SOBRE OS GRUPOS DAS CLASSES DE IDEAIS DOS CORPOS NUMÉRICOS ABELIANOS REAIS

Francisco Thaine Prada

Tese de Livre Docencia.

Para meus filhos

Marcia e Javier

AGRADECIMENTOS

Agradeço ao Professor Lawrence Washington pela sua indispensável ajuda e suas excelentes aulas na Universidade de Maryland, e ao Professor René Schoof pela prova do ponto crucial da Seção 2.

Agradeço à senhorita Elda Mortari pelo excelente trabalho de datilografia.

SOBRE OS GRUPOS DAS CLASSES DE IDEAIS DOS CORPOS NUMÉRICOS ABELIANOS REAIS(*)

Francisco Thaine

RESUMO. Se obtem uma relação entre os grupos das classes de ideais e os grupos das unidades dos corpos numéricos abelianos reais por meio do estudo da fatoração em ideais primos de certos inteiros ciclotômicos semelhantes às somas de Gauss. Se obtem anuladores de classes de ideais que satisfazem uma condição dada. Esta condição é satisfeita por todas as classes cuja ordem é uma potência de p se o corpo está contido num corpo p^n-ciclotômico (p primo).

Para uma classe de corpos, a relação mencionada induz uma outra entre o grupo das classes de ideais e o grupo quociente das unidades por as unidades circulatórias. Os subcorpos reais dos corpos p-ciclotômicos são dessa classe. Se dá uma aplicação ao último teorema de Fermat.

(*) Este trabalho foi parcialmente feito na Universidade de Maryland em College Park onde o autor estava com uma bolsa do CNPq.

INTRODUÇÃO E ALGUNS FATOS BÁSICOS

Sejam K um corpo numérico real abeliano, A seu anel de inteiros e $\zeta = \zeta_m$ uma raiz m-ésima primitiva da unidade, onde m é o menor inteiro positivo tal que $K \subseteq \mathbb{Q}(\zeta_m)$. Sejam Γ o grupo de Galois de $\mathbb{Q}(\zeta_m)/K$ e G o grupo de Galois de $K/\mathbb{Q}$.

Definimos os seguintes conjuntos de funções racionais na indeterminada X:

$$W(X) = \{f(X) = \pm \zeta^j \prod_{k=1}^{m-1} (X - \zeta^k)^{a_k} : j,\ a_k \in \mathbb{Z} \text{ e } f(1) \text{ é uma unidade de } \mathbb{Z}[\zeta]\},$$

$$V(X) = \{ \prod_{\sigma \in \Gamma} f^{\sigma}(X) : f(X) \in W(X) \}.$$

Claramente $V(X) \subseteq K(X)$ (funções racionais sobre K).

Seja U o grupo das unidades positivas de A. O conjunto $V(1)$ é um subgrupo de índice finito de U que nos chamamos de grupo das unidades circulatórias positivas de A (note que a conjugação complexa pertence a Γ). Definimos $\Omega = U/V(1)$.

Sejam q um primo racional impar que se decompõe completamente em A, e $\theta = \theta_q$ uma raiz q-ésima primitiva da unidade. Chamemos N_θ à norma de $K(\theta)$ em K. O seguinte fato é fundamental para este trabalho:

PROPOSIÇÃO 1. Se $f(X) \in V(X)$ então $N_\theta(f(\theta)) = 1$.

DEMONSTRAÇÃO. Temos $f(\theta) \in K(\theta)$, logo $N_\theta(f(\theta))$ é um elemento bem definido de K. Se $f(X) = \prod_{k=1}^{m-1} (X - \zeta^k)^{a_k}$, $a_k \in \mathbb{Z}$, então

$$N_\theta(f(\theta)) = \prod_{k=1}^{m-1} \left(\frac{1 - \zeta^{kq}}{1 - \zeta^k}\right)^{a_k} = \frac{\delta(\zeta^q)}{\delta(\zeta)}, \text{ onde}$$

$$\delta(\zeta) = \prod_{k=1}^{m-1} (1 - \zeta^k)^{a_k} \in A.$$

Como q se decompõe completamente em A, temos $\delta(\zeta^q) = \delta(\zeta)$ e a proposição segue.

Seja s uma raiz primitiva modulo q e seja τ o K-automorfismo de $K(\theta)$ tal que $\tau(\theta) = \theta^s$. Da Proposição (1) e do Teorema 90 de Hilbert concluimos que: Se $f(X) \in V(X)$ e $\varepsilon = f(\theta)$, então existe $\alpha \in A[\theta]$, $\alpha \neq 0$ tal que $\tau(\alpha) = \varepsilon\alpha$.

As idéias deste trabalho são uma extensão das idéias de Kummer que levaram ao Teorema de Stickelberger, mas enquanto o Teorema de Stickelberger não diz nada sobre os subcorpos reais de $\mathbb{Q}(\zeta)$, os resultados que nós obtivemos são mais naturalmente estabelecidos para esses corpos.

Na Seção (1) estudamos a fatoração em ideais primos dos elementos α definidos acima. Na Seção (2) relacionamos esta fatoração com a estrutura do grupo das unidades de A (Teorema 1). Isto é conseguido por meio de um teoremas local-global (Proposição 5). A ajuda dada e os belos teoremas de Teoria dos Corpos de

Classes mostrados para mim pelos Professores Lawrence Washington e René Schoof, o primeiro sugerindo a estratégia da prova e o segundo resolvendo o ponto principal, foram essenciais para chegar a este resultado.

Na Seção (3) usamos os resultados das seções anteriores para obtermos anuladores (em $\mathbb{Z}[G]$) de um conjunto de classes de ideais (Proposições 7, 8, 10). Este conjunto contém o p-Sylow subgrupo do grupo das classes de ideais de K se este corpo está contido num corpo p^e-ciclotômico (p primo). Os anuladores mencionados se expressam em termos dos maiores inteiros n tais que certas unidades de V(1) são n-ésimas potências de outras unidades.

Para corpos que satisfazem uma condição (Proposição 11) podemos ir além e estabelecer uma relação entre o grupo das classes C e o grupo Ω das unidades positivas modulo as unidades circulatórias (Teorema 2). Todos os subcorpos reais dos corpos p-ciclotômicos satisfazem essa condição e nós provamos que, para tais corpos, cada anulador do p-Sylow subgrupo Ω_p de Ω é também um anulador de p-Sylow subgrupo C_p de C. Quando $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ este resultado pode também ser obtido a partir de um de Mazur e Wiles (veja a referência [5] página 146). Uma aplicação ao primeiro caso do último teorema de Fermat é dada na Seção (4) (Teorema 3). La se estende para expoentes primos quaisquer, um resultado de [7], Parte II.

1. FATORAÇÃO DE CERTOS IDEAIS PRINCIPAIS

Seja q um primo impar fixo que se decompõe completamente em A e θ, s, τ como acima. Sejam $f(X)$ um elemento fixo de $V(X)$, $\varepsilon = f(\theta)$ e $\alpha \in A[\theta] \setminus \{0\}$ tais que $\tau(\alpha) = \varepsilon\alpha$. Denotemos por (α) o ideal principal $\alpha A[\theta]$. Temos que $\tau(\alpha) = (\alpha)$.

Seja Q um ideal primo de A acima de q e $\mathcal{B}$ o único ideal primo de $A[\theta]$ acima de Q. Como $K \cap \mathbb{Q}(\theta) = \mathbb{Q}$, cada $\sigma \in G = Gal(K/\mathbb{Q})$ pode ser estendido, numa única maneira, a um $\mathbb{Q}(\theta)$-automorfismo de $K(\theta)$, denotamos esta extensão ainda por σ e chamamos G' ao conjunto de todas tais extensões de elementos de G.

