ESTUDO DOS INTEIROS INVERSÍVEIS DE UM CORPO DE NÚMEROS ALGÉBRICOS COMO MÓDULO SOBRE O GRUPO DE GALOIS

Walter Ricardo Ferrer

Dissertação apresentada ao Instituto de Matemática e Estatística da Universidade de São Paulo para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Alfredo Jones

Durante a elaboração deste trabalho o autor recebeu apoio financeiro da FINEP.

Agosto de 1976

A G R A D E C I M E N T O S

Ao professor A.Jones pelo apoio material e matemático que me deu nos últimos tempos.

As autoridades do IME-USP que fizeram possível a continuação de meus estudos de matemática.

À Sonia M. R. De Ales pelo trabalho de datilografia.

Ao Sr. Armando Segura pelo trabalho de impressão.

P R E F Á C I O

O presente trabalho está baseado em dois artigos de James A x (ver [1] e [2]) sôbre a ação do grupo de Galois nos inversíveis de um anel de inteiros algébricos.

Seja K uma extensão normal de dimensão finita dos racionais. Seja $\mathcal{O}$ o anel dos inteiros de K, U os inversíveis de $\mathcal{O}$, C as raízes da unidade de K e $E = U/_C$. E é um grupo abeliano multiplicativo de posto r, onde r = número de Dirichlet de K. O grupo G = Gal(K,Q) opera de forma natural sobre E, dando a E uma estrutura de ZG-módulo, de posto finito sobre Z.

O objetivo do presente trabalho é estudar esse ZG-módulo E, estudo que nos dará informações sobre os inversíveis de K.

No capítulo II estudamos E como ZG-módulo e no capítulo III estudamos E localmente, ou seja como Z_pG-módulo onde p é um primo arbitrário de Q, e Z_p é o anel dos inteiros p-ádicos.

No estudo local aparece um problema formulado por Leopoldt [9] , qual seja: no caso de K ser uma extensão abeliana de Q o posto do regulador p-ádico (chamaremos r_p ao tal posto) coincide com o número de Dirichlet r ?

Também está naturalmente relacionado com o estudo local do E, um problema que é uma generalização do 7º problema de Hilbert.

Hilbert propos o seguinte problema: se α e β são números algébricos com $\alpha \neq 0$ e 1, provar que se $\alpha^{\gamma} = \beta$, então γ é transcendente ou racional.

Outra maneira de formular esse problema(que passou a historia com o nome de 7º problema de Hilbert) é a seguinte: Se α_1 e α_2 são números algébricos e lg α_1 e lg α_2 são linearmente dependentes sobre o corpo dos números algébricos, então são linearmente dependentes sobre os racionais.

Gelfond resolveu o 7º problema de Hilbert em 1934. Uma generalização natural aparece quando temos um número arbitrário de elementos algébricos $\alpha_1, \ldots \alpha_n$ e uma valorização arbitrária $| \, |$. Suponhamos que os $\alpha_1, \ldots, \alpha_n$ estejam nas condições nas quais é possível definir o logarítmo com respeito a valorização $| \, |$. É verdade que se os lg α_i $i = 1, \ldots, n$, são linearmente dependentes sobre o corpo dos números algébricos são também linearmente dependentes sobre Q ? (ver [1]).

Mahler [10] respondeu afirmativamente a tal pergunta (que chamaremos conjetura de Ax) no caso n=2 e a valorização uma valorização não arquimediana de Q.

Os dois casos de conjetura de Ax anteriormente mencionados (7º problema de Hilbert e teorema de Mahler) são os únicos conhecidos atualmente.

O interessante é que a verdade da conjetura de Ax implica a resposta afirmativa ao problema de Leopoldt mencionado anteriormente.

Passaremos agora a fazer um resumo dos principais resultados do trabalho.

O Capítulo I consta de pré-requisitos, a maioria deles enunciados sem demonstração.

Nas seções II.1,II.2 e II.3 definimos a estrutura do ZG-módulo E e provamos que E considerado com QG-módulo é isomorfo a um ideal, que chamaremos I', contido no ideal de aumentação de ZG, e que coincide com o ideal de aumento no caso em que a extensão K é real.

Na seção II.4, damos algumas aplicações; em em particular o teorema II.4.1 que no que segue será uma ferramenta útil.

Na secção II.5 estudamos o problema do ZG-isomorfismo entre E e I'. É bem conhecido o fato de que $E \otimes_Z Q = I' \otimes_Z Q$ como QG-módulos não implica que E = I' como ZG-módulos. Na Seção II.5 necessariamente estudamos numerosos exemplos e contra-exemplos para esse problema. Em particular construímos um exemplo no qual E e I' não são isomorfos como ZG-módulos.

Na seção II.6 demonstramos alguns resultados que nos serão úteis na seção II.7.

Na seção II.7 demonstramos que E e I' são ZG-isomorfos no caso de que G = Gal (K,Q) seja um grupo cíclico de ordem p, com p um primo tal que h(p) = 1 (h(p) = número de classes de ideais do corpo ciclotômico p-ésimo). Demonstremos também um resultado bastante mais fraco no caso de h(p) arbitrário.

As seções III.1,III.2 e III.3 introduzem técnicas e resultados que serão aplicados mais tarde.

Na seção III.4 cpnstruímos o análogo do I' e o análogo do isomorfismo da seção II.3 entre $E \otimes_Z Q$ e I', ou seja um morfismo λ_p entre $E \otimes_Z Z_p$ e $\lambda_p\ (E \otimes_Z Z_p)$. Esse morfismo não será injetor, em geral.

Na seção III.5 provamos que λ_p é injetor se e somente se o posto r_p do regulador p-ádico é igual ao número de Dirichlet r de K.

Na seção III.6 demonstramos alguns resultados parciais em torno da igualdade $r_p = r$, em particular o teorema III.6.2 que afirma que $r_p = r$ no caso de que o grupo G tenha expoente ≤ 4 ou 6.

As restrições sobre o expoente estão ligadas ao fato de que só conhecemos a validez da conjetura de Ax no caso n = 2, ou seja no caso do teorema de Mahler [10]. Pela observação 3 se conhecessemos a validez da tal conjetura poderíamos tirar conclusões sobre a igualdade $r_p = r$ sem fazer restrições sobre o expoente do grupo G.

