in x.H^\perp} a_g$.

ii) Para que $C(\chi) = c$ para todo $\chi \in H$, $\chi \neq 1$, é necessário e suficiente que $A_1 = A_x + c$, para todo $x \in X\setminus(1)$, onde A_x é como no ítem anterior.

Demonstração : Inicialmente podemos constatar que os elementos A_x acima introduzidos só dependem das classes $x.H^\perp$ e não do particular sistema de representantes X escolhido.

Visto que a matriz $M = \left(\chi(g) \right)_{\substack{\chi \in G^\wedge \\ g \in G}}$ tem determinante não nulo (Teorema 2.1.5), qualquer matriz N constituída de r linhas distintas da matriz M terá o posto igual a r. Por outro lado a matriz N cujas linhas são $(\chi(g))_{g \in G}$, $\chi \in H$; além de ter posto igual a $\#(H)$, tem a seguinte propriedade: se $g, g' \in G$ e $g.H^\perp = g'.H^\perp$, então as colunas $(\chi(g))_{\chi \in H}$ e $(\chi(g'))_{\chi \in H}$ são iguais.

Assim sendo, o sistema

$\sum_{g \in G} \chi(g).a_g = c$, $\chi \in \tilde{H}$, será substituido por:

$$\sum_{x \in X} \chi(x).A_x = c \qquad \text{se } \tilde{H} = H \quad \text{e} \qquad (1)$$

$$\sum_{x \in X} \chi(x).A_x = c \qquad \text{se } \tilde{H} = H \setminus (1). \qquad (2)$$

No sistema (1) temos $\#(X) = \#(G/H^\perp) = \#(H)$ incógnitas e $\#(H)$ equações. O posto da matriz $N = \left(\chi(x) \right)_{\substack{x \in X \\ \chi \in H}}$ é igual a $\#(H)$ e e portanto $\det N \neq 0$, consequentemente, o sistema (1) tem uma única solução. Evidentemente se tomarmos $A_1 = c$ e $A_x = 0$, $\forall\, x \in X$, $x \neq 1$, teremos aí uma, e portanto a única, solução de (1) e isto resolve o

item (i) do teorema. No item (ii) temos que resolver o sistema (2). Pelo argumento acima descrito, o conjunto-solução do sistema (2) é um subespaço afim de dimensão 1. Mais uma vez podemos constatar que o conjunto proposto satisfaz as condições requeridas e portanto está demonstrado o Teorema 2.1.7.

Quando o grupo G abeliano finito é isomorfo a $(\mathbb{Z}/n.\mathbb{Z})^*$ para algum número inteiro positivo n dizemos que os caracteres de G são caracteres de Dirichlet definidos mod n, ou simplesmente caracter mod n.

Daqui para frente consideraremos apenas caracteres de Dirichlet.

Sejam n um número inteiro positivo e χ um caracter mod n. Se m é um múltiplo de n, então χ induz um caracter de $(\mathbb{Z}/m.\mathbb{Z})^*$ em $\mathbb{C}^*$, fazendo a composição com o homomorfismo natural $(\mathbb{Z}/m.\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n.\mathbb{Z})^*$. Costumamos denotar esta composição também por χ. Neste caso podemos considerar χ como sendo definido mod n ou mod m, pois ambos são, essencialmente, o mesmo homomorfismo.

Dado um caracter χ, definido modm m, é conveniente encontrar o menor inteiro positivo n, divisor de m, tal que $\chi(k) = 1$ para todo $k \in \mathrm{Ker}\left[(\mathbb{Z}/m.\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n.\mathbb{Z})^*\right]$, ou seja, procuramos o menor inteiro positivon, divisor de m, tal que se $(k,m) = 1$ e $k \equiv 1 \pmod{n}$ então $\chi(k) = 1$. Este menor inteiro, denotado por f_χ, será chamado condutor do caracter χ. É claro então, que f_χ é o menor inteiro positivo n tal que χ está definido mod n.

Dizemos que um caracter χ é par se $\chi(-1) = 1$ e ímpar se $\chi(-1) = -1$.

Dado um caracter $\chi : (\mathbb{Z}/n.\mathbb{Z})^* \longrightarrow \mathbb{C}^*$, podemos interpretar χ como sendo uma função de $M = \{k \in \mathbb{Z};\ (k,m) = 1\}$ em $\mathbb{C}^*$, onde $\chi(k) = \chi(\bar{k})$ para todo $k \in M$, onde $\bar{k}$ é a classe de k em $(\mathbb{Z}/n.\mathbb{Z})^*$. Neste

caso podemos estender χ de M para $\mathbb{Z}$, fazendo $\chi(a) = 0$ se $(a,n) > 1$.

Sejam χ um caracter definido mod n e f_χ o condutorn de χ. Se $f_\chi < n$ então a extensão de χ acima descrita poderá ser diferente quando consideramos χ definido mod n e quando consideramos χ definido mod f_χ. Para evitar esta possível ambiguidade, fica estabelecido neste texto que toda extensão de χ será feita a partir de χ definido mod f_χ.

Dizemos que um caracter χ definido mod n é primitivo se $n = f_\chi$.

Dados dois caracteres χ_1 e χ_2 definidos mod n_1 e mod n_2, respectivamente, podemos considerar χ_1 e χ_2 definidos mod $n_1.n_2$ e portanto fazer o produto $\chi_1.\chi_2$ definido mod $n_1.n_2$.

Lema 2.1.8 : (Exercício 3.1, pg. 27 de [1]) Sejam χ_1 e χ_2 dois caracteres de condutor f_{χ_1} e f_{χ_2}, respectivamente. Se $(f_{\chi_1}, f_{\chi_2}) = 1$ então $f_{\chi_1.\chi_2} = f_{\chi_1}.f_{\chi_2}$.

Demonstração : Temos que provar que o homomorfismo

$$\theta : \left(\mathbb{Z} / (f_{\chi_1}.f_{\chi_2}).\mathbb{Z} \right)^* \longrightarrow \mathbb{C}^*$$

definido por $\theta(a) = \chi_1(a).\chi_2(a)$ é um caracter primitivo. Mostraremos que é impossível reduzir o módulo de definição de θ. Seja p um número primo que divide $f_{\chi_1}.f_{\chi_2}$. Sem perda de generalidade podemos supor que p divide f_{χ_1}. Suponhamos que θ é definido mod k, onde $k = \left(f_{\chi_1}.f_{\chi_2} \right)/p$. Seja $a \equiv 1 \pmod{f_{\chi_1}/p}$ tal que $(a, f_{\chi_1}) = 1$ e $\chi(a) \neq 1$. Pelo Teorema Chinês do Resto existe um número inteiro b tal que $b \equiv a \pmod{f_{\chi_1}}$ e $b \equiv 1 \pmod{f_{\chi_2}}$. Neste caso $b \equiv 1 \pmod{k}$

e $(b, f_{\chi_1}.f_{\chi_2}) = 1$, logo $1 = \theta(b) = \chi_1(b).\chi_2(b) \neq 1$, o que é uma contradição.

Observação : Sejam $n > 1$ um número inteiro e χ um caracter definido mod n. Se n não é uma potência de primo, podemos escrever $n = a.b$, com $(a,b) = 1$ e $1 < a,b < n$. Visto que $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/a\mathbb{Z})^* \oplus (\mathbb{Z}/b\mathbb{Z})^*$, podemos escrever $\chi = \chi_a.\chi_b$, onde χ_a é a restrição de χ aos elementos da forma $(x,1)$ e χ_b é a restrição de χ aos elementos da forma $(1,y)$. Pelo Lema 2.1.8, temos $f_\chi = f_{\chi_a}.f_{\chi_b}$. Mais ainda, todo número inteiro primo com n se escreve na forma $a.r + b.s$, com $r,s \in \mathbb{Z}$, $(s,a) = (b,r) = 1$ e vice-versa, se $(b,r) = (a,s) = 1$ então $(a.r + b.s, n) = 1$. Assim sendo $\chi(a.r + b.s) = \chi_a(b.s).\chi_b(a.r)$.

2.2 RELAÇÕES ENTRE UNIDADES CICLOTÔMICAS

Sejam m um número inteiro positivo e $\varepsilon = \xi_m^t.\prod_{i=1}^{m-1}(1-\xi_m^i)^{a_i} \in K_m$; $a_1,\ldots a_{m-1} \in \mathbb{Z}$. Descrever os números inteiros a_i, acima , para os quais $\varepsilon = 1$ é um problema extremamente complexo e até algumas informações sobre os inteiros a_i ajudariam a resolver questões em aberto na teoria dos números.

Aos elementos de K_m da forma $\varepsilon = \pm\, \xi_m^t.\prod_{i=1}^{m-1}(1-\xi_m^i)^{a_i}$, $t, a_i \in \mathbb{Z}$ dá-se o nome de elementos ciclotômicos de K_m, e se ε, $\varepsilon^{-1} \in \mathbb{Z}[\xi_m]$ diz-se que ε é uma unidade ciclotômica de K_m.

É imediato ver que o conjunto de todas unidades ciclotômicas de K_m é um grupo o qual denotaremos por C_m; e é um resultado

conhecido a finitude do índice deste grupo no grupo de todas as unidades de K_m (ver [Q], Teorema 1).

Lema 2.2.1 : Sejam m um número inteiro positivo, $m = \prod_{i=1}^{s} q_i^{b_i}$ sua fatoração em números primos ($b_i > 0$) e ε um elemento ciclotômico. Então ε pode ser escrito na forma:

$$\varepsilon = \pm\xi_m^t \cdot \prod_{\vec{i} \in T} \left(1 - \xi_{q_1^{b_1}}^{i_1} \ldots \xi_{q_s^{b_s}}^{i_s} \right)^{A_{i_1,\ldots,i_s}} \qquad (2.1)$$

onde $\vec{i} = (i_1,\ldots,i_s)$, $T = T_1 \times \ldots \times T_s$ e

$$T_j = \left\{ i_j \in \left\{ 0,\ldots,q_j^{b_j} - 1 \right\} : (i_j, q_j) = 1 \text{ ou } i_j = 0 \right\}.$$

Demonstração : É claro que dado $n \in \mathbb{Z}$ existem $n_1,\ldots,n_s \in \mathbb{Z}$ tais que $\xi_m^n = \xi_{q_1'}^{n_1} \ldots \xi_{q_s'}^{n_s}$ onde $q_i' = q_i^{b_i}$, $i = 1,\ldots,s$.

Para demonstrar o Lema 2.2.1 é suficiente provar que todo elemento ciclotômico da forma $1-\xi_{q_1'}^{n_1} \ldots \xi_{q_s'}^{n_s}$, onde $q_i' = q_i^{b_i}$, $i = 1,\ldots,s$; é um produto cujos fatores são do tipo $1 - \xi_{q_1'}^{c_1} \ldots \xi_{q_s'}^{c_s}$, com $c_i \in \mathbb{N}$, $i = 1,\ldots,s$ e $(c_i,q_i') = 1$ ou $c_i = q_i'$; e isto pode ser visto por indução sobre s. Se cada n_i é primo com o respectivo q_i o problema está resolvido. Se algum n_i é múltiplo de $q_i^{b_i}$ então aplicamos a hipótese de indução. Agora suponhamos, sem perda de generalidade, que $n_1 = q_1^d.k$, onde $(k,q_1) = 1$ e $1 \leq d < b_1$.

Visto que $(1 - X^{q_1^d}) = \prod_{j=0}^{q_1^d-1} (1 - \xi_{q_1^d}^{j} .X)$, segue-se que

$$1 - \xi_{q_1'}^{n_1} \cdots \xi_{q_s'}^{n_s} = 1 - \left(\xi_{q_1'}^{k} \cdot \xi_{q_2'}^{q_1^{-d} \cdot n_2} \cdots \xi_{q_s'}^{q_1^{-d} \cdot n_s}\right)^{q_1^d} =$$

$$\prod_{j=0}^{q_1^d - 1} \left(1 - \xi_{q_1^d}^{j} \cdot \xi_{q_1'}^{k} \cdot \xi_{q_2'}^{q_1^{-d} \cdot n_2} \cdots \xi_{q_s'}^{q_1^{-d} \cdot n_s}\right) =$$

$$\prod_{j=0}^{q_1^d - 1} \left(1 - \xi_{q_1'}^{k + j \cdot q_1^{b_1 - d}} \cdot \xi_{q_2'}^{q_1^{-d} \cdot n_2} \cdots \xi_{q_s'}^{q_1^{-d} \cdot n_s}\right).$$

(Quando escrevemos $\xi_{q_i'}^{q_1^{-d} \cdot n_i}$ estamos nos referindo a $\xi_{q_i'}^{n_i' \cdot n_i}$, onde $n_i' \cdot q_1^d \equiv 1 \pmod{q_i^{b_i}}$). Visto que $(k + j \cdot q_i^{b_i - d} \cdot q_1) = 1$, para $j = 0, \ldots, q_1^{b_1 - d}$, podemos repetir o processo para os outros índices, se preciso for, e o lema está demonstrado.

Sejam $m > 1$ um número inteiro e p um número primo. Definimos $\gamma_p(m)$ como sendo o maior número inteiro tal que $p^{\gamma_p(m)}$ divide m.

Todo caracter χ aqui mencionado será sempre um caracter primitivo de condutor f_χ. A notação χ_b significa que f_χ divide b.