Temos as seguintes decomposições em ideais primos:

$$qA = \prod_{\sigma \in G} \sigma(Q), \quad q\mathbb{Z}[\theta] = (\theta - 1)^{q-1}\mathbb{Z}[\theta],$$

$$qA[\theta] = \prod_{\sigma \in G'} \sigma(\mathcal{B})^{q-1}, \quad QA[\theta] = \mathcal{B}^{q-1}, \quad (\theta - 1)A[\theta] = \prod_{\sigma \in G'} \sigma(\mathcal{B}).$$

Como os primos acima de q são os únicos primos que se ramificam na extensão $K[\theta]/K$ e como $\tau(\alpha) = (\alpha)$ temos que

$$(1) \qquad (\alpha) = \mathcal{D} \prod_{\sigma \in G'} \sigma^{-1}(\mathcal{B})^{r_\sigma},$$

onde $r_\sigma \in \mathbb{Z}$ e $\mathcal{D}$ é um ideal de $A[\theta]$ relativamente primo com

q e que estende um ideal de A, i.e. $\mathcal{D} = (\mathcal{D} \cap A)\, A[\theta]$ (logo veremos a vantagem de escrever $\sigma^{-1}(\mathcal{B})^{r_\sigma}$ em vez de $\sigma(\mathcal{B})^{r_\sigma}$ em (1)).

Vamos determinar os expoentes r_σ, em (1), modulo $q-1$. O seguinte fato conhecido será usado para este propósito.

LEMA. Seja L um corpo numérico, R seu anel de inteiros, P um ideal primo de R e v a valorização correspondente a P. Se $\gamma \in L$ é tal que $v(\gamma) = 0$, então existem $\lambda \in R$ e $c \in \mathbb{Z}$ não divisíveis por P tais que $\gamma = \frac{\lambda}{c}$.

Sejam $\sigma \in G'$ e r_σ como em (1). Como $\tau(\alpha) = \varepsilon\alpha$, podemos escrever

$$(2) \qquad \left(\frac{\theta^s - 1}{\theta - 1}\right)^{r_\sigma} \tau(\gamma) = \varepsilon\gamma,$$

onde $\gamma = \dfrac{\alpha}{(\theta-1)^{r_\sigma}}$. Pelo lema acima, existem $\lambda \in A[\theta]$ e $c \in \mathbb{Z}$ não divisíveis por $\sigma^{-1}(\mathcal{B})$ tais que $\gamma = \frac{\lambda}{c}$. Claramente $\tau(\lambda) \equiv \lambda \bmod \theta - 1$, portanto $\tau(\gamma) \equiv \gamma \not\equiv 0 \bmod \sigma^{-1}(\mathcal{B})$.

Assim podemos cancelar $\tau(\gamma)$ e γ, em (2), modulo $\sigma^{-1}(\mathcal{B})$ e concluir que

$$s^{r_\sigma} \equiv \left(\frac{\theta^s - 1}{\theta - 1}\right)^{r_\sigma} \equiv \varepsilon \equiv f(\theta) \equiv f(1) \bmod \sigma^{-1}(\mathcal{B}).$$

Portanto,

$$s^{r_\sigma} \equiv \sigma(f(1)) \bmod \mathcal{B}$$

e finalmente, como $\mathcal{B} \cap A = Q$, temos

$$s^{r_\sigma} \equiv \sigma(f(1)) \bmod Q.$$

Resumimos os resultados desta seção na seguinte proposição.

PROPOSIÇÃO 2. Se $f(X) \in V(X)$, existe $\alpha \in A[\theta] \setminus \{0\}$ tal que $\tau(\alpha) = f(\theta)\alpha$. Para cada um de tais elementos α temos (em $A[\theta]$)

$$(\alpha) = \mathcal{D} \prod_{\sigma \in G'} \sigma^{-1}(\mathcal{B})^{r_\sigma},$$

onde $\mathcal{D}$ é um ideal primo com q e tal que $\mathcal{D} = (\mathcal{D} \cap A)\, A[\theta]$, e os r_σ, $\sigma \in G'$, são inteiros (determinados modulo $q-1$) tais que $s^{r_\sigma} \equiv \sigma(f(1)) \bmod Q$.

OBSERVAÇÃO. Segue da Proposição (2) que

$$(N_{K(\theta)/K}(\alpha)) = (\mathcal{D} \cap A)^{q-1} \prod_{\sigma \in G} \sigma^{-1}(Q)^{r_\sigma}.$$

Em particular, se o número das classes h de K divide

$q-1$, o ideal $\prod_{\sigma\in G} \sigma^{-1}(Q)^{r_\sigma}$ é principal.

Mais geralmente, seja e um expoente do grupo das classes de ideais de K, se $e = ab$ com a, b inteiros e se $a|q-1$ então o ideal

$$(\prod_{\sigma\in G} \sigma^{-1}(Q)^{r_\sigma})^b$$

é principal.

Para um elemento fixo $f(X) \in V(X)$, o conjunto dos $\alpha \in A[\theta]$ tais que $\tau(\alpha) = f(\theta)\alpha$ é um A-modulo não nulo M. Existe um conjunto natural $\{F_o, F_1, \ldots, F_{q-1}\}$ de geradores de M que satisfazem a relação

$$F_o + \theta F_1 + \ldots + \theta^{q-1} F_{q-1} = q,$$

esperamos estudar M e seus geradores em outro trabalho. A principal pergunta nesta linha é se algum elemento $\alpha \in M$ é um divisor de q.

2. CLASSES DE IDEAIS E UNIDADES. UM TEOREMA LOCAL-GLOBAL

Seja $f(X) \in V(X)$ fixado, escrevamos $\delta = f(1)$, esta é uma unidade circulatória positiva de A. Supomos que $\delta \neq 1$.

Para cada ideal Q de A, sobre um primo racional q que

se decompõe completamente em A, sejam $\theta = \theta_Q$ uma raiz q-ésima primitiva da unidade e $s = s_Q$ uma raiz primitiva modulo q. Se $\sigma \in G$, seja $r_\sigma = r_\sigma(Q)$ como na Proposição (2). Temos $s^{r_\sigma(Q)} \equiv \sigma(\delta) \bmod Q$.

Para cada unidade ε de A, $\varepsilon \neq \pm 1$, definimos o número $\phi(\varepsilon)$ como sendo o maior inteiro k tal que $\varepsilon = \mu^k$ para alguma unidade μ de A. Temos que $\phi(\sigma(\varepsilon)) = \phi(\varepsilon)$ para todo $\sigma \in G$.

PROPOSIÇÃO 3. Sejam Q como acima e $\sigma \in G$, então

$$\mathrm{mdc}(\phi(\delta), q-1) \mid r_\sigma(Q).$$

DEMONSTRAÇÃO. Seja μ uma unidade de A tal que $\delta = \mu^{\phi(\delta)}$. Existe um inteiro c tal que $\sigma(\mu) \equiv c \bmod Q$ (pois Q é de primeiro grau). Temos

$$s^{r_\sigma} \equiv \sigma(\delta) = \sigma(\mu)^{\phi(\delta)} \equiv c^{\phi(\delta)} \bmod Q,$$

portanto $s^{r_\sigma} \equiv c^{\phi(\delta)} \bmod q$. e a proposição segue.