Na seção III.7 demonstramos a conjetura de Leopoldt num caso particular, usando um resultado da teoria de corpos de classes de Hilbert.

C A P Í T U L O   I

Reuniremos aqui sem demonstração, alguns resultados e definições que serão de uso frequente no desenvolvimento do trabalho.

SEÇÃO I.1   PRÉ-REQUISITOS DE TEORIA DOS NÚMEROS

DEFINIÇÃO I.1 Um corpo de números algébricos é uma extensão K, algébrica finita dos racionais.

DEFINIÇÃO I.2 Chamam-se inteiros de K, aqueles elementos de K, que verificam um polinomio de coeficiente inicial um e coeficientes inteiros.

PROPRIEDADE I.1.1 Os inteiros de K formam um anel. Usualmente denotaremos esse anel como $\mathcal{O}$

DEFINIÇÃO I.1.3 Chamam-se inversíveis de K, aqueles elementos de $\mathcal{O}$ que possuem inverso em $\mathcal{O}$. Usualmente denotaremos esse grupo multiplicativo como $\mathcal{U}$.

PROPRIEDADE I.1.2. As raízes da unidade contidas em K, são elementos de $\mathcal{U}$. Ao subgrupo de $\mathcal{U}$ formado pelas raízes da unidade usualmente o denotaremos por C. C é um grupo finito.

PROPRIEDADE I.1.3 Se $\dim_Q K = n$, existem exatamente n isomorfismos diferentes de K, no corpo dos números complexos (Esses isomorfismos deixam Q fixo).

DEFINIÇÃO I.1.4 Se $\sigma : K \to C$ é um isomorfismo de K nos complexos, dizemos que σ é real se $\sigma(K) \subseteq R$.

DEFINIÇÃO I.1.5 Se $\sigma : K \to C$ é um isomorfismo, então a aplicação $\overline{\sigma}: K \to C$, $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$, chama-se isomorfismo conjugado de σ.

Chamaremos s ao número de isomorfismos reais e 2t ao número de isomorfismos complexos. É claro que $n = s + 2t$.

DEFINIÇÃO I.1.6 O número $r = s + t - 1$, chama-se número de Dirichlet da extensão K.

TEOREMA I.1.1 (Dirichlet)

Existem r inversíveis ε_i tais que o grupo $U = C \times \langle\varepsilon_1\rangle \times \ldots \langle\varepsilon_r\rangle$, onde C é o grupo finito das raízes da unidade contidas em K e $\langle\varepsilon_i\rangle$ indica o grupo cíclico infinito gerado pelo inversível ε_i.

O conjunto $\{\varepsilon_i : i=1\ldots r\}$ chama-se um conjunto de inversíveis fundamentais de K)

Seja agora $\sigma_1, \ldots \sigma_s, \sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}$ o conjunto dos isomorfismos de K em C, onde σ_i real para $1 \leq i \leq s$.

Seja $\varepsilon_1, \ldots \varepsilon_{s+t-1}$ um conjunto de inversíveis fundamentais.

DEFINIÇÃO I.1.7 Chama-se matriz regulador de K a matriz

$$R = \begin{pmatrix} \lg|\sigma_1(\varepsilon_1)|, \ldots, \lg|\sigma_s(\varepsilon_1)|, \ \lg|\sigma_{s+1}(\varepsilon_1)|^2, \ldots, \lg|\sigma_{s+t}(\varepsilon_1)|^2 \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ \lg|\sigma_1(\varepsilon_r)|, \ldots, \lg|\sigma_s(\varepsilon_r)|, \ \lg|\sigma_{s+1}(\varepsilon_r)|^2, \ldots, \lg|\sigma_{s+t}(\varepsilon_r)|^2 \end{pmatrix}$$

TEOREMA I.1.2 O posto da matriz R é igual a r, e em consequência não depende do conjunto dos inversíveis fundamentais escolhido.

DEFINIÇÃO I.1.8 Dado $x \in K$ define-se

$$Tr_{K,Q}(x) = \sigma_1(x) + \ldots + \sigma_n(x)$$

$$N_{K,Q}(x) = \sigma_1(x) \cdot \ldots \cdot \sigma_n(x)$$ onde $\sigma_1, \ldots \sigma_n$ são os isomorfismos de K em C.

Usualmente indicaremos $Tr_{K,Q}$ e $N_{K,Q}$ simplesmente como Tr e N respectivamente.

PROPRIEDADE I.1.4 a) $\forall x \in K$ $Tr_{K,Q}$ e $N_{K,Q}(x)$ são elementos de Q.

b) Se $a \in Q$, $Tr_{K,Q}(a) = na$ e $N_{K,Q}(a) = a^n$

c) $Tr_{K,Q}(x+y) = Tr_{K,Q}(x) + Tr_{K,Q}(y)$

$N_{K,Q}(xy) = N_{K,Q}(x) \cdot N_{K,Q}(y)$

DEFINIÇÃO I.1.9 Chama-se discriminante de uma base $\{\omega_1, \ldots \omega_n\}$ de K sobre Q ao elemento de Q, $\det(Tr_{K,Q}(\omega_i\omega_j)_{1 \leq i,j \leq n})$.

Usaremos a notação $\Delta(\omega_1, \ldots \omega_n)$ para o tal discriminante.

PROPRIEDADE I.1.5 Dada uma base arbitrária de K sobre Q,

$$\Delta(\omega_1, \ldots \omega_n) \neq 0.$$

DEFINIÇÃO I.1.10 Uma base de $\mathcal{O}$ sobre Z, chama-se uma base fundamental de K(é claro que toda base de $\mathcal{O}$ sobre Z é uma base de K sobre Q)

PROPRIEDADE I.1.6 Dadas duas bases $\{\omega_1, \ldots, \omega_n\}$ e $\{\omega'_1, \ldots, \omega'_n\}$ fundamentais de K, se verifica $\Delta(\omega_1, \ldots \omega_n) = \Delta(\omega'_1, \ldots, \omega'_n)$.