A seguir mostraremos alguns resultados de V. Ennola que serão usados somente no primeiro parágrafo do Capítulo 3.

Sejam $\lambda_x = \ln|1-\xi_m^x|$, $x = 1, \ldots, m-1$; W um $\mathbb{Z}$-módulo livre de posto $m-1$ e $R_1, \ldots, R_{m-1}$ uma base para W.

Sejam $R = \sum_{x=1}^{m-1} C_x \cdot R_x$, $C_x \in \mathbb{Z}$, um elemento qualquer de W e χ um caracter definido mod m, com condutor f_χ. Se d divide m, $d > 1$, e f_χ divide d, denotamos

$$T(\chi, d, R) = \sum_{\substack{x=1 \\ (x,d)=1}}^{d-1} \chi(x) \cdot C_{(m/d) \cdot x} \qquad (2.2)$$

e, caso $f_\chi > 1$, definimos

$$Y(\chi,R) = \sum_{d \mid m, f_\chi \mid d} \left(1/\phi(d)\right) . \prod_{\substack{q : \text{primo} \\ q \mid d}} . \left(1-\bar{\chi}(q)\right) . T(\chi,d,R). \qquad (2.3)$$

Para os primos q que dividem m definimos:

$$Y_q(R) = \sum_{x=1}^{q^\gamma - 1} (x,q^\gamma) . C_{(m/q^\gamma).x} \text{ , onde } \gamma = \gamma(m). \qquad (2.4)$$

Seja $\theta : W \longrightarrow \mathbb{R}$ o homomorfismo que leva R_x em λ_x, $x = 1,\ldots,m-1$.

Teorema 2.2.2 : Seja R um elemento de W. Então R está no núcleo de θ se e somente se:

i) $Y(\chi,R) = 0$ para todo caracter par não trivial χ.

ii) $Y_q(R) = 0$ para todo primo q que divide m.

A demonstração deste teorema plode ser encontrada em [10], pg. 28.

O homomorfismo θ acima citado indica, de fato, quando um elemeto ciclotômico tem valor absluto igual a 1 em $\mathbb{C}$.

Considerando os elementos ciclotômicos como sendo um subconjunto de $\mathbb{C}$, e se $\varepsilon \in \mathbb{C} \setminus \{0\}$ então $\varepsilon = 1$ se e somente se $|\varepsilon| = 1$ e o ângulo formado pelo vetor ε e o eixo positivo de X é um múltiplo inteiro de $2.\pi$, podemos descrever sob que condições um dado elemento ciclotômico $\varepsilon = \xi_m^t . \prod_{i=1}^{m-1} \left(1-\xi_m^i\right)^{a_i}$ é igual a 1.

Seja $\delta : \mathbb{C} \setminus \{0\} \longrightarrow \mathbb{R}$ o homomorfismo que a cada número complexo não nulo α associa o ângulo formado por α e o eixo positivo do X. Para simplificar a notação, quando escrevemos $\delta(\varepsilon) = t$ estamos nos referindo a $\delta(\varepsilon) \equiv t \pmod{2.\pi}$.

Lema 2.2.3 : Preservando a notação acima, se $\varepsilon = \xi_m^t . \prod \left(1-\xi_m^i\right)^{a_i}$

então $\delta(\varepsilon) = \frac{2.\pi.t}{m} + \pi.\sum_{i=1}^{m-1} a_i.\left(\frac{i}{m} - \frac{1}{2}\right)$.

Demonstração : Visto que δ é um homomorfismo, a prova do lema se resume em mostrar que $\delta(1 - \xi_m^k) = \pi.\left(\frac{k}{m} - \frac{1}{2}\right)$. De fato $\delta(\xi_m^k) = \frac{2.\pi.k}{m}$ e $\delta(-\xi_m^k) = \frac{2.\pi.k}{m} - \pi$, ver figura 1 abaixo

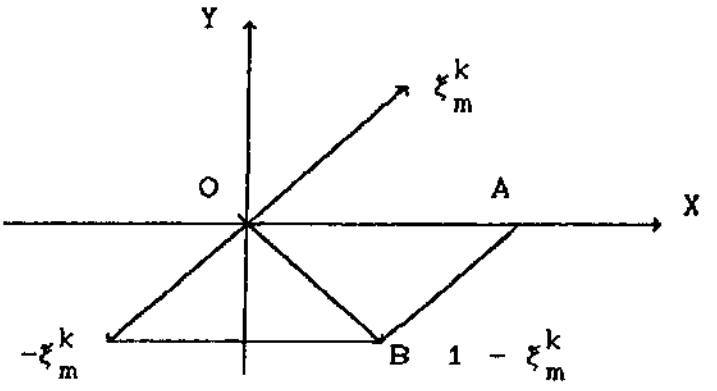


fig. 1

A figura 1 se obtém com $\overline{OA} = 1$ e o segmento BA paralelo ao segmento $O\xi_m^k$. Visto que $OAB(-\xi_m^k)$ forma um paralelogramo então o segmento OB divide o ângulo $AO(-\xi_m^k)$ ao meio e portanto $\delta(1 - \xi_m^k) = \frac{1}{2}\delta(-\xi_m^k) = \pi.\left(\frac{k}{m} - \frac{1}{2}\right)$.

Dado $\varepsilon = \xi_m^t.\prod_{i=1}^{m-1}\left(1-\xi_m^i\right)^{a_i} \in K_m$, seja $R = \sum_{i=1}^{m-1} a_i.R_i \in W$. Então $\theta(R) = \ln|\varepsilon|$. Com isto podemos definir as funções $Y(\chi,\_\,)$ e $Y_q(\_)$ sobre os elementos ciclotômicos do seguinte modo: dado um elemento ciclotômico $\varepsilon \in K_m$ existe um elemento $R \in W$ tal que $\theta(R) = \ln|\varepsilon|$.

Definimos $Y(\chi,\varepsilon)$ (respectivamente $Y_q(\varepsilon)$) como sendo $Y(\chi,R)$ respectivamente $Y_q(R)$). A verificação de que se pode definir as funções $Y(\chi,\_)$ e $Y_q(\_)$ sobre os elementos ciclotómicos se completa ao constatar-se que as funções acima são homomorfismos de W em $\mathbb{C}$.

Lema 2.2.4 : Sejam $\lambda = \sum_{\tau\in G_m} a_\tau.\tau \in \mathbb{Z}[G_m]$ e $\varepsilon \in C_m$. Então

$$Y(\varepsilon^\tau,\chi) = \left(\sum_{\tau\in G_m} a_\tau.\chi(\tau)\right).Y(\varepsilon,\chi) \qquad (2.5)$$

Demonstração : É evidente que podemos supor $\varepsilon = \prod_{i=1}^{m-1}\left(1-\xi_m^i\right)^{a_i}$; $a_i \in \mathbb{Z}$.

Visto que $Y(\_,\chi)$ é um homomorfismo de C_m em $\mathbb{C}$, só resta provar que $Y(\varepsilon^\tau,\chi) = \chi(\tau).Y(\varepsilon,\chi)$, onde $\chi(\tau) = \chi(r)$ com $\tau(\xi_m) = \xi_m^r$. De fato

$$\varepsilon^\tau = \prod_{i=1}^{m-1}\left(1-\xi_m^{i.r}\right)^{a_i} = \prod_{i=1}^{m-1}\left(1-\xi_m^{i}\right)^{b_i},\ b_{r.i} = a_i \text{ (subíndices mod m).}$$

Agora $T(\varepsilon^\tau,d,\chi) = \sum_{\substack{i=1\\(i,d)=1}}^{d-1}\chi(i).b_{(m/d).i} = \sum_{\substack{i=1\\(i,d)=1}}^{d-1}\chi(i).a_{(m/d).(r^{-1}.i)} =$

$\sum_{\substack{i=1\\(i,d)=1}}^{d-1}\chi(r.i).a_{(m/d).i} = \chi(r).T(\varepsilon,d,\chi)$. Logo

$$Y(\varepsilon^\tau,\chi) = \sum_{\substack{d\mid m\\ f_\chi\mid d}}\left(1/\phi(d)\right).\prod_{q\,:\,\text{primo}}(1-\bar{\chi}(q))\left(\chi(r).T(\varepsilon,d,\chi)\right) = \chi(r).Y(\varepsilon,\chi)$$

e o lema está provado.

Corolário 2.2.5 : Sejam m um número inteiro positivo e $\varepsilon \in V_m$. Suponhamos que m não seja uma potência de primo, digamos $m = a.b$, com $(a,b) = 1$ e $1 < a,b < m$. Se χ é um caracter definido mod m cujo condutor seja um divisor de a, então

$$Y(\varepsilon,\chi) = (1/\phi(m)).Y(N_{K_m/K_a}(\varepsilon),\chi) \qquad (2.6)$$

Demonstração : Visto que $[K_m : K_a] = \phi(b)$, pois $(a,b) = 1$, e $N_{K_m/K_a}(\varepsilon) = \prod_{\gamma\in G} \varepsilon^{\gamma}$, onde $G = Gal(K_m/K_a)$; só precisamos mostrar que $Y(\varepsilon^{\gamma},\chi) = Y(\varepsilon,\chi)$, para todo $\gamma \in G$. Mas γ fixa K_a e portanto podemos supor que $\gamma(\xi_m) = \xi_m^t$, com $t \equiv 1 \pmod a$ (Lema 1.3.15). Pelo Lema 2.2.4, temos $Y(\varepsilon^{\gamma}, \chi) = \chi(t).Y(\varepsilon,\chi)$. Visto que o condutor de χ é um divisor de a e $t \equiv 1 \pmod a$, deduzimos que $\chi(t) = 1$ e o corolário está provado.

2.3 UNIDADES CIRCULARES

Sejam K um corpo abeliano de condutor m e k_n a intersecção de K com K_n , $n \in \mathbb{N}$.

Para cada $n \in \mathbb{N}$, $n > 2$, e $a \in \{ 1,2,\ldots,n-1 \}$, denotaremos por $\alpha(n,a)$ a norma de K_n para k_n do elemento $1-\xi_n^a$, e U_n será o subgrupo de K_n^* gerado pelos elementos $1-\xi_n^a$, $a = 1,\ldots,n-1$.

Lema 2.3.1 : Sejam r e s dois números inteiros positivos. Se r divide s então $N_{K_s/K_r}(U_s) \subseteq U_r$.

Demonstração : A prova do Lema 2.3.1 resume-se em mostrar que $N_{K_s/K_r}(1-\xi_s^a) \in U_r$, $\forall$ a = 1,...,s-1. Basta supor o caso em que s = p.r, onde p é um número primo. Se p $\nmid$ r então existem inteiros x e y tais que p.x + r.y = 1. Logo $\xi_{p.r}^{a(p.x+r.y)} = \xi_r^{a.x}.\xi_p^{a.y}$ e portanto

$$N_{K_s/K_r}(1 - \xi_s^a) = N_{K_s/K_r}(1 - \xi_r^{a.x}.\xi_p^{a.y}) = \prod_{j=1}^{p-1}\left(1 - \xi_r^{a.x}.\left(\xi_p^{a.y}\right)^j\right) =$$

$$\frac{1-\xi_r^{p.a.x}}{1-\xi_r^{a.x}} \in U_r.$$

Por outro lado, se $p|r$, digamos $p^b||r$, então $Gal(K_s/K_r)$ tem ordem $\phi(s)/\phi(r) = p$ e, portanto, $Gal(K_s/K_r)$ é cíclico gerado por qualquer K_r-automorfismo diferente da identidade. É claro que o automordfismo τ_{r+1} de K_s que leva ξ_s em ξ_s^{r+1} é diferente da identidade e fixa K_r (Lema 1.3.15), logo um gerador de $Gal(K_s/K_r)$. Ora, $\tau_{r+1}(\xi_s) = \xi_s^{r+1} = \xi_{p.r}^{r+1} = \xi_{p.r}^{r}.\xi_{p.r} = \xi_p.\xi_{p.r}$. Logo $N_{K_s/K_r}(1-\xi_s^a) = \prod_{i=1}^{p}\tau_{r+1}^i(1-\xi_s^a) =$

$$\prod_{i=1}^{p}(1-\xi_p^{i.a}.\xi_{p.r}^a) = \begin{cases} (1-\xi_r^{a/p})^p & \text{se } a \equiv 0 \pmod p \\ (1-\xi_{p.r}^{p.a}) = (1-\xi_r^a) & \text{se } a \not\equiv 0 \pmod p. \end{cases}$$

Conclui-se pois que $N_{K_s/K_r}(1-\xi_s^a) \in U_r$ e o lema está provado.

O grupo das unidades circulares de K definido por Sinnott em [6] e aqui denotado por $C_S(K)$, é a intersecção de $\mathcal{O}_K^*$ com o subgrupo de K^* gerado por -1 e os elementos $\alpha(n,a)$, $n \in \mathbb{N}$, $n > 2$, e $a \in \{1,\ldots,n-1\}$.

Visto que $K_n \cap K_m = K_{(n,m)}$, $k_n = k_{(n,m)}$ (Teorema 1.3.7) e e $N_{K_n/K_{(n,m)}}(U_n) \subseteq U_{(n,m)}$ (Lema 2.3.1), deduzimos que na definição de $C_S(K)$ só precisamos considerar os números inteiros n que dividem m.