Como na Seção (1), sejam $\tau = \tau_Q$ o K-automorfismo de $K(\theta)$ tal que $\tau(\theta) = \theta^s$, e $\alpha = \alpha_Q \in A[\theta] \setminus \{0\}$ tal que $\tau(\alpha) = f(\theta)\alpha$. Pelas Proposições (2) e (3) temos em A as seguintes fatorações:

$$(3) \qquad (N_\theta(\alpha_Q)) = \mathfrak{P}^{q-1} \prod_{\sigma \in G} \sigma^{-1}(Q)^{r_\sigma(Q)} = \mathfrak{E}^{\mathrm{mdc}(\phi(\delta), q-1)}$$

para alguns ideais $\mathcal{D}$ e $\mathfrak{E}$ de A.

Agora consideremos os ideais Q como percorrendo por uma classe de ideais para obter uma especie de recíproca da Proposição (3). Sejam E uma classe de ideais de K e a um inteiro positivo. Definimos E_a como o conjunto de todos os ideais primos de E que estão acima primos racionais (positivos) q que se decompõem completamente em K e tais que $q \equiv 1 \bmod a$.

Se E e a são tais que E_a é não vazio e $\sigma \in G$, denotamos por $\eta = \eta(\delta, E, a, \sigma)$ o maior divisor comum de a e de todos os $r_\sigma(Q)$ tais que $Q \in E_a$ (note que o $mdc(r_\sigma(Q), a)$ não depende da raiz primitiva módulo q, s_Q escolhida, pois $a \mid q-1$).

A seguinte proposição é uma consequência das definições.

PROPOSIÇÃO 4. Sejam $\sigma \in G$ e E, a, η como acima, então para todo $Q \in E_a$ existe $\beta_Q \in \mathbb{Z}$ tal que $\sigma(\delta) \equiv \beta_Q^\eta \bmod Q$.

Nosso principal objetivo nesta seção é provar o seguinte:

TEOREMA 1. Se E_a é não vazio, então para todo $\sigma \in G$ temos que $\eta(\delta, E, a, \sigma)$ divide $2\phi(\delta)$.

Este teorema é uma consequência da Proposição (4), mas para prova-lo temos que usar métodos mais poderosos (principalmente o Teorema de Densidade de Tchebotarev). A maior parte das idéias envolvidas na prova foram sugeridas para mim pelo

Professor Lawrence Washington. O ponto crucial foi resolvido pelo Professor René Schoof que demonstrou o seguinte resultado geral:

TEOREMA. Sejam K um corpo numérico e L/K uma extensão finita. Seja f um divisor de K e suponha que existe uma classe de ideais generalizada $E \in I_f/P_f$ tal que sempre que um primo P de K está em E então P se decompõe completamente em L/K. Então L/K é uma extensão abeliana. (Podemos restringir a nossa atenção a P de grau absoluto 1, e também permitir um número finito de primos excepcionais P).

Não damos aqui a prova deste teorema, porque nos realmente precisamos do seguinte resultado menos geral, porém mais forte (a prova inclui pequenas modificações dos argumentos do Professor Schoof):

PROPOSIÇÃO 5. Sejam K um corpo numérico abeliano real, A seu anel de inteiros, δ uma unidade positiva de A, E uma classe de ideais de K, a um inteiro positivo e E_a o conjunto dos ideais primos de primeiro grau pertencentes a E e que dividem primos racionais (positivos) $q \equiv 1 \bmod a$ (permitimos que um número finito de tais ideais não pertença a E_a).

Seja c um divisor de a. Suponha que E_a é não vazio e que para todo $Q \in E_a$ existe $\beta_Q \in A$ tal que $\delta \equiv \beta_Q^c \bmod Q$.

Então existe $\beta \in A$ tal que:

$$\delta = \beta^c \quad \text{se} \quad c \quad \text{é impar e}$$

$$\delta = \beta^{c/2} \quad \text{se} \quad c \quad \text{é par.}$$

OBSERVAÇÃO. Podemos obter $\delta = \beta^c$ também quando c é par em muitas situações, mas este é um assunto delicado (em relação com isto ver [2] Teorema (1), Capítulo (9) e Teorema (1), Capítulo (10)).

DEMONSTRAÇÃO. (Se n é um inteiro positivo denotamos por ζ_n uma raiz n-ésima primitiva da unidade). Seja $\nu = \sqrt[c]{\delta}$ a raiz positiva c-ésima de δ e seja L o fecho normal de $K(\nu)$ sobre K. Seja $p(X)$ o polinômio irredutível de ν sobre K, então $p(X) \mid X^c - \delta$ e L é o corpo de decomposição de $p(X)$ sobre K. Portanto $L = K(\nu, \zeta_e)$ para algum $e \mid c$.

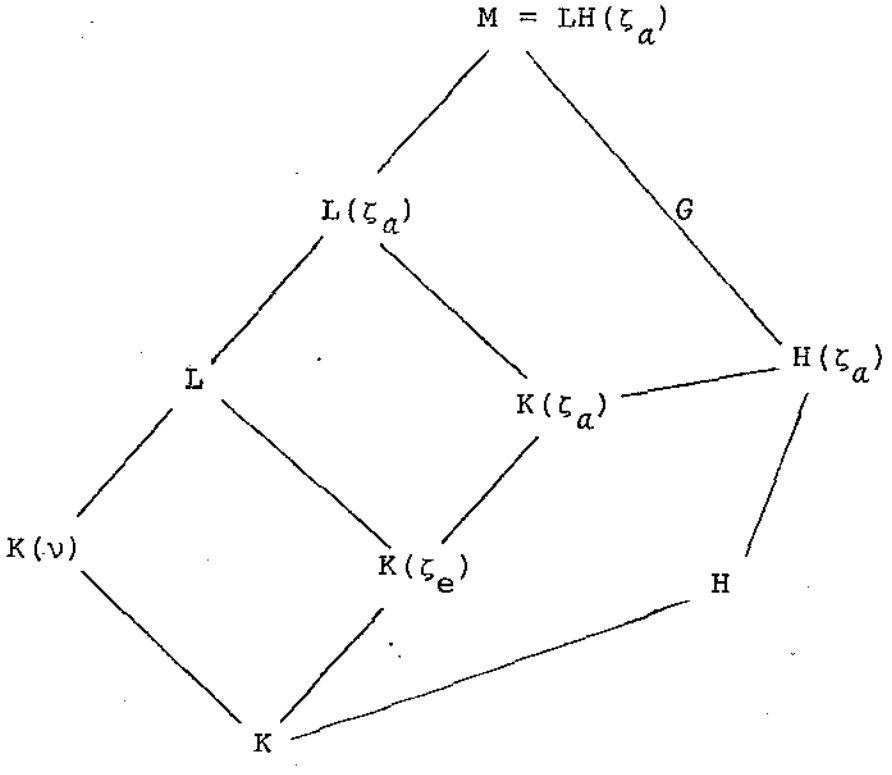
Seja H o corpo de classes de Hilbert de K. Vamos provar que $L \subseteq H(\zeta_a)$. A proposição segue disto porque então teremos que L/K e $K(\nu)/K$ são abelianas (pois $H(\zeta_a)/K$ é abeliana). Portanto $L = K(\nu)$, $\zeta_e \in K(\nu) \subseteq \mathbb{R}$, $\zeta_e = \pm 1$ e $p(X) = X - \nu$ se c é impar, $p(X) = X - \nu$ ou $p(X) = X^2 - \nu^2$ se c é par. No primeiro caso (c impar) tomamos $\beta = \nu$, no outro caso tomamos $\beta = \nu^2$.