Essa propriedade é consequência de uma propriedade mais geral que afirma que dadas duas bases $\{\omega_1, \ldots \omega_n\}$ e $\{\omega'_1, \ldots, \omega'_n\}$ de K sobre Q de modo que $\omega'_i = \sum_{j=1}^{n} c_{ij}\omega_j$ $i = 1, \ldots n$, então

$$\Delta(\omega_1',\ldots,\omega_n') = (\det(c_{ij})^2\ \Delta(\omega_1,\ldots\ \omega_n)\ .$$

DEFINIÇÃO I.1.11 O número $\Delta(\omega_1,\ldots\omega_n)$ discriminante de uma base fundamental de K, chama-se discriminante do corpo de números algébricos.

PROPRIEDADE I.1.7 Dada $\{\omega_1,\ldots,\omega_n\}$ uma base de K sobre Q, se $\sigma_1,\ldots\sigma_n$ são os isomorfismos de K em C, então

$$\Delta(\omega_1,\ldots\omega_n) = (\det(\sigma_i(\omega_j)))^2$$

PROPRIEDADE I.1.8 O anel $\mathcal{O}$ dos inteiros de K é um anel de Dedekind.

DEFINIÇÃO I.1.12 Dado um elemento p ∈ Q, p primo, dizemos que o ideal primo P está sobre p se $P/\mathcal{O}_p$ (onde $\mathcal{O}p$ é o ideal principal de $\mathcal{O}$ gerado por p, e o símbolo $P/\mathcal{O}_p$ se deve entender no sentido usual da divisibilidade de ideais em aneis de Dedekind).

Nas duas seguintes definições P é um primo que está sobre p.

DEFINIÇÃO I.1.13 Chama-se grau de inércia de P ao número $f_p = \dim_{F_p} \sum p$ onde $\sum_p = \mathcal{O}/_p$ e F_p é o corpo finito com p elementos.

DEFINIÇÃO I.1.14 Chama-se índice de ramificação de P ao número e_p que verifica $P^{e_p}/\mathcal{O}_p$, $P^{e_p+1} \nmid \mathcal{O}_p$.

PROPRIEDADE I.1.7 Para todo primo p ∈ Q fixo vale que:

$$\sum_P e_p\, f_p = \dim_Q K,$$

onde P percorre o conjunto dos primos de $\mathcal{O}$ que estão sobre p.

DEFINIÇÃO I.1.5 Seja P um primo que está sobre p. Define-se

$$N_{K,Q}(P) = (p)^{f_p}$$

onde (p) indica o ideal de Z gerado pelo primo p em Z.

Para um ideal arbitrário A de $\mathcal{O}$, $A = P_1^{t_1} \ldots P_s^{t_s}$ define-se $N_{K,Q}(A)$ multiplicativamente.

PROPRIEDADE I.1.8 Se $\alpha \in \mathcal{O}$, $N_{K,Q}((\alpha)) = (N_{K,Q}(\alpha))$.

$N_{K,Q}(A)$ é um ideal de Z. Em consequência existe um número $\mathcal{N}$ inteiro positivo tal que $N_{K,Q}(A) = (\mathcal{N})$. Um tal $\mathcal{N}$ chama-se norma absoluta do ideal A, e usaremos a notação $\mathcal{N} = \mathcal{N}_{K,Q}(A)$ ou $(\mathcal{N} = \mathcal{N}(A))$

PROPRIEDADE I.1.9

$$\mathcal{N}_{K,Q}(A) = \# (\mathcal{O}/_A) \quad \text{onde A é um ideal arbitrário de } \mathcal{O}.$$

DEFINIÇÃO I.1.16 Dois ideais A e B de $\mathcal{O}$ diz-se que estão na mesma classe de ideais de $\mathcal{O}$ se existem α e $\beta \in \mathcal{O}$ tais que $\alpha A = \beta B$

TEOREMA I.1.3 O número, h, de classes de ideais de um corpo de números algébricos é finito.

PROPRIEDADE I.1.10 h = 1 se e somente se o anel $\mathcal{O}$ é um anel fatorial.

DEFINIÇÃO I.1.17 Seja h(p) o número de classes de ideais do corpo $Q(\xi)$ onde ξ é uma raíz p-ésima primitiva da unidade. Um primo $p \in Q$ diz-se regular se $p \nmid h(p)$.

SEÇÃO I.2 PRÉ-REQUISITOS DE ANÉIS DE GRUPOS E TEORIA DE REPRESENTAÇÕES

A referência básica para essa parte será [13]

Seja R um anel comutativo com unidade e seja V um módulo livre de dimensão finita sobre R.

Usaremos a notação GL(V) para indicar o grupo multiplicativo dos R homomorfismos inversíveis de V em si mesmo.

DEFINIÇÃO I.2.1. Seja G um grupo finito arbitrário. Uma representação de G sobre R é um homomorfismo $T : G \longrightarrow GL(V)$

O número $\text{posto}_R\, V$ chama-se grau de representação.

PROPRIEDADE I.2.1. A toda representação $T : G \longrightarrow GL(V)$ de grau n corresponde uma classe de equivalência de representações matriciais, ou seja uma classe de equivalência de aplicações $T : G \longrightarrow GL_n(R)$, onde $GL_n(R)$ indica o grupo das matrizes n x n a coeficientes em R, inversíveis. Duas representações $T,T' : G \longrightarrow GL_n(R)$ dizem-se equivalentes (u R-rquivalentes) se $S \in GL_n(R)$ tal que $\forall g \in G$ acontece que $T(g) = ST'(g)S^{-1}$.