O grupo das unidades circulares de K, introduzido por Thaine e aqui denotado por $C_T(K)$, é definido como se segue: Se m é o

condutor de K e j é um número inteiro positivo, seja

$$C_j(X) = \left\{ f(X) = \pm \prod_{i=1}^{j} . \prod_{r=1}^{m-1} (X^i - \xi_m^r)^{a_{ir}} \ : \ a_{ir} \in \mathbb{Z},\ f(X) \in K(X) \text{ e } f(1) \in \mathfrak{O}_K^* \right\}$$

onde X é uma indeterminada, então

$$C_T(K) = \bigcup_{j=1}^{\infty} C_j(1).$$

Em [4] Thaine afirma que $C_T(K) \supseteq C_S(K)$ e externa seu interesse em saber quão maior do que $C_S(K)$ é $C_T(K)$. A meta deste parágrafo é mostrar que $C_S(K) = C_T(K)$ e uma demonstração resumida deste fato pode ser encontrada em [2].

Para cada número inteiro positivo n, múltiplo do condutor m de K, e j um inteiro positivo, escrevemos:

$$C_j(X,n) = \left\{ f(X) = \pm \prod_{i=1}^{j} \prod_{r=1}^{n-1} \left(X^i - \xi_n^r \right)^{a_{ir}} : \ a_{ir} \in \mathbb{Z}, f(X) \in K(X) \text{ e } f(1) \in \mathfrak{O}_K^* \right\},$$

onde X é uma indeterminada. Seja $C_j(1,n) = \left\{ f(1) : \ f(X) \in C_j(X,n) \right\}$.

É fácil ver que $C_j(1,n)$ é um grupo, qualquer que seja n múltiplo de m e j = 1,2,... Por outro lado $C_1(1,n) \subseteq C_2(1,n) \subseteq \ldots$ pois se $f(X) \in C_j(X,n)$, digamos $f(X) = \pm \prod_{i=1}^{j} \prod_{r=1}^{n-1} \left(X^i - \xi_n^r \right)^{a_{ir}}$, podemos considerar $f(X) = \pm \prod_{i=1}^{j+1} \prod_{r=1}^{n-1} \left(X^i - \xi_n^r \right)^{b_{ir}}$, com $b_{ir} = \begin{cases} a_{ir} & \text{se } i \leq j \\ 0 & \text{se } i = j+1. \end{cases}$

Com isto vemos que $C_j(X,n) \subseteq C_{j+1}(X,n)$ e, consequentemente, $C_j(1,n) \subseteq C_{j+1}(1,n)$. Como consequência imediata desta observação concluimos que $\bigcup_{j=1}^{\infty} C_j(1,n)$ é um grupo, o qual denotaremos por C(n), e que C(m) $= C_T(K)$.

Lema 2.3.2 : Com a notação acima tem-se:

i) $C_j(X,n) \leq C_1(X,t.n)$ para algum inteiro positivo t.

ii) $C_1(1,n) \leq C_1(1,t.n)$ para todo inteiro positivo t.

iii) $C = \bigcup_{t=1}^{\infty} C_1(1,t.m)$ é um grupo.

iv) $C_T(K) \leq C$.

Demonstração :

i) Se $f(X) \in C_j(X,n)$ então as raízes de f(X) são raízes dos polinômios $X^i - \xi_n^r$, $i=1,\ldots,j$ e $r=1,\ldots,n-1$; ou seja, se θ é uma raiz de f(X) então $\theta^i = \xi_n^r$ e portanto $\theta^{i.n} = 1$, $i = 1,\ldots,j$; logo as raízes de f(X) são raízes t.n-ésimas da unidade, onde $t = [1,\ldots,j]$ e portanto $f(X) = \pm\prod_{i=1}^{tn-1}(X-\xi_{t.n}^i)^{b_i} \in C_1(X,t.n)$.

ii) A inclusão $C_1(1,n) \leq C_1(1,t.n)$ decorre imediatamente do seguinte fato: Se $f(X) \in C_1(X,n)$ então $f(X) = \pm\prod_{i=1}^{n-1}\left(X-\xi_n^i\right)^{a_i} = \pm\prod_{i=1}^{tn-1}\left(X-\xi_{t.n}^i\right)^{b_i}$, onde $b_i = \begin{cases} a_{i/t} & \text{se } i \equiv 0 \pmod t \\ 0 & \text{caso contrário,} \end{cases}$

e portanto $f(X) \in C_1(X,t.n)$, ou seja, $f(1) \in C_1(1,t.n)$.

iii) Para mostrarmos que $C = \bigcup_{t=1}^{\infty} C_1(1,t.m)$ é um grupo é suficiente mostrar que dados dois elementos de C então o produto destes está em C. De fato, sejam $f(1)$, $g(1) \in C$, digamos $f(1) \in C_1(1,t_1.m)$ e $g(1) \in C_1(1,t_2.m)$; t_1, t_2 inteiros positivos. Desde que $C_1(1,t_1.m)$, $C_2(1,t_2.m) \leq C_1(1,t_1.t_2.m)$ (pelo ítem (ii)) e $C_1(1,t_1.t_2.m)$ é um grupo $f(1).g(1) \in C_1(1,t_1.t_2.m) \leq C$.

iv) Sabemos que $C_T(K) = C(m) = \bigcup_{j=1}^{\infty} C_j(1,m)$. Mas $C_j(1,m) \subseteq C_j(1,t.m)$ para algum t (ver item (i)), logo $\bigcup_{j=1}^{\infty} C_j(1,m) \subseteq \bigcup_{t=1}^{\infty} C_1(1,t.m) = C$, ou seja, $C_T(K) \subseteq C$ e a demonstração do lema está completa.

O próximo lema mostra como fatorar certos polinômios $f(X) \in K[X]$ em produtos que serão convenientes para os nossos propósitos.

Lema 2.3.3 : Se $f(X) = \prod_{i=1}^{m-1}\left(X-\xi_m^i\right)^{a_i} \in K[X]$ então $f(X) = \prod_{j \mid m} f_j(X)$, onde $f_j(X) = \prod_{\substack{i=1 \\ (i,m)=j}}^{m-1}\left(X-\xi_m^i\right)^{a_i} \in k_{m/j}[X]$.

Demonstração : É claro que podemos escrever $f(X) = \prod_{j \mid m} f_j(X)$, com $f_j(X) = \prod_{\substack{i=1 \\ (i,(m/j))=1}}^{(m/j)-1} \ldots \left(X-\xi_{m/j}^i\right)^{b_{ij}} \in K_{m/j}[X]$, pois sendo $(i,m) = j$, digamos $i = j.k$, $m = j.(m/j)$, com $(k,(m/j)) = 1$, teremos

$$f_j(X) = \prod_{\substack{k=1 \\ (k,(m/j))=1}}^{(m/j)-1}\left(X-\xi_m^{j.k}\right)^{a_{j.k}} = \prod_{\substack{k=1 \\ (k,(m/j))=1}}^{(m/j)-1}\left(X-\xi_{m/j}^{k}\right)^{a_{j.k}}$$

e aí fazemos $b_{ij} = a_{j.i}$, $(i,(m/j)) = 1$. É evidente que $f_j(X) \in K_{m/j}[X]$. Para finalizar falta mostrar que $f_j(X) \in K[X]$, isto é, $f_j^{\gamma}(X) = f_j(X)$ para todo $\gamma \in G = Gal(K_m/K)$ (onde γ age sobre os coeficientes dos polinômios). De fato $f^{\gamma}(X) = f(X)$ pois $f(X) \in K[X]$ e γ fixa K. Logo se $\gamma(\xi_m) = \xi_m^c$, devemos ter $a_i = a_{i.c}$ (subíndices mod m), pois $\prod_{i=1}^{m-1}\left(X-\xi_m^i\right)^{a_i} = \prod_{i=1}^{m-1}\left(X-\xi_m^i\right)^{b_i}$ se e somente se $a_i = b_i$, $i=1,\ldots,m-1$. Com

isto, se $(i,m) = j$, então $(X-\xi_m^i)^{a_i}$ divide $f_j(X)$, logo $(1-\xi_m^{i.c})^{a_i}$ também divide $f_j(X)$, pois $(i.c, m) = (i,m) = j$. Portanto $f_j^{\gamma}(X)$ divide $f_j(X)$. Como são polinômios mônicos e do mesmo grau, segue que $f_j^{\gamma}(X) = f_j(X)$ e, consequentemente, $f_j(X) \in K[X]$, o que completa a demonstração do Lema 2.3.3.

Lema 2.3.4 : Sejam n um número inteiro positivo, L um subcorpo de K_n e $G' = Gal(K_n/L)$. Seja $\langle \theta_1, \ldots, \theta_s \rangle$ um conjunto de representantes das classes de G_n/G'. Então:

i) Os polinômios $g_i(X) = \prod_{\gamma \in G'} \left(X-\xi_n^{\theta_i \cdot \gamma}\right)$ pertencem a $L[X]$ e são irredutíveis em L, i=1...s.

ii) $g_i(1) = N_{K_n/L}(1-\xi_n^{\theta_i})$, i=1,...,s.

iii) O grupo multiplicativo

$$S = \{ g(X) = \prod_{i=1}^{n-1} (X-\xi_n^i)^{a_i} : a_i \in \mathbb{Z} \text{ e } g(X) \in L(X) \}$$

é um $\mathbb{Z}$-módulo livre de posto $[L:\mathbb{Q}]$ e gerado por $\langle g_i(X), i=1,\ldots,s \rangle$.

Demonstração :

i) Podemos ver que se $\alpha \in G'$ então $g_i^{\alpha}(x) = \prod_{\delta \in G'} \left(X-\xi_n^{\alpha.\delta.\theta_i}\right) =$

$\prod_{\delta \in G'} \left(X-\xi_n^{\alpha.\theta_i}\right) = g_i(X)$ e portanto $g_i(X) \in L[X]$. Seja $h(X)$ um fator irredutível de $g_i(X)$ em $L[X]$ e $X-\xi_n^{\alpha.\theta_i}$ um fator de $h(X)$ em $K_n[X]$, então $h(X) = (X-\xi_n^{\alpha.\theta_i}).v(X)$, $v(X) \in K_n(X)$. Seja $\mu \in G'$; visto

que $h(X) \in L[X]$ então $h^{\mu}(X) = h(X) = (X-\xi_n^{\mu.\alpha.\theta_i}).v^{\mu}(X)$ e portanto $(X-\xi_n^{\mu.\alpha.\theta_i})$ divide $h(X)$ para todo $\mu \in G'$ e consequentemente $g_i(X) = \prod_{\mu \in G'} \left(X-\xi_n^{\mu.\alpha.\theta_i}\right)$ divide $h(X)$ pois os monômios $X-\xi_n^{\mu.\alpha.\theta_i}$, que são todos distintos, dividem $h(X)$. Ora, $h(X)$ é um fator irredutível de $g_i(X)$ em $L[X]$ e $g_i(X)$ divide $h(X)$, então $g_i(X)$ e $h(X)$ diferem por uma unidade de L e portanto $g_i(X)$ é irredutível.

ii) Decorre imediatemente da definição de $g_i(X)$.

iii) Seja $g(X) \in S$. Podemos supor, sem perda de generalidade, que $g(X) \in L[X]$; então $g(X)$ pode ser escrito na forma:

$$g(X) = \prod_{\substack{i=1 \\ \mu \in G'}}^{s} \left(X-\xi_n^{\mu.\theta_i}\right)^{a_{i\mu}}, \qquad (2.7)$$

onde $a_{i\mu}$ são números inteiros não negativos. Desde que $g(X) \in L[X]$, segue-se que $g^{\alpha}(X) = g(X)$ para todo $\alpha \in G'$ e portanto o expoente de $X-\xi_n^{\mu.\theta_i}$ é o mesmo expoente de $X-\xi_n^{\mu.\alpha.\theta_i}$ na equação (2.7), ou seja, $a_{i\mu} = a_{i(\mu.\alpha)}$, $\forall\ \alpha,\mu \in G'$, isto é, $a_{i\mu}$ só depende de i e portanto $g(X) = \prod_{\mu \in G'} \left[\prod_{i=1}^{s}\left(X-\xi_n^{\mu.\theta_i}\right)\right]^{a_i\mu} = \prod_{i=1}^{s} g_i(X)^{a_i}$, onde $a_i = a_{i\mu}$, $\forall\ \mu \in G'$. Quanto ao posto de S decorre do fato de s ser o índice de G' em G e portanto o grau de L sobre $\mathbb{Q}$ e o lema está provado.

Com estes resultados, podemos responder a questão proposta por Thaine em [4], pg 1.

Teorema 2.3.5 : Sejam K um corpo abeliano de condutor m, $C_S(K)$ e

$C_T(K)$ as unidades circulares de K definidas por Sinnott e Thaine, respectivamente. Então $C_S(K) = C_T(K)$.