Para provar que $L \subseteq H(\zeta_a)$ observemos primeiro que cada

$Q \in E_a$ se decompõe completamente em $K(\nu)$. De fato, $p(X) \mid X^c - \delta$ e o polinômio $X^c - \overline{\delta} = X^c - \overline{\beta}_Q^c \in A/Q[X]$ se decompõe em fatores lineares porque o corpo A/Q contém as raizes c-ésimas da unidade (pois $c \mid a$ e $a \mid q - 1 = \#(A/Q)^*$). Como também Q não divide o discriminante de ν sobre K concluímos que Q se decompõe completamente em $K(\nu)$ (referência [3]).

Portanto cada $Q \in E_a$ se decompõe completamente no fecho normal L.

O grupo das classes de ideais de K é isomorfo a $Gal(H/K)$ via a aplicaçao de Artin. Seja $\varphi \in Gal(H/K)$ a aplicação que corresponde a E. Seja $M = LH(\zeta_a)$ (ver o diagrama).



Por hipótese existe $Q_o \in E_a$, como $\varphi = F_{Q_o}$ é o automorfismos de Frobenius para Q_o e como Q_o se decompõe completamente em $K(\zeta_a)$ temos que a restrição de φ a $K(\zeta_a) \cap H$ é a aplicação idêntica, portanto podemos estender φ a um automorfismo $\tilde{\varphi}$ de M tal que $\tilde{\varphi}(\zeta_a) = \zeta_a$.

Seja $G = \mathrm{Gal}(M/H(\zeta_a))$ e seja $g \in \tilde{\varphi}G$. Pelo Teorema de Densidade de Tchebotarev (referência [3]) existem infinitos ideais primos P de M tais que o automorfismo de Frobenius F_P para $M/K(\zeta_a)$ é g e tal que o primo P' de $K(\zeta_a)$ abaixo de P é de grau absoluto 1.

Como a restrição $F_P\big|_H = g\big|_H = \varphi$ é o automorfismo de Frobenius F_Q para $Q = P \cap A$, devemos ter $Q \in E$.

Como P' é grau absoluto 1, devemos ter ambos: que o mesmo vale para Q e que o primo racional q abaixo de Q é congruente com 1 módulo a. Assim $Q = P \cap A \in E_a$ (escolha P de modo a evitar as finitas exceções permitidas).

Assim Q se decompõe completamente em L e logo $F_P\big|_L = id_L$. Portanto $g = F_P \in \mathrm{Gal}(M/L)$.

Portanto $\tilde{\varphi}G \subseteq \mathrm{Gal}(M/L)$, $\tilde{\varphi} \in \mathrm{Gal}(M/L)$ e finalmente $G \subseteq \mathrm{Gal}(M/L)$, o qual implica que $L \subseteq H(\zeta_a)$ como queríamos.

O Teorema (1) segue das Proposições (4) e (5), e do seguinte fato.

LEMA. Seja $\delta \in U$, se $\delta = \beta^c$ com $\beta \in A$, então $c|\phi(\delta)$.

DEMONSTRAÇÃO. Escrevemos $\phi = \phi(\delta)$. Seja $\nu \in A$ tal que $\delta = \nu^{\phi}$. Sejam d o maior divisor comum de c e ϕ, e $x, y \in \mathbb{Z}$ tais que $xc + y\phi = d$, então $\delta = (\nu^x \beta^y)^{[c,\phi]}$, onde $[c,\phi]$ é o mínimo múltiplo comum de c e ϕ. Por definição de ϕ temos então que $[c,\phi] \leq \phi$, portanto $c|\phi$.

3. UMA RELAÇÃO ENTRE O GRUPO DAS CLASSES DE IDEAIS E O GRUPO DAS UNIDADES DE K

Conservamos as notações das seções anteriores, denotamos por C o grupo das classes de ideais de K. Sejam $f(X) \in V(X)$, $\delta = f(1)$ e $E \in C$. Seja a um inteiro positivo tal que E_a é não vazio. Da Proposição (2) (ver a observação que segue a essa proposição) concluímos que se $Q \in E_a$, então

$$\mathfrak{D}^a \prod_{\sigma \in G} \sigma^{-1}(Q)^{r_\sigma} = (\beta) \tag{4}$$

para algum $\beta \in A$ e algum ideal $\mathfrak{D}$ de A, onde os $r_\sigma = r_\sigma(Q)$ são inteiros tais que

$$s^{r_\sigma} \equiv \sigma(\delta) \bmod Q.$$

Denotemos por $\gamma = \gamma(Q)$ o elemento $\sum_{\sigma \in G} r_\sigma(Q)\sigma^{-1}$ do anel de

grupo $\mathbb{Z}[G]$ e por F a inversa da classe de $\mathcal{D}$ em C. Por (4) temos

$$E^{\gamma} = F^{a}. \tag{5}$$

Desta maneira, estudando casos nos quais $F^{a} = 1$ (o elemento unitário de C), vamos obter anuladores de certos subgrupos de C. Estes anuladores estão relacionados com a estrutura do grupo das unidades como provamos a seguir.

Denotemos por $\phi(\delta,a)$ o maior divisor comum de a e $\phi(\delta)$ (se $\delta = 1$ façamos $\phi(\delta,a) = a$), e como antes, se $\sigma \in G$ seja $\eta(\delta,E,a,\sigma)$ o maior divisor comum de a e de todos os $r_{\sigma}(Q)$ tais que $Q \in E_{a}$, então

$$\omega\eta(\delta,E,a,\sigma) = \phi(\delta,a), \tag{6}$$

onde $\omega \in \{1, \frac{1}{2}\}$.

De fato, da Proposição (3) concluímos que $\phi(\delta,a) \mid \eta(\delta,E,a,\sigma)$ e o Teorema (1) implica que $\eta(\delta,E,a,\sigma) \mid 2\phi(\delta,a)$.

Consideremos mais uma vez a fórmula (5), temos que $F^{a} = 1$ em vários casos (ver por exemplo a Proposição (7)), para estes casos (se E_{a} é não vazio) as fórmulas (5) e (6) dão uma relação entre anuladores de E e unidades. Nós provaremos que esta relação aparentemente complicada entre C e U fica simples em

muitas situações importantes. A seguinte proposição garante que os p-Sylow subgrupos dos subcorpos reais dos corpos p^n-ciclotômicos tem as propriedades desejadas.

PROPOSIÇÃO 6. Se $K \subseteq \mathbb{Q}(\zeta_{p^n}) \cap \mathbb{R}$ e $a = p^k$ para algum primo p e alguns inteiros positivos n e k, então E_a e não vazio para todo $E \in C$.

DEMONSTRAÇÃO. Seja $r = \sup\{n,k\}$, temos que $K \subseteq \mathbb{Q}(\zeta_{p^r})$. Como o primo acima de p se ramifica completamente na extensão $\mathbb{Q}(\zeta_{p^r})/K$, a aplicação norma é uma aplicação sobrejetora do grupo das classes de ideais de $\mathbb{Q}(\zeta_{p^r})$ sobre C (ver referência [5], Teorema 10.1). Seja $E \in C$, denotemos por N a aplicação norma e por E' uma classe de ideais de $\mathbb{Q}(\zeta_{p^r})$ tal que $E = N(E')$.

Sabemos que existem infinitos ideais primos de $\mathbb{Q}(\zeta_{p^r})$ de grau absoluto 1 pertencendo a E', se Q' é um tal ideal afirmamos que $N(Q') \in E_a$. De fato, claramente o ideal $Q = N(Q')$ é um ideal primo de A de grau absoluto 1, pertencente a E. Seja q o primo racional abaixo de Q, como Q' é de primeiro grau temos que $q \equiv 1 \bmod p^r$, donde $q \equiv 1 \bmod p^k = a$. Portanto $Q \in E_a$ como foi afirmado.