Dado um grupo G e um anel R comutativo com unidade consideremos o conjunto das combinações lineares formais:

$\sum_{g\in G} r(g)g$ onde $r(g) \in R$. Dizemos que $\sum_{g\in G} r(g)g = \sum_{g\in G} r'(g)g$ se e somente se $r(g) = r'(g)$ $\forall g \in G$. Dados dois elementos $\sum_{g\in G} r(g)g = x$ e $\sum_{g\in G} s(g)g = y$ podemos definir

$$x + y = \sum_{g\in G} (r(g)+s(g))g$$

$$xy = \sum_{g\in G} t(g)g \quad \text{onde } t(g) = \sum_{h_1h_2=g} r(h_1)\, s(h_2)$$

DEFINIÇÃO I.2.2. Chama-se anel de grupo de G sobre R ao conjunto

$RG = \{ \sum_{g \in G} r(g)g : r(g) \in R \quad \forall g \in G\}$ RG com a soma e produto definida anteriormente é um anel com unidade

TEOREMA I.2.1. Existe uma correspondência bijetora entre as representações do grupo G sobre o anel R e os RG-módulos livres sobre R de dimensão finita

DEMONSTRAÇÃO

Essa tal correspondência está dada da seguinte forma:

Dada $T : G \longrightarrow GL(V)$, damos a V uma estrutura de RG-módulo da seguinte forma $(\sum_{g \in G} r(g)g) \cdot v = \sum_{g \in G} r(g)\, T(g)(v) \in V$.

Um resultado útil no caso de representações sobre um corpo e o teorema de Maschke

TEOREMA I.2.2. *(Maschke)* Seja K um corpo e G um grupo finito. Então KG é semi-simples se e somente se car $K \nmid |G|$.

Se sabemos que o anel KG é semisimples sabemos que todo M módulo sobre KG é semisimples. Então temos informações sobre as representações de G sobre K.

DEFINIÇÃO I.2.3. Chama-se morfismo de aumentação ou função índice de RG ao seguinte morfismo de RG em R.

$$\varepsilon \left(\sum_{g \in G} r(g)g \right) = \sum_{g \in G} r(g)$$

DEFINIÇÃO I.2.4. O $\operatorname{Ker} \varepsilon = \{ \sum_{g \in G} r(g)g : \sum_{g \in G} r(g) = 0\}$ chama-se ideal de aumentação de **RG**. Usualmente denotaremos esse ideal como I_R(ou I quando o anel esteja subentendido).

PROPRIEDADE I.2.2. O conjunto $\{g - 1 : g \in G\}$ é uma R-base de I_R sobre R, em particular $\dim_R I_R = |G| - 1$

Vamos considerar rapidamente algumas propriedades relacionadas com a extensão do anel de coeficientes.

Dada uma representação inteira $T : G \longrightarrow GL_n(Z)$ chamaremos $T^Q : G \longrightarrow GL_n(Q)$ a função $i \circ T = T^Q$ onde i é a função inclusão $i : GL_n(Z) \longrightarrow GL_n(Q)$

PROPRIEDADE I.2.3. Se chamarmos M(T) ao ZG-módulo associado à representação inteira T e $M(T^Q)$ ao QG-módulo associado à representação racional T^Q, temos que $M(T^Q) = Q \otimes_Z M$, onde a estrutura de QG-módulo de $Q \otimes_Z M$ está dada por $g.(r \otimes m) = r \otimes gm$.

Essa propriedade vale também se substituirmos Z por um corpo arbitrário K e Q por uma extensão arbitrária L de K.

No caso de corpos temos uma ferramenta muito útil que é o teorema de Noether-Deuring

TEOREMA I.2.3. (Noether-Deuring)

Sejam M e N KG-módulos de dimensão finita sobre K.Então os FG-módulos $F \otimes_k M$ e $F \otimes_k N$ são isomorfos se e somente se M e N são isomorfos como KG-módulos.

Esse resultado não é valido para o caso de Z e Q. Ou seja existem Z-representações G que como Q-representações são isomorfos mas não são isomorfos como Z-representações.

EXEMPLO I.2.1. (ver [4])

Seja G o grupo cíclico de dois elementos. Sejam as representações $T : G \longrightarrow GL_2(Z)$ $U : G \longrightarrow GL_2(z)$ definidas sobre um gerador g de G da seguinte forma:

$$T(g) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad U(g) = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

É claro que $T \sim_Q U$ (pois ambos tem o mesmo polinômio mininal que tem só fatores lineares).

Mas não existe uma matriz $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ tal que $\alpha,\beta,\gamma,\delta \in Z$ e $\alpha\delta - \beta\gamma = \pm 1$ e

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} .$$

Pois dessa igualdade tiraríamos que

$$\begin{pmatrix} \alpha & \beta \\ -\gamma & -\delta \end{pmatrix} = \begin{pmatrix} \alpha & \alpha - \beta \\ \gamma & \gamma - \delta \end{pmatrix}$$

Então $\gamma = 0$, $\alpha = 2\beta$ logo $\det \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} = 2\beta\delta \neq \pm 1.$

C A P Í T U L O   II

SEÇÃO II.1   A REPRESENTAÇÃO $\underline{E}$

Seja K uma extensão de Galois de grau n. Suponhamos $n = s + 2t$ onde s é o número de $\mathbb{Q}$-isomorfismos reais de K e $2t$ é o número de $\mathbb{Q}$-isomorfismos complexos agrupados em pares de automorfismos complexos conjugados $(\bar{\sigma}(x + iy) = \overline{\sigma(x + iy)})$. O número de Dirichlet de K, que chamaremos $\underline{r}$ é igual a : $r = s + t - 1$. Como a extensão K é normal, se existe σ(automorfismo de K) tal que $\sigma(K) \subset \mathbb{R}$ então $\sigma(K) = K \subset \mathbb{R}$. Logo $\forall$ η automorfismo de K, $\eta(K) = K \subset \mathbb{R}$, ou seja $t = 0$, ou seja, os automorfismos ou são todos reais ou nenhum é real. No primeiro caso, $r = n - 1$, no segundo n é par e $r = \frac{n}{2} - 1$.

Consideremos o anel dos inteiros de K, que chamaremos de $\mathcal{O}$ e dentro dele o grupo multiplicativo dos inversíveis de $\mathcal{O}$ que chamaremos $\mathcal{U}$. O teorema de Dirichlet (ver Seção I.1.) , nos dá a estrutura do grupo abeliano $\mathcal{U}$.

$\mathcal{U} = \mathbb{C} \times \langle\varepsilon_1\rangle \times \ldots \times \langle\varepsilon_r\rangle$ onde o produto é produto direto, $\mathbb{C}$ é o grupo finito das raízes da unidade contidas em K, r é exatamente o número de Dirichlet de K e os $\langle\varepsilon_1\rangle,\ldots,\langle\varepsilon_r\rangle$ são grupos cíclicos infinitos com geradores $\varepsilon_1, \ldots,\varepsilon_r$, chamados inversíveis fundamentais.