Demonstração : Primeiramente vamos mostrar que $C_S(K) \subseteq C_1(1)$. Seja $\delta \in C_S(K)$. Então $\delta = \prod_{n|m} \delta_n$, onde $\delta_n = \prod_{a=1}^{n-1} \alpha(n,a)^{b_{n,a}}$. Sejam $f_{n,a}(X) = \prod_{\mu \in G'_n} (X - \xi_n^{a\mu})$, onde $G'_n = Gal(K_n/K)$, $f_n(X) = \prod f_{n,a}^{b_{n,a}}(X)$ e $F(X) = \prod_{n|m} f_n(X)$. É claro que $f_{n,a}(X) \in K[X]$ e $f_{n,a}(1) = \alpha(n,a)$. Logo $f_n(1) = \delta_n$ e $F(1) = \delta$. Sendo $F(X) = \prod_{n|m} f_n(X)$ podemos escrever $F(X) = \prod_{i=1}^{m-1} (X - \xi_m^i)^{a_i}$, com $F(X) \in K(X)$, (pois cada $f_{n,a}(X) \in K(X)$) e $F(1) \in \mathcal{O}_K^*$, ou seja, $\delta = F(1) \in C_1(1)$.

Agora mostraremos que $C \subseteq C_S(K)$. Seja $\delta \in C$. Então $\delta \in C_1(1,n)$ para algum múltiplo n de m e seja $f(X) = \prod_{i=1}^{n-1} (X - \xi_n^i)^{a_i} \in K(X)$ tal que $f(1) = \delta$. Pelo Lema 2.3.3, $f(X) = \prod_{j|n} f_j(X)$, com $f_j(X) \in k_{n/j}(X)$. Agora, segue do Lema 2.3.4, que para cada divisor j de n existem polinômios $g_{ij}(X) \in k_{n/j}[X]$ tais que $f_j(X) = \prod_i g_{ij}(X)^{b_{ij}}$ e $g_{ij}(1) = N_{K_{(n/j)}/k_{(n/j)}}\left(1 - \xi_{n/j}^i\right)$. Então $f_j(1) = \prod_i N_{K_{(n/j)}/k_{(n/j)}}\left(1 - \xi_{n/j}^i\right)^{b_{ij}}$ e portanto $f(1) = \prod_{j|n} f_j(1) \in C_S(K)$. No Lema 2.3.2 (iv) provamos que $C_T(K) \subseteq C$ e pelo que acabamos de demonstrar deduzimos que $C_T(K) \subseteq C_S(K)$. Visto que $C_T(K) \supseteq C_1(1) \supseteq C_S(K)$ a igualdade segue e o teorema está provado.

Corolário 2.3.6 : Os grupos $C_j(1)$ definidos por Thaine em [4] são todos iguais entre si, consequentemente $C_T(K) = C_1(1)$.

Demonstração : Segue imediatamente da definição de $C_T(K) = \bigcup_{j=1}^{\infty} C_j(1)$, uma vez que, pelo Teorema 2.3.5, $C_T(K) \leq C_1(K)$.

UNIDADES ESPECIAIS

Sejam K um corpo de números abeliano, n o seu condutor, p um primo racional que se decompõe completamente em K e L = K.K_p^+. Seja $u \in \mathfrak{O}_L^*$ tal que $N_{L/K}(u) = 1$. Pelo Teorema 90 de Hilbert, existe $\alpha \in L$, $\alpha \neq 0$, tal que $u = \alpha^{\tau-1}$, onde τ é um gerador de $Gal(L/K) \simeq (\mathbb{Z}/p\mathbb{Z})^*/(\pm 1)$.

Seja $(\alpha) = \mathfrak{q}_1^{a_1} \ldots \mathfrak{q}_s^{a_s}$ a fatoração do ideal principal $\alpha\mathfrak{O}_L$ em ideais primos de $\mathfrak{O}_L$. De $u = \alpha^{\tau-1}$, com $u \in \mathfrak{O}_L^*$, segue que $(\alpha) = (\alpha)^\tau$. Se $\mathfrak{m}$ é um ideal primo de K que não se ramifica em L e $\tilde{\mathfrak{m}}$ é um ideal primo de L acima de $\mathfrak{m}$, que aparece na fatoração do ideal $\alpha\mathfrak{O}_L$, então $\tilde{\mathfrak{m}}^{\tau^i}$, $i = 1, \ldots, (p-1)/2$; são todos os ideais primos de L acima de $\mathfrak{m}$ e todos aparecem na fatoração de $\alpha\mathfrak{O}_L$ com o mesmo expoente, digamos $w \in \mathbb{Z}$. Visto que $\mathfrak{m}$ não se ramifica em L, segue que $\alpha\mathfrak{O}_L = \mathfrak{m}^w.\mathfrak{n}$, onde $\mathfrak{n}$ é um ideal de $\mathfrak{O}_L$, não necessariamente principal e $\nu_{\tilde{\mathfrak{m}}}(\mathfrak{n}) = 0$. Aplicando o mesmo procedimento para o ideal $\mathfrak{n}$, pois $\mathfrak{n}^{1-\tau} = (1)$, e e assim por diante, concluimos que $\alpha\mathfrak{O}_L = \mathfrak{A}.\mathfrak{B}$, onde $\mathfrak{A}$ é o levantamento de um ideal de K e $\mathfrak{B}$ é um ideal de L em cuja fatoração só aparecem ideais primos de L que estão acima de ideais primos de K que se ramificam em L. Mas os ideais primos de K que se ramificam em L estão acima de primos ideais de $\mathbb{Q}$ que se ramificam em K_p^+, e só

primo p se ramifica em K_p^+, logo, somente os ideais primos de K acima de p se ramificam em L. Sejam $\Delta = Gal(K/\mathbb{Q})$ e Q um ideal primo de K acima de p. Visto que p se ramifica completamente em K_p^+ então assim se comporta Q em L e portanto existe um único ideal primo de L, digamos B, acima de Q.

Desde que podemos identificar $Gal(L/K_p^+)$ com Δ, então B^γ (resp. Q^γ), $\gamma \in \Delta$, são os únicos ideais primos de L (resp. K) acima de p. Além disto B^γ é o único ideal primo de L acima de Q^γ.

Visto isso temos:

$$\alpha\mathfrak{O}_L = \mathfrak{A}.\prod_{\gamma\in\Delta}\gamma^{-1}(B)^{r_\gamma} \qquad r_\gamma \in \mathbb{Z},\ \gamma \in \Delta. \tag{3.1}$$

Aplicando a norma de ideais nesta equação, temos:

$$N_{L/K}(\alpha)\mathfrak{O}_K = \mathfrak{A}^{(p-1)/2}.\prod_{\gamma\in\Delta}\gamma^{-1}(Q)^{r_\gamma}. \tag{3.2}$$

Com isto, se, por exemplo, $p \equiv 1 \pmod{2.h_K}$, onde h_K é o número das classes do corpo K, então $\sum_{\gamma\in\Delta} r_\gamma.\gamma^{-1}$ é um anulador para o elemento do grupo das classes de K representado por Q.

O único ideal primo de K_p^+ acima de p é $(1-\xi_p)(1-\xi_p^{-1})\mathfrak{O}_{K_p^+}$ e este se decompõe completamente em L, ou seja

$$\prod_{\gamma\in\Delta} B^\gamma = (1-\xi_p)(1-\xi_p^{-1})\mathfrak{O}_L. \tag{3.3}$$

Seja $\delta = \alpha/\left((1-\xi_p)(1-\xi_p^{-1})\right)^{r_\gamma} \in L$. Por (3.2) e (3.3), a valorização $\gamma^{-1}(B)$-ádica aplicada em δ é nula e portanto podemos escrever $\delta = \lambda/\mu$, $\lambda, \mu \in \mathfrak{O}_L$ tais que a valorização $\gamma^{-1}(B)$-ádica

de λ e μ é nula (ver [4], pg. 6).

Por (3.3) temos $2-(\xi_p+\xi_p^{-1}) \in B^{\gamma}$, $\forall\ \gamma \in \Delta$ e portanto

$$\xi_p+\xi_p^{-1} \equiv 2 \pmod{B^{\gamma}} \quad \forall\ \gamma \in \Delta. \tag{3.4}$$

Seja s uma raiz primitiva mod p, tal que $\tau(\xi_p+\xi_p^{-1}) = \xi_p^{s}+\xi_p^{-s}$.

Como

$$\xi_p^{s} + \xi_p^{-s} \equiv \xi_p + \xi_p^{-1} \pmod{(1-\xi_p)(1-\xi_p^{-1}).\mathfrak{D}_L}, \tag{3.5}$$

temos, para todo $\gamma \in \Delta$, a congruência

$$\tau(\xi_p+\xi_p^{-1}) \equiv \xi_p+\xi_p^{-1} \pmod{B^{\gamma}} \tag{3.6}$$

e, consequentemente, $\tau(\lambda) \equiv \lambda \not\equiv 0 \pmod{\gamma^{-1}(B)}$ e $\tau(\mu) \equiv \mu \not\equiv 0 \pmod{\gamma^{-1}(B)}$. Logo $\tau(\delta) \equiv \delta \pmod{\gamma^{-1}(B)}$ e portanto temos:

$$\delta = \frac{\alpha}{[(1-\xi_p)(1-\xi_p^{-1})]^{r_{\gamma}}} \equiv \tau(\delta) = \frac{\alpha.u}{[(1-\xi_p^{s})(1-\xi_p^{-s})]^{r_{\gamma}}} \not\equiv 0 \pmod{\gamma^{-1}(B)}.$$

Mas

$$\left(1-\xi_p^{s}\right)\left(1-\xi_p^{-s}\right)/\left(1-\xi_p\right)\left(1-\xi_p^{-1}\right) = \left(1+\xi_p+\ldots+\xi_p^{s-1}\right)\left(1+\xi_p^{-1}+\ldots+\xi_p^{-(s-1)}\right)$$

$$= s + (\xi_p + \xi_p^{-1})(s-1) + \ldots + (\xi_p^{s-1} + \xi_p^{-(s-1)})(s-(s-1)).$$

Mas $\xi_p^{i} + \xi_p^{-i} \equiv 2 \pmod{B^{\gamma}}$ $\forall\ \gamma \in \Delta$, logo

$$\left((1-\xi_p)(1-\xi_p^{-1})\right)^{\tau-1} \equiv s + 2.[(s-1) + \ldots + 1\ ] = s^2 \pmod{B^{\gamma}},\ \forall\ \gamma \in \Delta.$$

Ou seja,

$$\frac{\alpha . S^{2r_\gamma}}{[(1-\xi_p)(1-\xi_p^{-1})]^{r_\gamma}} \equiv \frac{\alpha . u}{[(1-\xi_p)(1-\xi_p^{-1})]^{r_\gamma}} \pmod{\gamma^{-1}(B)}.$$

Logo,

$$\frac{\alpha}{[(1-\xi_p)(1-\xi_p^{-1})]^{r_\gamma}} \cdot \left(u - S^{2r_\gamma}\right) \equiv 0 \pmod{\gamma^{-1}(B)},$$

e portanto

$$u \equiv S^{2r_\gamma} \pmod{\gamma^{-1}(B)}, \ \forall\ \gamma \in \Delta, \qquad (3.7)$$

pois $\dfrac{\alpha}{[(1-\xi_p)(1-\xi_p^{-1})]^{r_\gamma}} \not\equiv 0 \pmod{\gamma^{-1}(B)}$.

Suponhamos que $\varepsilon \in \mathfrak{O}_K^*$ é tal que $\varepsilon^2 \equiv u \pmod{(1-\xi_p)(1-\xi_p^{-1}).\mathfrak{O}_L}$.

Por (3.7) temos $\varepsilon^2 \equiv S^{2r_\gamma} \pmod{\gamma^{-1}(Q)}$, pois ε, $S \in K$, e portanto

$$S^{2r_\gamma} \equiv \gamma(\varepsilon)^2 \pmod{Q}, \text{ para todo } \gamma \in \Delta. \qquad (3.8)$$

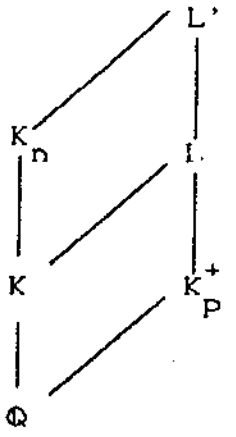
Estas congruências nos permitem obter informações sobre os coeficientes do anulador $\sum_{\gamma\in\Delta} r_\gamma . \gamma^{-1}$ da classe de ideais representada por Q e, em casos importantes, estas congruências nos levam a obter anuladores de todo o grupo das classes.

Após estas considerações torna-se evidente a importância das unidades ε de K tais que $\varepsilon^2 \equiv u \pmod{(1-\xi_p)(1-\xi_p^{-1}).\mathfrak{O}_L}$, para alguma unidade u de L tal que $N_{L/K}(u) = 1$.

3.1 UNIDADES ESPECIAIS, SEGUNDO RUBIN

Neste parágrado K denotará um corpo abeliano de condutor n e se p é um primo racional, L_p e L'_p denotarão os corpos $K.K_p^+$ e $K_n.K_p^+$, respectivamente. Quando o primo p é fixado denotaremos L_p e L'_p por L e L', respectivamente.

Temos assim, o seguinte diagrama:



Sejam $\Gamma_p = \left\{ u \in \mathcal{O}_L^* : \ N_{L/K}(u) = 1 \right\}$ e

$\mathcal{C}_p = \left\{ \varepsilon \in \mathcal{O}_K^*; \text{ existe } u \in \Gamma_p \text{ tal que } \varepsilon^2 \equiv u \pmod{\mathfrak{p}} \right\}$, onde $\mathfrak{p}$ é o produto de todos os ideais primos de L acima de p.