A Proposição (7) seguinte é válida para corpos numéricos abelianos reais K arbitrarios. Se também $K \subseteq \mathbb{Q}(\zeta_{p^n})$, nos fornece um conjunto não vazio de anuladores para cada classe do

p-Sylow subgrupo de C, devido à Proposição (6).

PROPOSIÇÃO 7. Seja ℓ um primo. Seja ℓ^ν um expoente do ℓ-Sylow subgrupo C_ℓ de C. Se $E \in C_\ell$, $Q \in E_{\ell^\nu}$ e se δ e os $r_\sigma = r_\sigma(Q)$ $(\sigma \in G)$ são como antes, então

$$\prod_{\sigma \in G} \sigma^{-1}(E)^{r_\sigma} = 1.$$

DEMONSTRAÇÃO. Temos, por (4), que

$$\prod_{\sigma \in G} \sigma^{-1}(E)^{r_\sigma} = F^{\ell^\nu}$$

para algum $F \in C$. Claramente $F \in C_\ell$, portanto $F^{\ell^\nu} = 1$ e a proposição segue.

Temos estado trabalhando com unidades arbitrarias $\delta = f(1) \in V(1)$. As congruências $s^{r_\sigma} \equiv \sigma(\delta) \bmod Q$ da Proposição (2), sugerem que certas δ "bem comportadas" com respeito a conjugações devem ser especialmente consideradas a fim de obtermos um conjunto de expoentes r_σ com o qual possamos trabalhar. O objetivo é obter anuladores eficientes de subgrupos de C, podemos (e faremos) restringimos a considerar os ℓ-Sylow subgrupos C_ℓ.

PROPOSIÇÃO 8. Sejam ℓ um número primo e $a = \ell^\nu$ um expoente de C_ℓ. Suponhamos que $\delta = f(1)$ (com $f(X) \in V(X)$) é uma unidade

tal que para todo $\sigma \in G$ existam um inteiro c_σ relativamente primo com a, e uma unidade ε_σ de A tais que

$$\sigma(\delta) = \delta^{c_\sigma} \varepsilon_\sigma^a . \tag{7}$$

Seja $E \in \mathcal{C}_\ell$. Se E_a é não vazio, então

$$\Big(\prod_{\sigma \in G} \sigma^{-1}(E)^{c_\sigma} \Big)^{2\phi(\delta,a)} = 1.$$

DEMONSTRAÇÃO. Sejam $Q \in E_a$, q o primo racional abaixo de Q e s uma raiz primitiva módulo q. Como Q é de primeiro grau, existe um inteiro $d = d(Q)$ tal que $\delta \equiv s^d \bmod Q$.

Das Proposições (7) e (2) concluímos que

$$\prod_{\sigma \in G} \sigma^{-1}(E)^{r_\sigma} = 1,$$

onde $s^{r_\sigma} \equiv \sigma(\delta) = \delta^{c_\sigma} \varepsilon_\sigma^a \equiv s^{dc_\sigma + j_\sigma a} \bmod Q$ para algum inteiro j_σ. Como $a \mid q-1$ temos que $r_\sigma \equiv dc_\sigma \bmod a$ e, como $E^a = 1$, concluímos que

$$\Big(\prod_{\sigma \in G} \sigma^{-1}(E)^{c_\sigma} \Big)^{d(Q)} = 1. \tag{8}$$

É claro que, dado $\sigma \in G$, $\eta = \eta(\delta, E, a, \sigma)$ é também o maior divisor comum de a e de todos os $d(Q)$ tais que $Q \in E_a$

(porque c_σ e a são relativamente primos). Como a fórmula (8) acima vale para todo $Q \in E_a$ e como $E^a = 1$ temos que

$$\Big(\prod_{\sigma \in G} \sigma^{-1}(E)^{c_\sigma}\Big)^\eta = 1$$

e a Proposição segue da fórmula (6).

A Proposição (8) nos mostra a conveniência de buscar unidades $\delta \in V(l)$ que satisfazem (7) e tais que $\phi(\delta, a)$ é mínimo. Vamos trabalhar nessa direção.

Sejam ℓ um primo e ℓ^μ um expoente do ℓ-Sylow subgrupo Ω_ℓ de $\Omega = U/V(l)$. Dada a sequência $L = \{c_\sigma\}_{\sigma \in G}$ de inteiros c_σ relativamente primos com $a = \ell^\mu$ (um expoente de C_ℓ) definimos $S_a = S_{a,L} = \{\varepsilon \in U : \varepsilon^{\sigma - c_\sigma} \in U^a$ para todo $\sigma \in G$ e $\varepsilon^{\ell^\mu} \in V(l)\}$. Este é um subgrupo de U. Se S' é um subgrupo de S_a, então $S'/S' \cap V(l)$ é canonicamente isomorfo a um subgrupo de Ω_ℓ. Chamamos $I(S')$ ao menor inteiro positivo que é um expoente para $S'/S' \cap V(l)$, $I(S')$ é uma potência de ℓ. Por último definimos

$$\phi_a(S') = \inf\{\phi(\varepsilon, a) : \varepsilon \in S'\}.$$

PROPOSIÇÃO 9. Dados L, $a = \ell^\mu$ e $S_a = S_{a,L}$ como acima, temos que

$$\phi_a(S_a \cap V(l)) \mid \phi_a(S')I(S'),$$

para todos os subgrupos S' de S_a.

DEMONSTRAÇÃO. Seja $\varepsilon \in S'$ tal que $\phi_a(S') = \phi(\varepsilon,a)$, seja $\delta = \varepsilon^{I(S')}$, então $\delta \in S_a \cap V(1)$ e (se $\varepsilon \neq 1$)

$$\phi(\delta) = I(S')\phi(\varepsilon),$$

portanto $\phi(\delta,a) \mid I(S')\phi(\varepsilon,a)$.

Como $\phi_a(S_a \cap V(1)) \leq \phi(\delta,a)$ e como ambos números são potências de ℓ, o primeiro divide o segundo e a proposição segue.

PROPOSIÇÃO 10. Sejam ℓ um número primo, $a = \ell^\nu$ um expoente de C_ℓ, $L = \{c_\sigma\}_{\sigma \in G}$ uma sequência de inteiros relativamente primos com a, $\lambda = \sum_{\sigma \in G} c_\sigma \sigma^{-1}$, e $S_a = S_{a,L}$ como acima. Se $E \in C_\ell$ é tal que E_a é não vazio, então para todos os subgrupos S' de S_a,

$$E^{2\phi_a(S')I(S')\lambda} = 1.$$

DEMONSTRAÇÃO. Segue da Proposição (8) que

$$E^{2\phi_a(S_a \cap V(1))\lambda} = 1,$$

agora usamos a Proposição (9) para obter o resultado.

Estamos procurando conjuntos L e unidades $\varepsilon \in S_{a,L}$ adequados tais que $\phi(\varepsilon,a)$ seja mínimo. É conveniênte descrever estas coisas em termos de matrizes, como segue:

Seja $\varepsilon_1, \ldots, \varepsilon_r$ $(r = \#\, G - 1)$ um sistema fundamental de unidades de A. Para $\sigma \in G$ e $1 \leq j \leq r$, escrevemos

$$\varepsilon_j^{\sigma} = \pm \prod_{i=1}^{r} \varepsilon_i^{y_{ij}},$$

com $y_{ij} = y_{ij}(\sigma)$ inteiros. Definimos

$$Y_{\sigma} = [y_{ij}(\sigma)]_{1 \leq i,j \leq r}.$$

Se $\gamma = \pm\, \varepsilon_1^{x_1} \varepsilon_2^{x_2} \ldots \varepsilon_r^{x_r}$, então $\gamma^{\sigma} = \pm\, \varepsilon_1^{z_1} \varepsilon_2^{z_2} \ldots \varepsilon_r^{z_r}$, onde

$$\begin{pmatrix} z_1 \\ z_2 \\ \cdot \\ \cdot \\ \cdot \\ z_r \end{pmatrix} = Y_{\sigma} \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_r \end{pmatrix}.$$

Como $\varepsilon_1^{\sigma}, \varepsilon_2^{\sigma}, \ldots, \varepsilon_r^{\sigma}$ é também um sistema fundamental de unidades, temos que $\det Y_{\sigma} = \pm 1$.