Então o grupo $E = U/C$ é um grupo livre de posto r. Seja $G = Gal(\kappa, \mathbb{Q})$. Podemos dar a U uma estrutura de ZG-módulo à esquerda fazendo $\forall \sigma \in G$ e $\forall \varepsilon \in U$, $\sigma\varepsilon = \sigma(\varepsilon) \in U$ (é claro que a imagem de um inversível por um automorfismo é um inversível). É claro que isso define uma estrutura de ZG-módulo em U, tal que C é um ZG-submódulo à esquerda de U. Logo o quociente $E = U/C$ é um ZG-módulo que como Z-módulo é livre, de tipo finito.

Esse ZG-módulo é então uma representação do grupo G, de posto $r = n - 1$ ou $\frac{n}{2} - 1$ de acordo com que o corpo κ seja real ou complexo.

SEÇÃO II.2 A REPRESENTAÇÃO I'

Seja o ZG-módulo à esquerda $ZG = \{ \sum_{\sigma \in G} a_\sigma \sigma \mid a_\sigma \in Z, \sigma \in G \}$.

Seja $\varepsilon : ZG \to Z$ o morfismo de aumentação definido como $\varepsilon(\sum_{\sigma \in G} a_\sigma \sigma) = \sum_{\sigma \in G} a_\sigma$. ε é morfismo de anéis sobrejetor. O Ker ε é um ideal bilateral de ZG, logo um ZG-módulo à esquerda. Ainda mais é claro que uma Z-base de Ker ε é $\{ \sigma - 1 \mid \sigma \in G \}$ (Ver I.2). Então Ker $\varepsilon = I$ é uma representação de G de posto $n - 1$.

Para definir a representação I' consideramos:

a) κ real; então $I' = I$

b) κ complexo. Se c é o automorfismo de conjugação definimos

$$I' = \{ \sum_{\sigma \in G} a_\sigma \sigma \mid a_\sigma \in Z, \sigma \in G, \sum_{\sigma \in G} a_\sigma = 0 \quad a_\sigma = a_{\sigma c} \} \subset I$$

I' é um ideal à esquerda de ZG, pois de $\sum_{\sigma \in G} a_\sigma \sigma \in I'$ e $\tau \in G$,

$$\tau\left(\sum_{\sigma \in G} a_\sigma \sigma\right) = \sum_{\sigma \in G} a_\sigma \tau\sigma = \sum_{\mu \in G} a_{\tau^{-1}\mu}\mu \Longrightarrow \sum_{\mu \in G} a_{\tau^{-1}\mu} = 0 \quad e$$

$$a_{\tau^{-1}(\mu c)} = a_{(\tau^{-1}\mu)c} = a_{\tau^{-1}\mu}$$

LEMA II.2.1 $\dim_Z I' = r$

Demonstração

a) κ real; nesse caso $I' = I$ e $r = n - 1$ e $\dim_Z I = n - 1$

b) κ complexo. Nesse caso consideramos os elementos de G ordenados como segue: $1, c, \sigma_1, \sigma_1 c, \ldots, \sigma_r, \sigma_r c$.

Se $x \in I'$, $x = a_0 + a_0' c + a_1\sigma_1 + a_1'\sigma_1 c + \ldots + a_r\sigma_r + a_r'\sigma_r c$, com $a_0 = a_0', \ldots, a_r = a_r'$ e $\sum_i (a_i + a_i') = 0$; ou seja $\sum_i a_i = \sum_i a_i' = 0$.

$x = a_0 + a_0 c + a_1\sigma_1 + a_1\sigma_1 c + \ldots + a_r\sigma_r c$ com $\sum a_r = 0$,

$a_0 = - a_1 - a_2 - \ldots - a_r$.

$$x = a_0(1+c) + a_1\sigma_1(1+c) + \ldots + a_r\sigma_r(1+c) = a_1(\sigma_1 - 1)(1+c) + \ldots + a_r(\sigma_r - 1)(1+c)$$

Os elementos $(\sigma_1 - 1)(1+c), \ldots, (\sigma_r - 1)(1+c)$ são livres sobre $\mathbf{Z}$; pois se $\sum_{i=1}^{r} \alpha_i(\sigma_i - 1)(1+c) = 0 = \left(-\sum_{i=1}^{r} \alpha_i\right) + \left(-\sum_{i=1}^{r} \alpha_i\right)c + \alpha_1\sigma_1 + \alpha_1\sigma_1 c + \ldots + \alpha_r\sigma_r c$, temos que $\alpha_1 = \ldots = \alpha_r = 0$. Então os elementos $\{ (\sigma_i-1)(1+c) \}_{1\leq i\leq r}$ são base de I', então $\dim_Z I' = r$.

c.q.d.

SEÇÃO II.3 *A $\mathbb{Q}$-EQUIVALÊNCIA DE $\underline{E}$ E $\underline{I'}$*

Vamos supor $r > 0$. No caso $r = 0$, ou seja o caso de uma extensão de grau 1, ou dos corpos imaginários quadráticos, ambas representações se reduzem à representação trivial e o problema carece de sentido.

Observamos na Seção II-2 que E e I' tem a mesma dimensão sobre Z. Provaremos aqui um fato mais forte, isto é, que E e I' são equivalentes como $\mathbb{Q}G$-módulos.

LEMA II.3.1 - $I' \otimes_Z L \cong I'_L$ como LG-módulos, onde L é uma extensão arbitrária de $\mathbb{Q}$ e I'_L se define em LG da mesma forma que I' em ZG.

Demonstração

$\dim_L(I' \otimes_Z L) = \dim_Z I' = r$. É claro que $\dim_L I'_L = r$.