Definição 3.1.1 : Sejam K um corpo abeliano e ε uma unidade de K. Dizemos que ε é uma unidade especial de K se $\varepsilon \in \mathcal{C}_p$ para quase todo primo p que se decompõe completamente em K. (onde "para quase todo" significa para todo, exceto para um número finito).

O conjunto de todas as unidades especiais de K é um grupo que será aqui denotado por S(K).

Visto que p se ramifica completamente em K_p^+, se p se decompõe completamente em K então o ideal $\mathfrak{p}$ é principal e gerado por

$(1-\xi_p)(1-\xi_p^{-1})$. Neste caso temos a seguinte congruência:

$$\xi_p+\xi_p^{-1} \equiv 2 \pmod{\mathfrak{p}}. \qquad (3.9)$$

Donde:

$$\xi_p+\xi_p^{-1} \equiv 2 \pmod{(1-\xi_p)(1-\xi_p^{-1})\mathfrak{O}_{L'}}. \qquad (3.10)$$

Teorema 3.1.2 : Seja K um corpo abeliano. Então $C_N(K) \leq S(K)$.

Demonstração : Sejam n o condutor de K e $\varepsilon = \xi_n^t \cdot \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{a_i}$ uma unidade ciclotômica de K_n. Devemos mostrar que para quase todo primo racional p que se decompõe completamente em K existe $u \in \mathcal{O}_p$ tal que $N_{L/K}(\varepsilon) \equiv u \pmod{\mathfrak{p}}$. Sejam

$$v = \xi_n^{2t} \cdot \prod_{i=1}^{n-1}\left\{\left(1-\xi_n^i \cdot \xi_p\right)\left(1-\xi_n^i \cdot \xi_p^{-1}\right)\right\}^{a_i} \text{ e } u = N_{L'/L}(v).$$

Visto que $\left(1-\xi_p^i\right)\left(1-\xi_p^{-i}\right)/\left(1-\xi_p\right)\left(1-\xi_p^{-1}\right)$ é uma unidade de L, i = $1,\ldots,(p-1)/2$; segue que $\mathfrak{p} = (1-\xi_p^i)(1-\xi_p^{-i})\mathfrak{O}_{L'}$; $i = 1,\ldots,(p-1)/2$. Ora, da congruência (3.10) segue que $\varepsilon^2 \equiv u \pmod{(1-\xi_p)(1-\xi_p^{-1})\mathfrak{O}_{L'}}$, logo $\varepsilon^2 - u = (1-\xi_p)(1-\xi_p^{-1}).x$, $x \in \mathfrak{O}_{L'}$. Para qualquer $\tau \in Gal(L'/L)$ $\varepsilon^{2\tau} - u^\tau = (1-\xi_p)(1-\xi_p^{-1}).x^\tau$, pois τ fixa K_p^+. Assim sendo, $\varepsilon^{2\tau} \equiv u^\tau$ $\pmod{(1-\xi_p)(1-\xi_p^{-1})\mathfrak{O}_{L'}}$ e portanto

$$N_{L'/L}(\varepsilon^2) \equiv N_{L'/L}(v) \left[\mathrm{mod}\ (1-\xi_p)(1-\xi_p^{-1})\mathfrak{O}_{L'}\right].$$

Neste caso $N_{L'/L}(\varepsilon^2) - u = (1-\xi_p)(1-\xi_p^{-1}).y$, para algum $y \in \mathfrak{O}_{L'}$. Visto que $(1-\xi_p)(1-\xi_p^{-1}) \in \mathfrak{O}_{L'}$, segue $y \in \mathfrak{O}_{L'}$ e portanto $N_{L'/L}(\varepsilon^2) \equiv$ $u \pmod{\mathfrak{p}}$. Para finalizar falta mostrar que $u \in \mathcal{O}_p$. Identificando

Gal(L/K) com Gal($K_p^+/\mathbb{Q}$), temos:

$$N_{L/K}(u) = N_{L/K}\left(N_{L'/L}(v)\right) = N_{L'/K}(v) = N_{K_n/K}\left(N_{L'/K_n}(v)\right) =$$

$$N_{K_n/K}\left(\xi_n^{2t(p-1)/2} \cdot \prod_{i=1}^{n-1} \cdot \prod_{j=1}^{(p-1)/2} \left[(1-\xi_n^i \cdot \xi_p^j)(1-\xi_n^i \cdot \xi_p^{-j})\right]^{a_i}\right) =$$

$$N_{K_n/K}\left(\xi_n^{t(p-1)} \cdot \prod_{i=1}^{n-1} \cdot \prod_{j=1}^{p-1}\left(1-\xi_n^i \xi_p^j\right)\right) = N_{K_n/K}\left\{\xi_n^{t(p-1)} \cdot \prod_{i=1}^{n-1}\left(\frac{1-\xi_n^{pi}}{1-\xi_n^i}\right)^{a_i}\right\} =$$

$\left(N_{K_n/K}(\varepsilon)\right)^{\tau_p - 1}$, onde τ_p é o automorfismo de Frobenius para o primo p. Como p se docompõe completamente em K, então τ_p é a indentidade quando restrito a K. Mas $N_{K_n/K}(\varepsilon) \in K$ e portanto $N_{L/K}(u) = 1$ e o teorema está demonstrado.

Corolário 3.1.3: (Teorema 2.1 de [7]) Se $K = K_n^+$ então $C_N(K) \subseteq S(K)$.

Teorema 3.1.4 : Seja n um número inteiro positivo. Se $K = K_n^+$ então $C_J(K) \subseteq S(K)$.

Demonstração : Sejam p um primo racional que se decompõe completamente em K_n^+ e $\tilde{\mathfrak{p}} = (1-\xi_p)(1-\xi_p^{-1})\mathfrak{O}_{L'}$. Dado $\varepsilon = \pm\xi_n^t \cdot \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{a_i}$ $\in K_n^+$, seja $u = u(\varepsilon) = \xi_n^{2t} \cdot \prod_{i=1}^{n-1}\left[\left(1-\xi_n^i \cdot \xi_p\right)\left(1-\xi_n^i \cdot \xi_p^{-1}\right)\right]^{a_i}$. Visto que $(1-\xi_n^i)^2 \equiv (1-\xi_n^i \cdot \xi_p)\cdot(1-\xi_n^i \cdot \xi_p^{-1}) \pmod{\tilde{\mathfrak{p}}}$, então $\varepsilon^2 \equiv u \pmod{\tilde{\mathfrak{p}}}$. De $\varepsilon \in K_n^+$ tem-se $\varepsilon = \bar{\varepsilon}$, onde a barra significa a conjugação complexa, e isto equivale a $\pm \xi_n^t \cdot \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{a_i} = \pm \xi_n^{-t} \cdot \prod_{i=1}^{n-1}\left(1-\xi_n^{-i}\right)^{a_i}$. Mas

$(1-\xi_n^{-i})^{a_i} = (-1)^{a_i}.\xi_n^{-i.a_i}.(1-\xi_n^{i})^{a_i}$, logo $\xi_n^{t}.\prod_{i=1}^{n-1}\left(1-\xi_n^{i}\right)^{a_i} =$

$\xi_n^{-t}.\left[(-1)^{\sum_{i=1}^{n-1}a_i}.\xi_n^{-\sum_{i=1}^{n-1}i.a_i}.\prod_{i=1}^{n-1}\left(1-\xi_n^{i}\right)^{a_i}\right]$, ou seja, $\varepsilon = \bar{\varepsilon}$ se e somente se $\xi_n^{a} = (-1)^{b}$, onde $a = 2.t + \sum_{i=1}^{n-1} i.a_i$ e $b = \sum_{i=1}^{n-1} a_i$ e, portanto, $4.t + 2.\sum_{i=1}^{n-1} i.a_i \equiv 0 \pmod{n}$. Para que $u \in L$ é necessário e suficiente que $u = \bar{u}$, pois a identidade e a conjugação complexa formam o grupo de Galois de L' sobre L. Como no caso de ε, $u = \bar{u}$ se e somente se $4.t + 2.\sum_{i=1}^{n-1} i.a_i \equiv 0 \pmod{n}$, ou seja, se $\varepsilon \in K$, então $u \in L$. Para finalizar devemos mostrar que $N_{L/K}(u) = 1$. Ora, $L \cap K_n = K_n^{+}$, logo $Gal(L/K_n^{+}) \simeq Gal(L'/K_n)$ e $N_{L/K}(u) = N_{L'/K_n}(u) = \xi_n^{2.t.(p-1)/2}.\prod_{i=1}^{n-1} N_{L/K}\left[\left(1-\xi_n^{i}.\xi_p\right).\left(1-\xi_n^{i}.\xi_p^{-1}\right)\right]^{a_i}$. Mas

$N_{L'/K_n}\left[\left(1-\xi_n^{i}.\xi_p\right).\left(1-\xi_n^{i}.\xi_p^{-1}\right)\right]^{a_i} = \prod_{j=1}^{(p-1)/2}\left[\left(1-\xi_n^{i}.\xi_p^{j}\right)\left(1-\xi_n^{i}.\xi_p^{-j}\right)\right]^{a_i}$,

pois $Gal(L/K_n) \simeq Gal(K_p^{+}/\mathbb{Q})$. Visto que

$\prod_{j=1}^{(p-1)/2}\left[\left(1-\xi_n^{i}.\xi_p^{j}\right)\left(1-\xi_n^{i}.\xi_p^{-j}\right)\right] = \left(1-\xi_n^{p.i}\right)/\left(1-\xi_n^{i}\right)$, temos: $N_{L'/K_n}(u) =$

$\xi_n^{t(p-1)}.\prod_{i=1}^{n-1}\left[\left(1-\xi_n^{pi}\right)/\left(1-\xi_n^{i}\right)\right]^{a_i} = \varepsilon^{\tau_p - 1}$, onde τ_p é o automorfismo de Frobenius para p. Visto que p se decompõe completamente em K_n^{+}, então τ_p é a identidade quando restrito a K_n^{+} e portanto $N_{L/K}(u) = 1$ e o teorema está provado.

Já sabemos, pelo Lema 1.3.16, que $C_N(K_n^+) \leq C_J(K_n^+)$, mas para destacar a importância do Teorema 3.1.4, provaremos que o índice de $C_N(K_n^+)$ em $C_J(K_n^+)$ é consideravelmente grande.

Lema 3.1.5 : Seja n um número inteiro positivo. Se n é a potência de um número primo, digamos $n = p^a$ ($a \geq 2$ se $p = 2$), então $C_N(K_n^+) = C_J(K_n^+)^2$.

Demonstração : Se $\varepsilon \in C_J(K_n^+)$ então $\varepsilon^2 = N_{K_n/K_n^+}(\varepsilon) \in C_N(K_n^+)$, ou seja, $C_J(K_n^+)^2 \subseteq C_N(K_n^+)$. Por outro lado se $\varepsilon \in C_N(K_n^+)$ então $\varepsilon = \prod_{i=1}^{n-1}\left[\left(1-\xi_n^i\right)\left(1-\xi_n^{-i}\right)\right]^{a_i} = (-1)^{\sum_{i=1}^{n-1} a_i} \cdot \xi_n^{-\sum_{i=1}^{n-1} i.a_i} \cdot \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{2.a_i}$. Se $p = 2$ e, para cada $i = 1,\ldots,2^a-1$; fazemos $i = 2^{r_i}.t_i$, $(t_i,2) = 1$; temos $\sum_{i=1}^{n-1} i.a_i = \sum_{i=1}^{n-1} 2^{r_i}.t_i.a_i \equiv \sum_{i=1}^{n-1} 2^{r_i}.a_i \pmod 2$. Visto que $\sum_{i=1}^{n-1} 2^{r_i}.a_i = 0$ (Teorema 1.3.13), segue-se que $\sum_{i=1}^{n-1} i.a_i \equiv 0$ (mod 2) e portanto $\varepsilon = (-1)^{\sum_{i=1}^{n-1} a_i} \cdot \beta^2$, onde $\beta = \xi_n^{-\sum_{i=1}^{n-1} (i.a_i)/2} \cdot \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{a_i}$ $\in K_n$. Se $\sum_{i=1}^{n-1} a_i \equiv 0$ (mod 2) então $\beta \in K_n^+$ e $\varepsilon = \beta^2 \in C_J(K_n^+)^2$. Se $\sum_{i=1}^{n-1} a_i \equiv 1 \pmod 2$ então $\varepsilon = -\beta^2$, com $\overline{\beta} = -\beta$ e portanto $\beta \notin C_J(K_n^+)$. Fazendo $\delta = \xi_n^{n/4}.\beta \in K_n$, temos $\delta = \overline{\delta}$ e portanto $\delta \in C_J(K_n^+)$ e $\varepsilon = \delta^2 \in C_J(K_n^+)^2$, isto é, se $n = 2^a$ então $C_N(K_n^+) = C_J(K_n^+)^2$.