Seja H o grupo das matrizes $r \times r$ com entradas em $\mathbb{Z}$ e determinante ± 1 (matrizes unimodulares). As seguintes afirmações

são fáceis de provar:

A aplicação $\sigma \mapsto Y_\sigma$ é um homomorfismo injetivo de grupos de G em H (assim, $Y_{\sigma_2} Y_{\sigma_1} = Y_{\sigma_1} Y_{\sigma_2} = Y_{\sigma_1\sigma_2}$ para todos os $\sigma_1, \sigma_2 \in G$). A classe de conjugação de Y_σ em H não depende do sistema fundamental de unidades particular escolhido para definir esta matriz. Também $\sum_{\sigma \in G} Y_\sigma = 0$.

Sejam L e $S_{a,L}$ como acima, uma unidade $\varepsilon = \pm \varepsilon_1^{x_1} \varepsilon_2^{x_2} \dots \varepsilon_r^{x_r}$ pertence a $S_{a,L}$ se e somente se $\varepsilon^{\ell^\mu} \in V(1)$ e

$$Y_\sigma X \equiv c_\sigma X \bmod a \quad \text{para todo} \quad \sigma \in G,$$

onde X é o vetor coluna com coordenadas $x_1, \dots, x_r$.

O número $\phi(\varepsilon, a)$ é igual à maior potência de ℓ que divide a e o vetor X.

PROPOSIÇÃO 11.

1) Seja ℓ um número primo, as seguintes condições em K e ℓ são equivalentes:

(a) Se $\gamma = \sum_{\sigma \in G} d_\sigma \sigma \in \mathbb{Z}[G]$ é tal que $\pm \varepsilon^\gamma \in U^\ell$ para todo $\varepsilon \in U$, então $d_\sigma \equiv d_\tau \bmod \ell$ para todo $\sigma, \tau \in G$.

(b) As matrizes Y_σ, $\sigma \in G$, $\sigma \neq id_G$ são linearmente

independentes módulo ℓ (para algum sistema fundamental de unidades escolhido).

2) Se K satisfaz as condições acima para o primo ℓ, então todos os subcorpos de K também as satisfazem.

DEMONSTRAÇÃO. A parte (1) é clara. Para provar a parte (2) suponhamos que K e ℓ satisfazem as condições da parte (1). Sejam L um subcorpo de K e G' o grupo de Galois de $L/\mathbb{Q}$. Suponhamos que $\gamma_o = \sum_{\sigma' \in G'} e_{\sigma,\sigma'} \in \mathbb{Z}[G]$ é tal que $\pm \varepsilon^{\gamma_o} \in U'^{\ell}$ para todo $\varepsilon \in U' = U \cap L$. Para cada $\sigma' \in G'$, seja $\sigma \in G$ tal que $\sigma' = \sigma|_L$. Se Δ é o grupo de Galois de K/L e

$$\gamma = \left(\sum_{\sigma' \in G'} e_{\sigma,\sigma}\right)\left(\sum_{\tau \in \Delta} \tau\right) = \sum_{\sigma',\tau} e_{\sigma,\sigma\tau},$$

então $\pm \varepsilon^{\gamma} \in U^{\ell}$ para todo $\varepsilon \in U$. Portanto $e_{\sigma_1'} \equiv e_{\sigma_2'} \bmod \ell$ para todo $\sigma_1', \sigma_2' \in G$, como queriamos provar.

Agora, seja ℓ um primo que divide o número das classes de K e, como antes, seja $a = \ell^{\nu}$ um expoente de C_{ℓ}. Seja $\psi : G \to (\mathbb{Z}/a\mathbb{Z})^*$ um homomorfismo de grupos e para cada $\sigma \in G$ escolhamos um inteiro c_{σ} na classe $\psi(\sigma)$. Temos $c_{\sigma\tau} \equiv c_{\sigma} c_{\tau} \bmod a$ para todo $\sigma, \tau \in G$. Chamemos $L = \{c_{\sigma}\}_{\sigma \in G}$. Seja $M_L = \sum_{\sigma \in G} c_{\sigma} Y_{\sigma}^{-1}$. Temos que

$$Y_\sigma M_L \equiv c_\sigma M_L \bmod a \quad \text{para todo} \quad \sigma \in G.$$

Se K e ℓ satisfazem as condições equivalentes da Proposição (11) e se ψ não é o homomorfismo trivial (i.e. se $c_\sigma \not\equiv 1 \bmod a$ para algum $\sigma \in G$), então $M_L \not\equiv 0 \bmod \ell$. Assim, alguma coluna de M_L, digamos a i-ésima, não é divisível por ℓ. Seja E_i o vetor coluna com i-ésima coordenada 1 e j-ésima coordenada 0 se $j \neq i$. Se o número das classes de K é $\ell^t k$ com $\ell \nmid k$, a unidade ε_i^k é tal que $(\varepsilon_i^k)^{\ell^\mu} \in V(1)$. Por outra parte temos

$$Y_\sigma M_L(kE_i) \equiv c_\sigma M_L(kE_i) \bmod a$$

e

$$M_L(kE_i) = kM_L E_i \not\equiv 0 \bmod \ell.$$

Isto corresponde à existência de uma unidade ε tal que $\varepsilon^{\ell^\mu} \in V(1)$ e tal que $\phi(\varepsilon^\lambda, a) = 1$, onde $\lambda = \sum_{\sigma \in G} c_\sigma \sigma^{-1}$. Definamos $T = \{\varepsilon \in U : \varepsilon^{\ell^\mu} \in V(1)\}$. Nós acabamos de provar que, sob as condições da Proposição (11), $\phi_a(T^\lambda) = 1$ (note que $T^\lambda \subseteq S_{a,L}$).

Temos também que

$$\frac{T^\lambda}{T^\lambda \cap V(1)} \simeq \Omega_p^\lambda,$$

portanto $I(T^\lambda)$ é igual ao menor expoente de Ω_p^λ. Destes fatos

e da Proposição (10) concluímos o seguinte:

TEOREMA 2. Sejam ℓ um primo que divide o número das classes de K, $a = \ell^{\nu}$ um expoente de C_{ℓ}, c_{σ}, $\sigma \in G$ inteiros relativamente primos com a tais que $c_{\sigma\tau} \equiv c_{\sigma}c_{\tau} \bmod a$ para todo $\sigma, \tau \in G$ e $\lambda = \sum_{\sigma \in G} c_{\sigma}\sigma^{-1}$. Suponhamos que K e ℓ satisfazem as condições equivalentes da Proposição (11). Chamemos ρ ao menor expoente de Ω_{ℓ}^{λ}. Então, se $E \in C_{\ell}$ é tal que E_a é não vazio, temos que

$$E^{2\rho\lambda} = 1.$$

Eu não sei se subcorpos reais arbitrários de $\mathbb{Q}(\zeta_{p^e})$ (p primo, $e \geq 1$) satisfazem as condições da Proposição (11) para $\ell = p$, quando isto ocorre podemos concluir do Teorema (2) e da Proposição (6) que duas vezes o menor expoente de Ω_p^{λ} é um expoente de C_p^{λ} para λ como no Teorema (2). Ora, se $e = 1$ todas as coisas funcionam e temos o seguinte resultado:

COROLÁRIO. Se $K \subseteq \mathbb{Q}(\zeta_p) \cap \mathbb{R}$, onde p é um primo impar, então todo anulador (em $\mathbb{Z}[G]$) de Ω_p, anula também C_p.