Seja $\alpha : I' \times L \longrightarrow I'_L$ definida assim:

$$\alpha (\Sigma\, a_i g_i \;, k) = \Sigma(ka_i)g_i$$

Essa aplicação induz $\bar{\alpha} : I' \otimes L \longrightarrow I'_L$, $\bar{\alpha} (\Sigma\, a_i g_i \otimes k) = \Sigma\, (ka_i)g_i$. É claro que $\bar{\alpha}$ é LG-linear. Provaremos que é sobrejetora. Um conjunto de L-geradores de I'_L é formado por elementos da forma $(g_i-1)(1+c)$ onde os g_i se escolhem adequada mente da mesma forma que antes. Mas é claro que:

$\bar{\alpha}((g_i - c)(1 + c) \otimes 1) = (g_i - 1)(1 + c)$ e $(g_i - 1)(1+c) \in I'$.

Logo a aplicação $\bar{\alpha}$ é sobrejetora. Como $I' \otimes_Z L$ e I'_L tem a mesma dimensão, $\bar{\alpha}$ é isomorfismo.

No caso real, a demonstração é parecida.

c.q.d.

TEOREMA II.3.1 - $E \otimes_Z \mathbb{Q} \cong I' \otimes_Z \mathbb{Q}$ como $\mathbb{Q}G$-módulos à esquerda.

Demonstração

Provaremos que $E \otimes_Z \mathbb{R} \cong I' \otimes_Z \mathbb{R}$ como $\mathbb{R}G$-módulos à esquerda, onde $\mathbb{R}$ é o corpo dos números reais. O teorema de Noether-Deuring (ver I.2) nos assegura que se existe um isomorfismo como $\mathbb{R}G$-módulos entre $E \otimes_Z \mathbb{R}$ e $I' \otimes_Z \mathbb{R}$, existe um isomorfismo como $\mathbb{Q}G$-módulos entre $E \otimes_Z \mathbb{Q}$ e $I' \otimes_Z \mathbb{Q}$. Provaremos o teorema provando que $E \otimes_Z \mathbb{R}$ e $I' \otimes_Z \mathbb{R}$ são isomorfos como $\mathbb{R}G$-módulos a $I'_{\mathbb{R}}$.

Seja $\gamma : E \times \mathbb{R} \longrightarrow \mathbb{R}G$ definida como segue:

$\gamma(e,r) = \sum_{\sigma \in G} (r \lg |\sigma^{-1}u|)\sigma$ onde $u \in U$ é tal que no homomorfismo canônico $U \longrightarrow E$, $u \longrightarrow e$. γ está bem definida, isto é, dados u_1 e u_2 tais que $u_1 = \xi u_2$ com $\xi \in \mathbb{C}$, então :

$$\sum_{\sigma \in G} (r \lg |\sigma^{-1}u_1|)\sigma = \sum_{\sigma \in G} (r \lg |\sigma^{-1}u_2|)\sigma$$

Isso é claro pois $|\sigma^{-1}(\xi)| = 1$. γ é obviamente linear na segunda variável. Na primeira temos:

$$\gamma(e_1 e_2, r) = \sum_{\sigma \in G} (r \lg |\sigma^{-1}(u_1 u_2)|)\sigma = \sum_{\sigma \in G} (r \lg |\sigma^{-1}u_1 . \sigma^{-1}u_2|)\sigma =$$

$$= \sum_{\sigma\in G} (r \lg|\sigma^{-1}u_1|)\sigma + \sum_{\sigma\in G} (r \lg|\sigma^{-1}u_2|)\sigma = \gamma(e_1,r) + \gamma(e_2,r)$$

onde u_1 é um representante de e_1 e u_2 de e_2.

Existe então $\phi : E \otimes_Z \mathbb{R} \longrightarrow \mathbb{R}G$ que faz o diagrama

$$\begin{tikzcd} E \times \mathbb{R} \arrow[r, "\gamma"] \arrow[d, "\theta"] & \mathbb{R}G \\ E \otimes_Z \mathbb{R} \arrow[ur, "\phi"'] & \end{tikzcd}$$

comutativo, onde θ é o homomorfismo canônico.

Devemos comprovar que ϕ é um $\mathbb{R}G$-morfismo. Evidentemente é um $\mathbb{R}$-morfismo. Precisamos comprovar que ϕ comuta com a ação de G sobre $E \otimes_Z \mathbb{R}$.

Seja $\tau \in G$

$$\phi(\tau(e \otimes r)) = \phi((\tau e) \otimes r) = \sum_{\sigma\in G} (r \lg|\sigma^{-1}\tau u|)\sigma$$

Chamando $\sigma = \tau\eta$ temos que

$$\sum_{\sigma\in G}(r \lg|\sigma^{-1}\tau u|)\sigma = \sum_{\eta\in G}(r \lg|\eta^{-1}u|)\tau\eta = \tau \sum_{\eta\in G}(r \lg|\eta^{-1}u|)\eta.$$

Então $\phi(\tau(e \otimes r)) = \tau\phi(e \otimes r)$

Temos também que $\phi(E \otimes_Z \mathbb{R}) \subset I_{\mathbb{R}}$. $I_{\mathbb{R}}$ = ideal de aumentação de $\mathbb{R}G$. Pois se $\varepsilon : \mathbb{R}G \longrightarrow \mathbb{R}$ é o homomorfismo de aumentação (Ver I.2) temos que

$$(\varepsilon \circ \phi)(e \otimes r) = r \sum_{\sigma\in G} \lg|\sigma^{-1}u| = r \lg \prod_{\sigma\in G} |\sigma^{-1}u| =$$

$$= r \lg \Big|\prod_{\sigma\in G} \sigma u\Big| = r \lg 1 = 0.$$ Isto é consequência do fato que $\prod_{\sigma\in G} \sigma(u) = N(u) = \pm 1$ dado que u é inversível. Então fica provado que $\phi(I \otimes_Z \mathbb{R}) \subset I_{\mathbb{R}}$:

No caso em que a extensão κ seja real, $I_{\mathbb{R}} = I'_{\mathbb{R}}$. No caso complexo queremos provar que $\phi(I \otimes_Z \mathbb{R}) \subset I'_{\mathbb{R}}$.

$\phi(e \otimes r) = \sum_{\sigma \in G} r\ (1g|\sigma^{-1}|)\sigma$. Devemos comparar $1g|\sigma^{-1}u|$ e $1g|(\sigma c)^{-1}u|$. Eles são evidentemente iguais, logo $\phi(I \otimes_Z \mathbb{R}) \subset I'_{\mathbb{R}}$.