Agora suponhamos $n = p^a$, p um primo ímpar. Seja $\beta =$

$-\frac{n+1}{2}\sum_{i=1}^{n-1} i.a_i$
ζ_n $\cdot \prod_{i=1}^{n-1}\left(1-\zeta_n^i\right)^{a_i}$. Desde que $\sum_{i=1}^{n-1} a_i \equiv \sum_{i=1}^{n-1} p^{r_i}.a_i \pmod 2$ e $\sum_{i=1}^{n-1} p^{r_i}.a_i = 0$ (Teorema 1.2.13), onde $p^{r_i} \,||\, i$, segue-se que $\varepsilon = \beta^2$, como $\varepsilon > 0$, isto implica que $\beta \in C_I(K_n^+)$, o que completa a demonstração do teorema.

Observação 3.1.6: Dado um corpo abeliano real K, a parte de torção de $C_I(K)$ consiste das raizes da unidade contidas em K e portanto tal conjunto é $\{\pm 1\}$. Ainda por K ser um corpo real, o $\mathbb{Z}$-posto de $C_I(K)$ é $[K:\mathbb{Q}]-1$, pelo Teorema 1.2.2 e por $C_I(K)$ ter índice finito em $\mathcal{O}_K^*$. Visto que $C_I(K)^2$ é livre de torção, pode-se concluir facilmente que $[C_I(K):C_I(K)^2] = 2^{[K:\mathbb{Q}]}$, em particular, se $K = K_n^+$, então $[C_I(K):C_I(K)^2] = 2^{\phi(n)/2}$, onde ϕ é a função de Euler.

Teorema 3.1.7 : Para cado número inteiro positivo $n \geq 3$ seja $g(n)$ o índice $[C_I(K_n^+):C_N(K_n^+)]$. Então

$$g(n) = \begin{cases} 2^{\phi(n)/2} & \text{se n é uma potência de primo} \\ 2^{(\phi(n)/2)-1} & \text{caso contrário.} \end{cases}$$

Demonstração: Pela Observação 3.1.6 temos $[C_I(K_n^+):C_I(K_n^+)^2] = 2^{\phi(n)/2}$ e, por outro lado, sabemos que $[C_I(K_n^+):C_I(K_n^+)^2] = [C_I(K_n^+):C_N(K_n^+)].$ $[C_N(K_n^+):C_I(K_n^+)^2]$, pois $C_I(K_n^+)^2 \leq C_N(K_n^+) \leq C_I(K_n^+)$. Logo $g(n) = \left(2^{\phi(n)/2}\right)/[C_N(K_n^+):C_I(K_n^+)^2]$. Se n é uma potência de primo, o teorema decorre do Lema 3.1.5. Para completar a demonstração do

teorema falta mostrar que se n não é a potência de um número primo então $[C_N(K_n^+) : C_J(K_n^+)^2] = 2$. Seja $\varepsilon = \prod_{i=1}^{n-1}\left[\left(1-\xi_n^i\right).\left(1-\xi_n^{-i}\right)\right]^{a_i} \in C_N(K_n^+)$.

Se n é ímpar então $\beta = \xi_n^{-\frac{n+1}{2}\sum_{i=1}^{n-1} i.a_i} . \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{a_i} \in K_n$. Se além disso $\sum_{i=1}^{n-1} a_i \equiv 0 \pmod 2$ então $\beta \in C_J(K_n^+)$ e $\varepsilon = \beta^2 \in C_J(K_n^+)^2$. Mas se $\sum_{i=1}^{n-1} a_i \equiv 1 \pmod 2$ então tomamos $\varepsilon = (1-\xi_n)(1-\xi_n^{-1}).\varepsilon'$, donde $\varepsilon' = \prod_{i=1}^{n-1}\left\{\left(1-\xi_n^i\right).\left(1-\xi_n^{-i}\right)\right\}^{b_i}$, com $\sum_{i=1}^{n-1} b_i \equiv 0 \pmod 2$ e $\varepsilon' \in C_N(K_n^+)$, pois $\varepsilon, (1-\xi_n).(1-\xi_n^{-1}) \in C_N(K_n^+)$. Agora $\varepsilon' \in C_J(K_n^+)^2$ e portanto $\varepsilon \in (1-\xi_n)(1-\xi_n^{-1}).C_J(K_n^+)^2$.

Suponhamos agora que n é par. Se $\sum_{i=1}^{n-1} i.a_i \equiv 0 \pmod 2$ então $\beta = \xi_n^{-\sum_{i=1}^{n-1}\frac{j.a_i}{2}} . \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{a_i} \in K_n$. Se, além disto, $\sum_{i=1}^{n-1} a_i \equiv 0 \pmod 2$ então $\beta \in C_J(K_n^+)$ e $\varepsilon = \beta^2 \in C_J(K_n^+)^2$. Mas se $\sum_{i=1}^{n-1} a_i \equiv 1 \pmod 2$ então $\beta = \xi_n^{n/4}.\delta$, com $\delta \in C_J(K_n^+)$ e $\varepsilon = \delta^2$. Se, por outro lado, $\sum_{i=1}^{n-1} i.a_i \equiv 1 \pmod 2$, tomamos $\varepsilon = (1-\xi_n)(1-\xi_n^{-1}).\varepsilon'$, e, como no caso anterior, $\varepsilon \in (1-\xi_n)(1-\xi_n^{-1}).C_J(K_n^+)^2$. Com isto temos provado em ambos os casos, n par ou ímpar, que:

$C_N(K_n^+) \subseteq C_J(K_n^+)^2 \cup (1-\xi_n)(1-\xi_n^{-1}).C_J(K_n^+)^2$. Portanto, para concluir a

demonstração só precisamos mostrar que $(1-\xi_n)(1-\xi_n^{-1}) \notin C_I(K_n^+)^2$. Desde que $(1-\xi_n)(1-\xi_n^{-1}) = -\xi_n^{-1}(1-\xi_n)^2$, se $(1-\xi_n)(1-\xi_n^{-1}) \in C_I(K_n^+)^2 \subseteq (K_n^+)^2$ então $-\xi_n^{-1} \in (K_n^+)^2$, ou seja, $-\xi_n^{-1}$ seria uma raiz da unidade além se ser um número real positivo, isto é, $-\xi_n^{-1} = 1$. Logo $\xi_n^{-2} = 1$ e consequentemente $n = 2$, o que é um absurdo.

Corolário 3.1.8: Seja n um número inteiro positivo. Então $C_N(K_n^+)$ é um subgrupo próprio de $S(K_n^+)$.

Seria interessante estender estes resultados para corpos abelianos quaisquer.

Sejam K um corpo abeliano de condutor n e $\varepsilon \in C_I(K)$, digamos $\varepsilon = \xi_n^t \cdot \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{a_i}$ Seja $u = \xi_n^{2t} \cdot \prod_{j=1}^{(p-1)/2} \prod_{i=1}^{n-1}\left\{\left(1-\xi_n^i \cdot \xi_p^j\right)\cdot\left(1-\xi_n^i \cdot \xi_p^{-j}\right)\right\}^{b_{ij}}$

$\in K_n \cdot K_p^+$. Se $u \in L$ então $N_{L/K}(u) = \xi_n^{(p-1)\cdot t} \cdot \prod_{i=1}^{n-1}\left(\frac{1-\xi_n^{pi}}{1-\xi_n^i}\right)^{\sum_{j=1}^{(p-1)/2} b_{ij}}$.

Suponhamos $\sum_{j=1}^{(p-1)/2} b_{ij} = a_i$. Então $N_{L/K}(u) = \varepsilon^{\tau_p - 1}$, onde τ_p é o automorfismo de Frobenius para o primo p e portanto τ_p é a identidade quando restrito a K, uma vez que p se decompõe completamente em K, ou seja, $N_{L/K}(u) = 1$. Por outro lado é fácil ver que $\varepsilon^2 \equiv u \pmod{p}$ e portanto ε seria uma unidade especial.

Feitas estas considerações, o problema passa a ser: dado $\varepsilon = \xi_n^t \cdot \prod_{i=1}^{n-1}\left(1-\xi_n^i\right)^{a_i} \in K$, existem $b_{ij} \in \mathbb{Z}$ tais que $\sum_{j=1}^{(p-1)/2} b_{ij} = a_i$ e

$u = \xi_n^{2t} \cdot \prod_{j=1}^{(p-1)/2} \cdot \prod_{i=1}^{n-1}\left\{\left(1-\xi_n^i \cdot \xi_p^j\right)\cdot\left(1-\xi_n^i \cdot \xi_p^{-j}\right)\right\}^{b_{ij}} \in L$?

Ora, para que $u \in L$ é necessário e suficiente que $u^{\tau} = u$, para todo $\tau \in Gal(L'/L) \simeq Gal(K_n/K)$. Mas isto pode ser reescrito na forma: Dado ε e u, como acima, se $\tau \in G_n$ e $\varepsilon^{\tau} = \varepsilon$ então $u^{\tau} = u$? Visto isso, podemos supor que $Gal(K_n/K)$ é cíclico no seguinte sentido: Se queremos resolver o problema para os corpos abelianos, devemos fazê-lo também para os corpos com a condição acima. Por outro lado todo corpo abeliano de condutor n é a intersecção de subcorpos k de K_n, com $Gal(K_n/k)$ cíclico.

Voltando a $Gal(K_n/K)$, que suporemos cíclico, gerado por, digamos τ_r, com $\tau_r(\xi_n) = \xi_n^r$ e portanto a solução do nosso problema passa a ser a solução do seguinte sistema:

$$\begin{cases} \sum_{j=1}^{(p-1)/2} b_{ij} = a_i, \ i = 1, \ldots, n-1 \\ u^{\tau_r} = u. \end{cases} \qquad (3.11)$$

Seja $v = u^{\tau_r - 1}$. Para que v seja igual a 1 é necessário e suficiente que o ângulo $\delta(v)$, formado por v e o eixo positivo de X seja múltiplo inteiro de $2.\pi$ e $|v| = 1$, pois $v \neq 0$.

Lema 3.1.9: Sejam ε e u como acima. Então $\delta(v) = 2.\delta(\varepsilon^{\tau_r - 1})$. Em particular se $\varepsilon^{\tau_r} = \varepsilon$ então $\delta(v) \equiv 0 \pmod{2.\pi}$.

Demonstração: Pelo Lema 2.2.3, temos:

$$\delta(u) = \frac{2\pi(2.t)}{n} + \pi.\sum_{i=1}^{n-1} \sum_{j=1}^{(p-1)/2} b_{ij}\left[\left(\frac{p.i+n.j}{p.n} - \frac{1}{2}\right) + \left(\frac{p.i-n.j}{p.n} - \frac{1}{2}\right)\right] =$$

$$2.\left[\frac{2.\pi.t}{n} + \pi.\sum_{i=1}^{n-1}\left(\frac{i}{n} - \frac{1}{2}\right).\sum_{j=1}^{(p-1)/2} b_{ij}\right] =$$

$$2.\left[\frac{2.\pi.t}{n} + \pi.\sum_{i=1}^{n-1} a_i\left(\frac{i}{n} - \frac{1}{2}\right)\right] = 2.\delta(\varepsilon).$$

Analogamente $\delta(u^{\tau_r}) = 2.\delta(\varepsilon^{\tau_r})$, e portanto $\delta(u^{\tau_r-1}) = 2\delta(\varepsilon^{\tau_r-1})$

Pelo Teorema 2.2.2 e a observação que o segue, $|u^{\tau_r-1}| = 1$ se e somente se $Y(u^{\tau_r-1},\chi) = 0$ para todo caracter par não trivial χ definido mod p.n e $Y_q(u^{\tau_r-1}) = 0$ para todo primo q que divide p.n.

Pelo Teorema 1.3.13, $Y_q(u^{\tau_r-1}) = 0$ para todo primo que divide p.n se e somente se u^{τ_r-1} é uma unidade e pelo Lema 1.3.12, u^{τ_r-1} sempre é uma unidade; logo resolver a equação $|u^{\tau_r-1}| = 1$ equivale a resolver o sistema $Y(u^{\tau_r-1},\chi) = 0$ para todo caracter par não trivial definido mod p.n.

Ora, se χ é um caracter definido mod p.n , então podemos escrever $\chi = \chi_p.\chi_n$ com χ_p um caracter definido mod p e χ_n definido mod n. Além disto χ_p e χ_n têm a mesma paridade, pois χ é par. Visto que $\tau_r \in Gal(L'/L)$ então τ_r fixa $\xi_p+\xi_p^{-1}$ e portanto podemos supor $r \equiv 1 \pmod p$; com isto temos $\chi(r) = \chi_n(r)$. Pelo Lema 2.2.4 e a observação acima deduzimos que

$$Y(u^{\tau_r-1}, \chi_p.\chi_n) = (\chi_n(r)-1).Y(u, \chi_p.\chi_n). \qquad (3.12)$$

Como nosso interesse ficará restrito à $Y(u, \chi)$, podemos supor

$$u = \prod_{j=1}^{(p-1)/2} \cdot \prod_{i=1}^{n-1}\left\{\left(1-\xi_n^i.\xi_p^j\right).\left(1-\xi_n^i.\xi_p^{-j}\right)\right\}^{b_{ij}}. \qquad (3.13)$$

Mas $1-\xi_n^i.\xi_p^j = 1-\xi_{p.n}^{p.i+n.j}$ logo por razões práticas,reescrevemos

$$u = \prod_{j=1}^{(p-1)/2} \cdot \prod_{i=1}^{n-1} \left\{ \left(1-\xi_n^i.\xi_p^j\right).\left(1-\xi_n^i.\xi_p^{-j}\right) \right\}^{b_{p.i+n.j}} \qquad (3.14)$$

ou ainda

$$u = \prod_{k=1}^{p.n-1} \left(1-\xi_{p.n}^k\right)^{c_k} \text{, onde } c_k = \begin{cases} b_{p.i+nj} \text{ se } k \equiv p.i \pm n.j \pmod{p.n} \\ 0 \text{ caso contrário.} \end{cases} \qquad (3.15)$$

Agora $\sum_{j=1}^{(p-1)/2} b_{p.i+n.j} = a_i$. (3.16)

Feitas estas considerações, temos:

$$T(u,d,\chi_p.\chi_n) = \sum_{\substack{k=1 \\ (d,k)=1}}^{d-1} \chi_p.\chi_n(k).c_{(p.n/d).k}.$$

Se $p \nmid d$ então $c_{(p.n/d).k} = 0$,pois $(p.n/d).k \not\equiv p.i \pm n.j \pmod{p.n}$.