DEMONSTRAÇÃO. Sejam $d = \# G$, $f = \frac{p-1}{d}$ (note que f é par pois $K \subseteq \mathbb{R}$), g uma raiz primitiva $\bmod p$ e σ um gerador de G. Sejam p^{ν}, $\nu \geq 1$ um expoente de ambos C_p e Ω_p, e

$c = g^{fp^{\nu-1}}$, note que $c^d \equiv 1 \bmod p^\nu$.

Para $0 \leq k \leq d-1$ definimos

$$\lambda_k = \sum_{j=0}^{d-1} c^{kj}\sigma^{-j},$$

temos que $\sigma^i\lambda_k \equiv c^{ki}\lambda_k \bmod p^\nu$ para todos os inteiros i, também

$$\sum_{k=0}^{d-1} \lambda_k \equiv d \bmod p^\nu.$$

Vamos provar que o corpo K satisfaz as condições da Proposição (11) para $\ell = p$. Pela parte (2) da Proposição (11) é suficiente provar que o corpo $\mathbb{Q}(\zeta + \zeta^{-1})$, onde $\zeta = \zeta_p$, satisfaz essas condições equivalentes. Afirmamos que para este corpo (para o qual $d = \frac{p-1}{2}$) o polinômio $P(X) = 1 + x + \ldots + x^{d-1}$ é o polinômio minimal de $Y_\sigma \bmod p$. De fato, como 1 não é um autovalor de Y_σ e com $Y_\sigma^d = I$, temos que $P(Y_\sigma) = 0$. Por outra parte $P(X) \equiv (x - c)(x - c^2) \ldots (x - c^{d-1}) \bmod p$, e $c, c^2, \ldots, c^{d-1}$ são dois a dois não congruentes modulo p, assim é suficiente provar que c^k é um autovalor de $Y_\sigma \bmod p$ para $k = 1,2,\ldots,d-1$. Mas pela Proposição 8.13 de [5] temos, para $1 \leq k \leq d-1$, que

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \simeq \left(\frac{U}{U^p}\right)^{\lambda_k} = \frac{U^{\lambda_k}U^p}{U^p} \simeq \frac{U^{\lambda_k}}{U^{\lambda_k} \cap U^p}.$$

Logo o conjunto $U^{\lambda_k} \setminus U^{\lambda_k} \cap U^p$ é não vazio e podemos obter um autovalor mod p de Y_σ correspondente a c^k. Portanto $\mathbb{Q}(\zeta+\zeta^{-1})$ satisfaz a condição (b) da Proposição (11) para $\ell = p$ assim como seu subcorpo K.

Seja $E \in C_p$, pela Proposição (6) sabemos que E_{p^ν} é não vazio e como p é impar, segue do Teorema (2) que

$$(*) \qquad E^{\rho_k \lambda_k} = 1 \quad \text{para} \quad k = 0, 1, \ldots, d-1,$$

onde ρ_k é o menor expoente de $\Omega_p^{\lambda_k}$.

Agora, seja $\sum_{i=0}^{d-1} a_i \sigma^i \in \mathbb{Z}[G]$ um anulador de Ω_p. Temos

$$(\sum_{i=0}^{d-1} a_i \sigma^i)\lambda_k \equiv (\sum_{i=0}^{d-1} a_i c^{ki})\lambda_k \bmod p^\nu \quad \text{para} \quad 0 \leq k \leq d-1,$$

e p^ν é um expoente de Ω_p, portanto $\rho_k \mid \sum_{i=0}^{d-1} a_i c^{ki}$, digamos $\sum_{i=0}^{d-1} a_i c^{ki} = b_k \rho_k$. Então

$$d \sum_{i=0}^{d-1} a_i \sigma^i \equiv \sum_{i=0}^{d-1} a_i \sigma^i \sum_{k=0}^{d-1} \lambda_k \equiv$$

$$\equiv \sum_{k=0}^{d-1} \sum_{i=0}^{d-1} a_i c^{ki} \lambda_k = \sum_{k=0}^{d-1} b_k \rho_k \lambda_k \bmod p^\nu.$$

Este último elemento anula C_p por (*), e como p^ν é um expoente de C_p e $p \nmid d$ concluímos que $\sum_{i=0}^{d-1} a_i \sigma^i$ anula C_p

como queríamos provar.

4. UMA APLICAÇÃO AO PRIMEIRO CASO DO ÚLTIMO TEOREMA DE FERMAT

Sejam $p \geq 5$ um primo, $\zeta = \zeta_p$ uma raiz p-ésima primitiva da unidade e $K = \mathbb{Q}(\zeta + \zeta^{-1})$. Sejam g uma raiz primitiva mod p e σ o automorfismo de K tal que $\sigma(\zeta + \zeta^{-1}) = \zeta^g + \zeta^{-g}$, temos que $G = \langle \sigma \rangle$. Preservamos as notações das seções anteriores, neste caso particular, temos que $d = \# G = \frac{p-1}{2}$ e

$$V(1) = \{ \prod_{k=1}^{d} [(1-\zeta^k)(1-\zeta^{-k})]^{a_k} : a_k \in \mathbb{Z} \quad e \quad \sum_{k=1}^{d} a_k = 0 \}.$$

Lembramos que U é o grupo das unidades positivas de $A = \mathbb{Z}[\zeta + \zeta^{-1}]$, $\Omega = U/V(1)$, C é o grupo das classes de ideais de K e Ω_p, C_p são os p-Sylow subgrupos correspondentes. Chamamos $h^+ = \# C$ ao número das classes de K.

Seja p^ν, $\nu \geq 1$ um expoente de Ω_p, este é também um expoente de C_p como segue do Corolário do Teorema (2) (se $p \mid h^+$ podemos tomar p^ν = a maior potência de p que divide h^+). Seja $c = g^{2p^{\nu-1}}$ e para $0 \leq k \leq d-1$ definamos

$$\lambda_k = \sum_{j=0}^{d-1} c^{kj} \sigma^{-j}.$$

Para $1 \leq k \leq d-1$ definimos ρ_k como o menor expoente de

$\Omega_p^{\lambda_k}$. Segue do Corolário do Teorema (2) (e realmente é a principal etapa de sua prova) que ρ_k é um expoente de $C_p^{\lambda_k}$. Em particular se $\rho_k = 1$, então $C_p^{\lambda_k} = (1)$.

Por outra parte é bem conhecido que se $\rho_k > 1$ então $[(1 - \zeta)(1 - \zeta^{-1})]^{\lambda_k} = \alpha^p$ para algum $\alpha \in A$ e reciprocamente (para provar isto usar o congruência $\lambda_k^2 \equiv d\lambda_k \bmod p$, a recíproca segue da independência das unidades $(\frac{1 - \zeta^k}{1 + \zeta})\,(\frac{1 - \zeta^{-k}}{1 - \zeta^{-1}})$, $k = 2,3, \ldots, \frac{p-1}{2}$).