Vamos provar agora que $\dim_{\mathbb{R}}(\phi(E \otimes_Z \mathbb{R}) \geq r$. Para isso provaremos que $\phi(e_1 \otimes 1), \ldots, \phi(e_r \otimes 1)$ sao linearmente independentes onde $\{e_i\}_{1 \leq i \leq r}$ são as imagens pela projeção canônica de um conjunto $\varepsilon_1, \ldots, \varepsilon_r$ de inversíveis fundamentais de U.

Como $\phi(e_i \otimes 1) = \sum_{\sigma \in G} 1g\ |\sigma\ \varepsilon_i|\sigma^{-1}$, provar que $\phi(e_i \otimes 1)$ são linearmente independentes sobre $\mathbb{R}$ é o mesmo que provar que os vetores de $\mathbb{R}^n = \mathbb{R}^{s+2t}$.

$(1g\ |\sigma_1\varepsilon_i|,\ 1g\ |\sigma_2\varepsilon_i|,\ \ldots,\ 1g\ |\sigma_s\varepsilon_i|,\ 1g\ |\sigma_{s+1}\varepsilon_i|,\ 1g|\sigma_{s+1}c\varepsilon_i|,$ $\ldots,\ 1g\ |\sigma_{s+t}\varepsilon i|,\ 1g\ |\sigma_{s+t}c\varepsilon_i|)$ são linearmente independentes sobre $\mathbb{R}$, onde

$$G = \{\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \sigma_{s+1}c, \ldots, \sigma_{s+t}, \sigma_{s+t}c\}.$$

Usando a notação da Seção I.1 , temos que provar que os vetores

$$(1_1\varepsilon_i, 1_2\varepsilon_i, \ldots, 1_s\varepsilon_i, \tfrac{1}{2}\, 1_{s+1}\varepsilon_i, \ldots, \tfrac{1}{2}\, 1_{s+t}\varepsilon_i, \tfrac{1}{2}\, 1_{s+t}\varepsilon_i)$$

são linearmente independentes sobre $\mathbb{R}$. Mas do fato dos ε_i serem inversíveis fundamentais deduz-se a independência dos vetores acima (Ver Seção I.1).

Como $\dim_{\mathbb{R}} I'_{\mathbb{R}} = r$, deduz-se que ϕ é um $\mathbb{R}G$-isomorfismo entre $E \otimes_Z \mathbb{R}$ e $I'_{\mathbb{R}}$. Como, pelo Lema II.3.1, $I \otimes_Z \mathbb{R} \underset{\mathbb{R}G}{\cong} I'_{\mathbb{R}}$, fica demonstrado o teorema.

c.q.d.

SEÇÃO II.4 ALGUMAS APLICAÇÕES

LEMA II.4.1. Sejam M e N, ZG-módulos livres de posto finito sobre Z. Então $M \otimes_Z \mathbb{Q} \cong N \otimes_Z \mathbb{Q}$ como $\mathbb{Q}G$-módulos se e somente se existe um ZG-submódulo N_0 de N tal que $N/_{N_0}$ é finito e $M \cong N_0$ como ZG-módulos.

DEMONSTRAÇÃO

Seja $\psi : M \otimes_Z \mathbb{Q} \longrightarrow N \otimes_Z \mathbb{Q}$ um G-isomorfismo. Sabemos que (Ver Seção I.2)

$$\dim_{\mathbb{Q}}(M \otimes_Z \mathbb{Q}) = \dim_Z M = \dim (N \otimes_Z \mathbb{Q}) = \dim_Z N$$

Sejam $m_1, \ldots, m_d$ e $n_1, \ldots, n_d$, Z-bases de M e N respectivamente. Sabemos que $m_1 \otimes 1, \ldots, m_d \otimes 1$ e $n_1 \otimes 1, \ldots, n_d \otimes 1$ são $\mathbb{Q}$-bases de $M \otimes_Z \mathbb{Q}$ e $N \otimes_Z \mathbb{Q}$ respectivamente. Então:

$$\psi(m_i \otimes 1) = \sum_{j=1} n_j \otimes r_{ji} \ , \ 1 \leq i \leq d \text{ e } r_{ji} \in \mathbb{Q}$$

Seja $\alpha \in Z$, múltiplo comum de todos os denominadores dos r_{ji}.

Seja $\psi_0 : M \longrightarrow N$ definida assim:

$$\psi_0(m_i) = \sum_{j=1} (\alpha r_{ji}) n_j$$

Seja $\alpha : N \longrightarrow N$ a multiplicação por $\alpha \in Z$ de elementos de N. Então o diagrama que aparece abaixo comuta

$$\begin{tikzcd}
 & N \otimes_Z \mathbb{Q} & \\
M \otimes_Z \mathbb{Q} \arrow[ur, "\psi_0 \otimes 1"] \arrow[rr, "\psi"'] & & N \otimes_Z \mathbb{Q} \arrow[ul, "\alpha \otimes 1"']
\end{tikzcd}$$

Pois

$$(\alpha \otimes 1)\ \psi(m_i \otimes 1) = (\alpha \otimes 1)\ \left(\sum_{j=1}^{d} n_j \otimes r_{ji}\right) = \sum_{j=1}^{d} \alpha n_j \otimes r_{ji} =$$

$$= \sum_{j=1}^{d} n_j \otimes \alpha r_{ji} = \left(\sum_{j=1}^{d} \alpha r_{ji} n_j\right) \otimes 1 = (\psi_0 \otimes 1)\ (m_i \otimes 1).$$

Em consequência

$$(\alpha \otimes 1) \circ \psi = \psi_0 \otimes 1$$

Usando essa igualdade e o fato de que ψ comuta com a operação de G sobre M deduzimos facilmente que ψ_0 também comuta com a operação de G sobre M.

Como ψ é isomorfismo e $\alpha \otimes 1$ é injetora, deduzimos que ψ_0 é injetora.