Agora temos:

$$Y(u,\chi) = z.\sum_{\substack{d|n \\ f_\chi | p.d}} \left(1/\phi(d)\right). \prod_{q:\text{primo}, q|d} (1-\bar{\chi}(q)).T(u,p.d,\chi). \qquad (3.17)$$

onde $z = (1-\bar{\chi}(p))/\phi(p)$.

Mas $T(u,p.n,\chi) = \sum_{\substack{k=1 \\ (k,p.d)=1}}^{p.d-1} \chi(k).c_{(n/d).k}$ e $(n/d).k \equiv p.i+n.j \pmod{p.n}$

se e somente se $i = (n/d).t$ para algum t, $1 \le t < d$, e $k \equiv p.t+d.j \pmod{p.d}$. Neste caso $(k,p.d) = 1$ se e somente se $(j,p) = (t,d) = 1$

Logo

$$T(u,p.d,\chi) = \sum_{j=1}^{p-1} \sum_{\substack{t=1 \\ (t,d)=1}}^{d-1} \chi_p.\chi_n(p.t+n.j).c_{\frac{n}{d}.(p.t+n.j)}, \qquad (3.18)$$

ou seja,

$$T(u,p.d,\chi) = \sum_{j=1}^{p-1} \sum_{\substack{k=1 \\ (k,d)=1}}^{d-1} \chi_p . \chi_n(p.k+d.j) . c_{p.\left(\frac{n.k}{d}\right)+n.j} \qquad (3.19)$$

$$= \sum_{j=1}^{(p-1)/2} \sum_{\substack{k=1 \\ (k,d)=1}}^{d-1} \left[\chi_p\chi_n(p.k+d.j) + \chi_p\chi_n(p.k-n.j)\right] . b_p\left[(n/d).k\right]+n.j =$$

$$\chi_p(d).\chi_n(p).\sum_{j=1}^{(p-1)/2} \sum_{\substack{k=1 \\ (k,d)=1}}^{d-1} \left[\chi_p(j).\chi_n(k)+\chi_p(-j).\chi_n(k)\right] . b_p\left[(n/d).k\right]+n.j$$

Aqui podemos deduzir que se χ_p é um caracter ímpar então $T(u, p.d, \chi) = 0$ e portanto $Y(u,\chi) = 0$. Logo, daqui para frente, consideraremos χ_p e χ_n caractere pares, pois χ o é.

Com esta condição temos:

$$T(u,p.d,\chi) = 2.\chi_p(d).\chi_n(p).\sum_{j=1}^{(p-1)/2} \sum_{\substack{k=1 \\ (k,d)=1}}^{d-1} \chi_p(j).\chi_n(k).b_p\left[(n/d).k\right]+n.j$$

Se χ_p é o caracter trivial então

$$T(u,\ p.d,\ \chi) = 2.\chi_n(p).\sum_{\substack{k=1 \\ (k,d)=1}}^{d-1} \chi_n(k).\sum_{j=1}^{(p-1)/2} b_{p.\left[(n/d).k\right]+n.j} =$$

$$2.\chi_n(p).\sum_{\substack{k=1 \\ (k,d)=1}}^{d-1} \chi_n(k).a_{(n/d).k} = 2.\chi_n(p).T(\varepsilon,d,\chi_n)$$

Partindo da equação (3.17), com a hipótese de que χ_p é trivial, temos:

$$Y(u,\chi) = z'.\sum_{\substack{d|n \\ f_\chi \,|\, p.d}} \left[1/\phi(d)\right] \prod_{\substack{q:primo \\ q|d}} (1-\overline{\chi}_n(q)).T(\varepsilon,\ d,\ \chi_n)$$

onde $z' = 2.(\chi_n(p)-1)/\phi(p)$, ou seja, $Y(u,\chi) = z'.Y(\varepsilon,\chi_n)$. Mas χ é um caracter não trivial e χ_p, por hipótese, é um caracter trivial; logo χ_n é um caracter par não trivial. Visto que $\chi_n(r) \neq 1$ e $\varepsilon \in K$ segue que $Y(\varepsilon,\chi_n) = 0$ e portanto, para $\chi_p = 1$, temos $Y(u,\chi) = 0$.

O nosso objetivo restringe-se, agora, a analizar a nulidade de $Y(u,\chi_p\chi_n)$ com χ_p e χ_n caracteres pares, $\chi_n(r) \neq 1$ e χ_p não trivial. Neste caso $\chi_p(p) = 0$ e portanto $z = 2.\chi_n(p)/(p-1)$.

Observação 3.1.10 : Dados n um número inteiro positivo e $i \in \{1,\ldots,n-1\}$, é claro que podemos escrever $i = (n/d_i).k_i$, com d_i, k_i únicos se $(k_i,d_i) = 1$. De fato, se tomarmos $d_i = n/(n,i)$ e $k_i = i/(n,i)$, podemos constatar que d_i e k_i satisfazem as condições desejadas.

Teorema 3.1.11 : Seja K um corpo abeliano. Se o condutor de K é uma potência de primo então $C_I(K) \subseteq S(K)$.

Demonstração : Suponhamos $n = q_1^a$ o condutor de K. Se

$$\varepsilon = \pm\xi_n^t.\prod_{i=1}^{n-1}(1-\xi_n^i)^{a_i} \in K,$$

seja

$$u = \xi_n^{2t}.\prod_{j=1}^{(p-1)/2}\prod_{i=1}^{n-1}\left[\left(1-\xi_n^i.\xi_p^j\right)\left(1-\xi_n^i.\xi_p^{-j}\right)\right]^{b_{p.i+n.j}},$$

onde

$$b_{p.i+n.j} = \begin{cases} a_i & \text{se } j.d_i \equiv 1 \pmod p, \\ 0 & \text{caso contrário.} \end{cases}$$

onde d_i é como na Observação 3.1.10.

Com esta escolha para $b_{p.i+n.j}$ já temos satisfeito, trivialmente, a primeira condição de (3.11). Falta provar que $Y(u,\chi_n.\chi_p) = 0$ para χ_n , χ_p caracteres mod n e mod p, respectivamente, χ_p não trivial e $\chi_n(r) \neq 1$. Ora, nestas concições, temos $\prod_{\substack{q:primo \\ q|d}}(1-\overline{\chi}(q)) = 1$, para todo d que divide n, pois n é uma potência de primo. Logo

$$Y(u,\chi_n.\chi_p) = z.\sum_{\substack{d|n \\ f_{\chi_n}|d}}\left(1/\phi(d)\right)T(u,p.d,\chi_n.\chi_p), \text{ onde } z = 1/\phi(p), \text{ por}$$

(3.17). Mas

$$T(u,p.d,\chi_n.\chi_p) = 2\chi_n(p).\sum_{j=1}^{(p-1)/2}.\sum_{\substack{k=1 \\ (k,d)=1}}^{d-1}\chi_p(d.j).\chi_n(k).b_{p((n/d)k)+n.j}$$

Sendo $(k,d) = 1$ então $b_{p\left((n/d).k\right)+n.j} = a_k$ quando $j.d \equiv 1 \pmod p$ e zero nos demais casos, logo

$$T(u,p.d,\chi_n.\chi_p) = 2.\chi_n(p).\sum_{\substack{k=1 \\ (k,d)=1}}^{d-1}\chi_p(1).\chi_n(k).a_k = 2.\chi_n(p).T(\varepsilon,\chi_n) \text{ e,}$$

consequentemente,

$$Y(u,\chi_n.\chi_p) = 2.z.\chi_n(p).\sum_{\substack{d|n \\ f_{\chi_n}|d}}\left(1/\phi(d)\right)T(\varepsilon,d,\chi_n) = 2.z.\chi_n(p).Y(\varepsilon,\chi_n).$$

Mas χ_n é um caracter par e $\chi_n(r) \neq 1$, logo $Y(\varepsilon,\chi_n) = 0$ e portanto $Y(u,\chi_n.\chi_p) = 0$, e o teorema está provado.

3.2 UNIDADES ESPECIAIS, SEGUNDO THAINE.

Sejam $p \geq 5$ um primo racional, $K = K_p^+$ e $(A)_p$ a p-parte do grupo las classes de ideais de K_p^+.

Dado um caracter p-ádico de Dirichlet χ de $\Delta = Gal(K/\mathbb{Q})$, seja

$$e_\chi = \frac{1}{|\Delta|} \cdot \sum_{\gamma \in \Delta} \chi(\gamma) \cdot \gamma^{-1} \in \mathbb{Z}_p[\Delta] \qquad (3.20)$$

) idempotente correspondente.

Existe uma ação natural de $\mathbb{Z}_p[\Delta]$ em $(A)_p$ e, com consequência las propriedades dos idempotentes e_χ, obtemos

$$(A)_p = \oplus_{\chi \in \Delta^\wedge} e_\chi (A)_p. \qquad (3.21)$$

Fixado um caracter χ não trivial p-ádico de Dirichl , seja n ım número inteiro positivo tal que $p^n > |e_\chi(A)_p|$.

roposição 3.2.1 : Seja $C \in e_\chi(A)_p$. Então existem infinitos ideais rimos $Q \in C$ tais que $Q \cap \mathbb{Z} = q.\mathbb{Z}$, com $q \equiv 1 \pmod{p^n}$.

demonstração : Ver [4], Proposição 2.

Ora, se $q \equiv 1 \pmod p$ então q se decompõe completamente em K e $\mathfrak{l}^\gamma$, $\gamma \in \Delta$, são todos os ideais primos de K acima de q. Agora screvemos $q-1 = v.p^j$, com $(p,v) = 1$, $L = K(\xi_q)$, τ um gerador de al(L/K) e g uma raiz primitiva mod q tal que $\tau(\xi_q) = \xi_q^g$.

efinição 3.2.2 : Preservando a notação acima, $\delta \in \mathfrak{O}_K^*$ é uma unidade special para Q se existe $\delta' \in L$, com $N_{L/K}(\delta') = 1$, tal que $\delta'.\mathfrak{O}_L = F^{(\tau-1)^2}$, para algum ideal (fracionário não nulo) F de L e $\delta^v \equiv \delta'^v \pmod{(1-\xi_q)\mathfrak{O}_L}$.

Ora, se $\delta' \in L$ e $N_{L/K}(\delta') = 1$ então, pelo Teorema 90 de Hilbert, existe $\alpha \in L$, $\alpha \neq 0$, tal que $\delta' = \alpha^{\tau-1}$. Logo a condição $\delta^{\nu} \equiv \delta'^{\nu} \pmod{(1-\xi_q)\mathfrak{O}_L}$ equivale a $\delta^{\nu} \equiv (\alpha^{\tau-1})^{\nu} \pmod{(1-\xi_q)\mathfrak{O}_L}$, ou seja, a unidade δ de K é especial para Q se existem $\alpha \in L$, $\alpha \neq 0$, e F um ideal (fracionário não nulo) de L tais que:

a) $(\alpha^{\tau-1}) = F^{(\tau-1)^2}$,

b) $\delta^{\nu} \equiv (\alpha^{\tau-1})^{\nu} \pmod{(1-\xi_q)\mathfrak{O}_L}$.

A condição a) é equivalente a $(\alpha^{-1}.F^{\tau-1})^{\tau-1} = (1)$. Comparando esta equação com o comentário feito no início deste capítulo até a equação (3.1) deduzimos que se B é o único ideal primo de L acima de Q então a igualdade $(\alpha^{-1}.F^{\tau-1})^{\tau-1} = (1)$ equivale à existência de um ideal $\mathfrak{A}$ de K e números inteiros r_γ, $\gamma \in \Delta$, tais que

$$\alpha.\mathfrak{O}_L = \mathfrak{A}.F^{\tau-1}.\prod_{\gamma\in\Delta}(B^{\gamma})^{r_\gamma}. \qquad (3.22)$$

Por isto podemos redefinir as unidades especiais de K para Q como segue: Seja $\delta \in \mathfrak{O}_K^*$. Dizemos que δ é uma unidade especial para Q se existem $\alpha \in L$, $\alpha \neq 0$, um ideal $\mathfrak{A}$ de K, F um ideal de L e números inteiros r_γ, $\gamma \in \Delta$, tais que:

a) $\alpha.\mathfrak{O}_L = \mathfrak{A}.F^{\tau-1}.\prod_{\gamma\in\Delta}(B^{\gamma})^{r_\gamma}$

b) $\delta^{\nu} \equiv (\alpha^{\tau-1})^{\nu} \pmod{(1-\xi_q)\mathfrak{O}_L}$. (3.23)

Visto que q se ramifica completamente em K_q e se decompõe completamente em K, deduzimos que

$$(1-\xi_q).\mathfrak{O}_L = \prod_{\gamma\in\Delta} B^{\gamma}. \qquad (3.24)$$

Agora, para cada $\gamma \in \Delta$, seja $x_\gamma \in \mathfrak{O}_K$ tal que $x_\gamma \in Q^{\gamma} \setminus (\bigcup_{\substack{\mu\in\Delta \\ \mu\neq\gamma}} Q^{\mu})$.