Depois destas considerações podemos provar o seguinte resultado (chamamos B_n o n-ésimo número de Bernoulli definido por $t / (e^t - 1) = \sum_{j=0}^{\infty} (B_j / j!) t^j$).

TEOREMA 3. Sejam $a, b, c \in \mathbb{Z} \setminus p\mathbb{Z}$, suponhamos que $a^p + b^p = c^p$, então para todo r par, $2 \leq r \leq p - 3$, ou existe $\alpha \in \mathbb{Z}[\zeta]$ tal que

$$\prod_{i=1}^{p-1} (1 - \zeta^i)^{i^r} = \alpha^p,$$

e portanto $p \mid B_{p-1-r}$, ou existem $\beta \in \mathbb{Z}[\zeta]$ e $s \in \mathbb{Z}$ tais que

$$\left[\prod_{i=1}^{p-1} \left(\frac{1 - \zeta^i}{1 - \zeta}\right)^{i^r}\right]^s \prod_{i=1}^{p-1} (a + b\zeta^i)^{i^r} = \beta^p,$$

e portanto

$$s\,\frac{B_{p-1-r}}{p-1-r} \equiv \frac{1}{1-u}\sum_{j=1}^{p-1} j^{p-2-r}u^j \bmod p,$$

onde $u = -\frac{a}{b}$.

OBSERVAÇÕES. O Teorema (3) extende a primos arbitrarios p certos resultados de [7], Parte II, como foi prometido nesse artigo. Podemos pensar neste teorema como sendo um complemento do seguinte, que implica as congruências de Kummer-Mirimanoff (ver a referência [6]): Seja r impar $1 \leq r \leq p-3$, então ou $p|B_{r+1}$ ou existe $\gamma \in \mathbb{Z}[\zeta]$ tal que

$$\prod_{i=1}^{p-1}(a + b\zeta^i)i^r = \gamma^p,$$

e portanto $\sum_{j=1}^{p-1} j^{p-2-r}u^j \equiv 0 \bmod p$.

PROVA DO TEOREMA 3. Sejam r um inteiro par tal que $2 \leq r \leq p-3$ e $k = \frac{p-1-r}{2}$. Comecemos observando que

$$\lambda_k = \sum_{j=0}^{d-1} c^{kj_\sigma - j} \equiv \sum_{j=0}^{d-1} g^{2kj_\sigma - j} \equiv \sum_{j=0}^{d-1} g^{(p-1-2k)j_\sigma j} =$$

$$= \sum_{j=0}^{d-1} g^{rj_\sigma j} \equiv \sum_{i=1}^{d} i^r\sigma_i \bmod p,$$

onde σ_i é o automorfismo de K tal que

$$\sigma_i(\zeta + \zeta^{-1}) = (\zeta^i + \zeta^{-i}), \quad 1 \leq i \leq \frac{p-1}{2}.$$

Como foi dito nas observações que precedem o teorema, se $\rho_k > 1$, então $[(1-\zeta)(1-\zeta^{-1})]^{\lambda_k} = \alpha_o^p$ para algum $\alpha_o \in A$, portanto

$$\prod_{i=1}^{d} [(1-\zeta^i)(1-\zeta^{-i})]^{i^r} = \alpha_1^p \quad \text{para algum} \quad \alpha_1 \in A,$$

mas então

$$\prod_{i=1}^{p-1} (1-\zeta^i)^{i^r} = \alpha^p \quad \text{para algum} \quad \alpha \in A,$$

isto implica que $p \mid B_{p-1-r}$ (referências [6] e [7]).

Se $\rho_k = 1$ então $\Omega_p^{\lambda_k} = (1)$ e $C_p^{\lambda_k} = (1)$, i.e. λ_k anula Ω_p e C_p.

Como é sabido, temos que $(a + b\zeta)(a + b\zeta^{-1}) = A^p$ para algum ideal A de A, logo

$$[(a + b\zeta)(a + b\zeta^{-1})]^{\lambda_k} = A^{\lambda_k p}.$$

Se $2h^+ = p^t n.$ com $p \nmid n$, então

$\bar{A}^{\lambda_k n} = 1$ onde $\bar{A}$ é a classe de A em C (porque $\bar{A}^n \in C_p$).

Temos também que $\bar{A}^{\lambda_k p} = 1$, logo $\bar{A}^{\lambda_k} = 1$. Portanto

$$\varepsilon[(a+b\zeta)(a+b\zeta^{-1})]^{\lambda_k} = \beta_o^p \quad \text{para algum} \quad \beta_o \in A \quad \text{e algum} \quad \varepsilon \in U.$$

Como $\lambda_k^2 \equiv d\lambda_k \bmod p$ obtemos

$$\varepsilon^{n\lambda_k}[(a + b\zeta)(a + b\zeta^{-1})]^{dn\lambda_k} = \beta_o^{np\lambda_k}.$$

Seja $\bar{\varepsilon}$ a classe de ε em Ω, então $\bar{\varepsilon}^{n\lambda_k} = 1$, isto é $\varepsilon^{n\lambda_k} = \delta \in V(1)$. Logo $\varepsilon^{dn\lambda_k} = \delta^{\lambda_k} \in V(1)^{\lambda_k}$. Isto implica que $[(1-\zeta)(1-\zeta^{-1})]^{s_o\lambda_k}[(a+b\zeta)(a+b\zeta^{-1})]^{d^2n\lambda_k} = \beta_1^p$ para algum $\beta_1 \in A$ e algum $s_o \geq 0$ inteiro.

Como $p \nmid d^2n$ e $\lambda_k = \sum_{i=1}^{d} i^r\sigma_i \bmod p$, a igualdade acima implica que

$$\Big(\prod_{i=1}^{d}[(1-\zeta^i)(1-\zeta^{-i})]^{i^r}\Big)^{s_1}\prod_{i=1}^{d}[(a+b\zeta^i)(a+b\zeta^{-1})]^{i^r} = \beta_2^p$$

para algum $\beta_2 \in A$ e algum $s_1 \geq 0$ inteiro.

Portanto,

$$\prod_{i=1}^{p-1}\Big(\frac{1-\zeta^i}{1-\zeta}\Big)^{i^r s}\prod_{i=1}^{p-1}(a+b\zeta^i)^{i^r} = \beta^p$$

para algum $\beta \in \mathbb{Z}[\zeta]$ e algum $s \in \mathbb{Z}$, porque $\sum_{i=1}^{p-1} i^r \equiv 0 \bmod p$.

Como $\beta^p \equiv e \bmod p$ para algum $e \in \mathbb{Z}$, a igualdade acima implica que

$$s\,\frac{B_{p-1-r}}{p-1-r} \equiv \frac{1}{1-u}\sum_{j=1}^{p-1} j^{p-2-r}u^j \bmod p,$$

como é provado em [7], Proposição (2) da Parte II. Isto completa a prova do teorema.

REFERÊNCIAS

[1] S. LANG, "Algebra", Addison-Wesley, Reading, MA, 1956.

[2] E. ARTIN and J. TATE, "Class Field Theory", Benjamin, New York, 1967.

[3] S. LANG, "Algebraic Number Theory", Addison-Wesley, Reading, MA, 1970.

[4] S. LANG, "Cyclotomic Fields", Graduate Texts in Mathematics, Springer-Verlag, New York, 1978.

[5] L. C. WASHINGTON, "Introduction to Cyclotomic Fields", Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.

[6] F. THAINE, Polynomials generalizing binomial coefficients and their application to the study of Fermat's last theorem, J. Number Theory 15, (1982), 304 - 317.

[7] F. THAINE, On the first case of Fermat's last theorem, J. Number Theory 20, Nº 2, (1985), 128 - 142.