Seja $y_\gamma = x_\gamma + (1-\xi_q)$, $\gamma \in \Delta$. Visto que $x_\gamma \in Q^\gamma = (B^\gamma)^{q-1}$, segue que

$$y_\gamma \in B^\gamma \setminus \left((B^\gamma)^2 \cup \bigcup_{\substack{\mu \in \Delta \\ \mu \neq \gamma}} B^\mu \right). \qquad (3.25)$$

Teorema 3.2.3 : Sejam A o anel dos inteiros de K e D o anel dos inteiros de L. Então $D = A[\xi_q]$.

Demonstração : É claro que $A[\xi_q] \subseteq D$. Seja $\beta = a_0 + a_1.(1-\xi_q) + \ldots + a_{q-2}.(1-\xi_q)^{q-2}$, $a_i \in K$, $i = 1,\ldots,q-2$; um elemento qualquer de D. Devemos mostrar que $a_i \in A$, $i = 1,\ldots,q-2$. Visto que Q se ramifica completamente em L, temos $v_B(a_i) \equiv 0 \pmod{(q-1)}$. Mas $v_B((1-\xi_q)^i) = i$, logo, se $i \neq j$, temos $v_B(a_i.(1-\xi_q)^i) \neq v_B(a_j.(1-\xi_q)^j)$, pois mod q-1 estes números são distintos. Neste caso temos:

$$v_B(\beta) = \min \{ i + v_B(a_i),\ i = 0,\ldots,q-2 \} \geq 0. \qquad (3.26)$$

Concluimos com isto que $v_B(a_i) \geq 0$, $\forall\ i = 1,\ldots,q-2$.

Agora escrevemos

$$\beta_i = \beta^{\tau^i} = b_0 + b_1.\xi_q^{\tau^i} + \ldots + b_{q-2}.(\xi_q^{\tau^i})^{q-2},\ i = 0,\ldots,q-2. \qquad (3.27)$$

É claro que $v_B(b_i) \geq 0$, $i = 0,\ldots,q-2$; e o sistema (3.27) é equivalente à equação

$$\begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{q-2} \end{pmatrix} = E. \begin{pmatrix} b_0 \\ \vdots \\ b_{q-2} \end{pmatrix} \qquad (3.28)$$

onde E é a matriz $\left(\xi_q^{i.g^j} \right)_{i,j=0,\ldots,q-2}$, $\tau(\xi_q) = \xi_q^g$.

Sendo E uma matriz de Vandermonde temos $|E| = \pm \prod_{1 \le i < j \le q-1} (\xi_q^i - \xi_q^j)$ $= \pm \xi_q^t . (1-\xi_q)^w$, $t, w \in \mathbb{Z}$, $w > 0$; e, pela regra de Cramer, $b_i = \beta_i / |E|$. Seja δ um ideal primo de L que não está acima de q. Então $v_\delta(\beta_i) = v_\delta(b_i) - v_\delta(|E|) = v_\delta(b_i) \ge 0$. Com isto concluimos que a valorização q-ádica aplicada sobre os $b_{i,s}$ é sempre maior ou igual a zero, qualquer que seja o ideal primo q de L, ou seja, b_i é um elemento integral de L e, portanto, integral de K e o teorema está demonstrado.

Lema 3.2.4 : Dado $z_\gamma \in \mathfrak{O}_L$, temos que $z_\gamma \in B^\gamma \setminus \left((B^\gamma)^2 \cup \bigcup_{\substack{\mu \in \Delta \\ \mu \neq \gamma}} B^\mu \right)$ se e somente se ao escrevermos

$z_\gamma = b_0 + b_1 . (1-\xi_q) + \ldots + b_{q-2} . (1-\xi_q)^{q-2}$ temos: $b_0 \in Q^\gamma \setminus \left(\bigcup_{\substack{\mu \in \Delta \\ \mu \neq \gamma}} Q^\mu \right)$ e $b_1 \notin Q^\gamma$.

Demonstração: Pelo Teorema 3.2.3, dado $z_\gamma \in \mathfrak{O}_L$, existem $b_0, \ldots, b_{q-2} \in \mathfrak{O}_K$ tais que $z_\gamma = b_0 + b_1 . (1-\xi_q) + \ldots + b_{q-2} . (1-\xi_q)^{q-2}$. Visto que $1-\xi_q \in B^\gamma \setminus (B^\gamma)^2$, $\forall\, \gamma \in \Delta$, então $z_\gamma \in B^\gamma$ se e somente se $b_0 \in Q^\gamma$. Logo $b_0 \in (B^\gamma)^2$ e portanto $z_\gamma \notin (B^\gamma)^2$ se e somente se $b_1 \notin Q^\gamma$ e a demonstração do lema está completa.

Agora $\tau(y_\gamma) = x_\gamma + (1-\xi_q^g) = x_\gamma + (1-\xi_q).(1+\xi_q+\ldots+\xi_q^{g-1})$. Visto que $1 \equiv \xi_q \pmod{B^\gamma}$, $\forall\, \gamma \in \Delta$, segue-se que $y_\gamma^\tau \equiv x_\gamma + g.(1-\xi_q) \pmod{(B^\gamma)^2}$. Mas $x_\gamma \in (B^\gamma)^2$, logo $y_\gamma^\tau \equiv g.(x_\gamma + (1-\xi_q)) \pmod{(B^\gamma)^2}$, ou seja, $y_\gamma^\tau \equiv g.y_\gamma \pmod{(B^\gamma)^2}$. Com isto, $v_{B^\gamma}(y_\gamma^\tau) = v_{B^\gamma}(y_\gamma) = 1$ e,

consequentemente, $y_\gamma^{\tau-1} \equiv g \pmod{B^\gamma}$. Mais geralmente, se $z \in \mathfrak{O}_K$, $z \notin Q^\gamma$ então, reescrevendo $y_\gamma = x_\gamma + z.(1-\xi_q)$ deduzimos, ainda, que $y_\gamma^{\tau-1} \equiv g \pmod{B^\gamma}$. Também é claro que se $\mu \neq \gamma$ então $y_\gamma^{\tau-1} \equiv 1 \pmod{B^\mu}$.

Teorema 3.2.5 : Preservando a notação acima, seja $\delta \in \mathfrak{O}_K^*$, $\delta \equiv g^{c_\gamma} \pmod{Q^\gamma}$. Então δ é uma unidade especial para Q se e somente se existem ideais não nulos $\mathcal{A}$ e F, de K e L, respectivamente, e números inteiros r_γ, $\gamma \in \Delta$, tais que $r_\gamma \equiv c_\gamma \pmod{p^j}$, $\forall\, \gamma \in \Delta$, e $\mathcal{A}.F^{\tau-1}.\prod_{\gamma\in\Delta}(B^\gamma)^{r_\gamma}$ é um ideal principal.

Demonstração : Suponhamos que δ seja uma unidade especial para Q, $\delta \equiv g^{c_\gamma} \pmod{Q^\gamma}$, $\gamma \in \Delta$. Por (3.23) a), existem $\alpha \in L$, $\alpha \neq 0$, $\mathcal{A}$ um ideal não nulo de K, F um ideal não nulo de L e números inteiros r_γ, $\gamma \in \Delta$, tais que $\alpha.\mathfrak{O}_L = \mathcal{A}.F^{\tau-1}.\prod_{\gamma\in\Delta}(B^\gamma)^{r_\gamma}$. Mostraremos agora que $r_\gamma \equiv c_\gamma \pmod{p^j}$. Pelas considerações anteriores ao enunciado deste teorema, se $y = \prod_{\gamma\in\Delta} y_\gamma^{r_\gamma}$ então $y^{\tau-1} \equiv g^{r_\gamma} \pmod{B^\gamma}$, $\gamma \in \Delta$ e $(\alpha/y)^{\tau-1} \equiv 1 \pmod{B^\gamma}$, $\forall\, \gamma \in \Delta$, pois $\upsilon_{B^\gamma}(\alpha/y) = 0$ e portanto, para cada $\gamma \in \Delta$, existem z_γ, $w_\gamma \in \mathfrak{O}_L$ tais que $\alpha/y = z_\gamma/w_\gamma$ e $\upsilon_{B^\gamma}(z_\gamma) = \upsilon_{B^\gamma}(w_\gamma) = 0$ (ver [4], pg. 6). Como $z_\gamma^{\tau-1} \equiv w_\gamma^{\tau-1} \equiv 1 \pmod{B^\gamma}$, temos $(\alpha/y)^{\tau-1} \equiv 1 \pmod{B^\gamma}$, $\forall\, \gamma \in \Delta$. Disto deduzimos que $\alpha^{\tau-1} \equiv y^{\tau-1} \equiv g^{r_\gamma} \pmod{B^\gamma}$, $\gamma \in \Delta$. Elevando ambos os lados ao expoente v, temos $(\alpha^{\tau-1})^v \equiv (g^{r_\gamma})^v \pmod{B^\gamma}$ e, pela condição b) de (3.23) temos $\delta^v \equiv$

$(g^{r_\gamma})^v \pmod{B^\gamma}$, ou seja, $(g^{c_\gamma})^v \equiv (g^{r_\gamma})^v \pmod{q}$ e portanto $v.c_\gamma \equiv v.r_\gamma \pmod{q-1}$, isto é, $c_\gamma \equiv r_\gamma \pmod{p^j}$.

Reciprocamente, seja $\delta \in \mathfrak{O}_K^*$, $\delta \equiv g^{c_\gamma} \pmod{Q^\gamma}$ e suponhamos que existem ideais não nulos $\mathfrak{A}$ e F, de K e L, respectivamente, e números inteiros r_γ, $\gamma \in \Delta$, tais que $r_\gamma \equiv c_\gamma \pmod{p^j}$ e $\mathfrak{A}.F^{\tau-1}.\prod_{\gamma\in\Delta}(B^\gamma)^{r_\gamma}$ seja principal, digamos, gerado por $\alpha \in L$, $\alpha \neq 0$. Seja $\delta' = \alpha^{\tau-1}$. É claro que $N_{L/K}(\delta') = 1$ e $\delta'.\mathfrak{O}_L = F^{(\tau-1)^2}$. Pelo que vimos no início desta demonstração, $\alpha^{\tau-1} \equiv g^{r_\gamma} \pmod{B^\gamma}$, $\gamma \in \Delta$, e portanto $(\alpha^{\tau-1})^v \equiv (g^{r_\gamma})^v \pmod{B^\gamma}$. Mas $\delta \equiv g^{c_\gamma} \pmod{B^\gamma}$ e $c_\gamma \equiv r_\gamma \pmod{p^j}$, logo $v.c_\gamma \equiv v.r_\gamma \pmod{q-1}$ e $\delta^v \equiv g^{v.c_\gamma} \equiv g^{v.r_\gamma} \equiv (\delta')^v \pmod{B^\gamma}$ e portanto δ é uma unidade especial para o primo Q e o teorema está demonstrado.

REFERÊNCIAS

[1] L. C. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Mathematics, Springer-Verlag, New York (1.982).

[2] T. Nóbrega, Circular Units of Abelian Number Fields, An. Acad. Bras. Ci., 62 (1.990) 1-4.

[3] T. Nóbrega, A Note on Special Units of Rubin, C. R. Math. Rep. Acad. Sci. Canada, 12 (1.990) 131-134.

[4] F. Thaine, On the Ideal Class Groups of Real Abelian Number Fields, Ann. of Math. 128 (1.988) 1-18.

[5] S. Lang, Algebra, Addison-Wesley, Reading, MA (1.965).

[6] W. Sinnott, On the Stickelberger Ideal and Circular Units of an Abelian Number Field, Invent. Math. 622 (1.980) 181-234.

[7] K. Rubin, Global Units and Ideal Class Groups, Invent. Math. 89 (1.987) 511-526.

[8] F. Thaine, On the Orders of Ideal Classes in Prime Cyclotomic Fields, Math. Proc. Camb. Philos. Soc. 108 (1.990) 197-201.

[9] K. Ramachandra, On the Units of Cyclotomic Fields, Acta Arithmetica, 12 (1.966) 165-173.

[10] V. Ennola, On Relations Between Cyclotomic Units, J. Number Theory, 4 (1.972) 236-247.

[11] P. Samuel, Thèorie Algèbrique des Nombres, Hermann, Paris (1.967).

[12] W. Sinnott, On the Stickelberger Ideal and the Circular Units of a Cyclotomic Field, Ann. of Math. 108 (1.978) 107-134.

[13] G. Letl, A Note on Thaine's Circular Units, J. Number Theory, 35 (1.990) 224-226.