Seja $N_0 = \mathrm{Im}(\psi_0) \subset N$. Então $\dim_Z N_0 = \dim_Z \psi_0(M) = \dim_Z M = \dim_Z N$. Daí deduz-se imediatamente que todo elemento de N tem um múltiplo que está em N_0, ou seja $N/_{N_0}$ finito. Reciprocamente, se existe $\psi_0 : M \longrightarrow N_0 \subset N$, ZG-isomorfismo tal que $N/_{N_0}$ é finito $\dim_Z M = \dim_Z N$, então $\psi_0 \otimes 1 : M \otimes_Z \mathbb{Q} \longrightarrow N \otimes_Z \mathbb{Q}$ é monomorfismo pois ψ_0 é, e $\mathbb{Q}$ considerado como Z-módulo é "flat". Como $\dim_{\mathbb{Q}}(M \otimes_Z \mathbb{Q}) = \dim_{\mathbb{Q}}(N \otimes_Z \mathbb{Q})$, $\psi_0 \otimes 1$ é um G-isomorfismo entre $M \otimes_Z \mathbb{Q}$ e $N \otimes_Z \mathbb{Q}$.

c.q.d.

Uma aplicação deste resultado e da $\mathbb{Q}$-equivalência entre E e I' é o teorema seguinte que nos dá alguma informação sobre a estrutura de ZG-módulo E.

TEOREMA II.4.1. E contém um ZG-submódulo cíclico E_0, tal que $E/_{E_0}$ é finito.

DEMONSTRAÇÃO

Pelo Lema II.4.1., I' é isomorfo a um submódulo de E, de índice finito. Logo basta comprovar a afirmação do teorema para I'. Sabemos pelo Lema II.3.1. que $I' \otimes_Z \mathbb{Q} \cong_{\mathbb{Q}G} I'_{\mathbb{Q}} \subset \mathbb{Q}G$. $I'_{\mathbb{Q}}$ é somando direto de $\mathbb{Q}G$ ($\mathbb{Q}G$ semisimples, pelo teorema de Maschke, ver I.2), logo é principal, ou seja $I'_{\mathbb{Q}} = \mathbb{Q}G\,x$ com $x \in I'_{\mathbb{Q}}$. Como $x \in I'_{\mathbb{Q}}$, existe $r \in Z$ tal que $rx = y \in I'$ e $I'_{\mathbb{Q}} = \mathbb{Q}G(y/_r) = \mathbb{Q}Gy$. É fácil provar que $\mathbb{Q}Gy \cong ZGy \otimes_Z \mathbb{Q}$, como $\mathbb{Q}G$-módulos. Então temos que $I' \otimes_Z \mathbb{Q} \cong ZGy \otimes_Z \mathbb{Q}$ como $\mathbb{Q}G$-módulos. Aplicando novamente o Lema II.4.1. temos que I' contém um ZG-submódulo cíclico de índice finito.

c.q.d.

SEÇÃO II.5. ESTUDO DE ALGUNS CASOS PARTICULARES.

O teorema II.3.1 nos assegura que E e I' como $\mathbb{Q}G$-módulos são equivalentes, ou seja que existe um $\mathbb{Q}G$-isomorfismo entre $E \otimes_Z \mathbb{Q}$ e $I' \otimes_Z \mathbb{Q}$. Um problema básico é saber se E e I' são ZG-equivalentes.

Nesta seção daremos alguns resultados e exemplos sobre o problema de Z-equivalência de E e I'.

Seja $[K:\mathbb{Q}] = n$

a) $n = 1$. Nesse caso $r = 0$ e o problema carece de interesse.

b) $n = 2$. Temos duas possibilidades:

b_1) $r = 0$ e teremos a mesma situação que antes.

b_2) $r = 1$ (caso real). Nesse caso dizer que E e I' são $\mathbb{Q}$-

equivalentes (pensados como representações matriciais), quer dizer que são iguais, logo são Z-equivalentes.

c) $n = 3$. Nesse caso κ é real e $r = 2$, e $Gal(\kappa, \mathbb{Q}) \cong Z/_{3Z}$. Mais tarde demonstraremos o Teorema II.7.1., do qual se deduz que $E \cong I'$.

Provaremos agora a ZG-equivalência de E e I' diretamente.

Neste caso $I' = I = \{ a(\sigma-1) + b(\sigma^2-1) \mid a, b \in Z \}$.

$Z_3 = \{ 1, \sigma, \sigma^2 \} \cong Gal(\kappa, \mathbb{Q})$. A representação matricial associada a I é calculada como segue:

$$\sigma(\sigma - 1) = \sigma^2 - \sigma = (\sigma^2 - 1) - (\sigma - 1)$$

$$\sigma(\sigma^2 - 1) = \sigma^3 - \sigma = -(\sigma - 1)$$

Logo a representação associada a I é $T(\sigma) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$

Logo a representação matricial associada a E é:

$$U(\sigma) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Sabemos que as matrizes $T(\sigma)$ e $U(\sigma)$ são semelhantes sobre $\mathbb{Q}$ $(T \underset{\mathbb{Q}}{\sim} U)$.

Procuramos um par de inteiros $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ tal que os vetores

$\left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} ; \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\}$ sejam uma base de Z^2, ou seja, tenham determinante igual a ± 1. Nesse caso, dado que o polinômio característico de U é $x^2 + x + 1$ temos que

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \underset{Z}{\sim} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \underset{Z}{\sim} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$ onde a

última equivalência é óbvia.

Devemos achar então x_1 e x_2 inteiros tais que

$$\det\begin{pmatrix} x_1 & a_{11}x_1 + a_{12}x_2 \\ x_2 & a_{21}x_1 + a_{22}x_2 \end{pmatrix} = \pm 1$$

$$\det\begin{pmatrix} x_1 & a_{11}x_1 + a_{12}x_2 \\ x_2 & a_{21}x_1 + a_{22}x_2 \end{pmatrix} = x_1(a_{21}x_1 + a_{22}x_2) - x_2(a_{11}x_1 + a_{12}x_2) =$$

$$= a_{21}x_1^2 + (a_{22} - a_{11})x_1x_2 - a_{12}x_2^2$$

Devemos resolver em números inteiros a equação diofantina $a_{21}x_1^2 + (a_{22} - a_{11})x_1x_2 - a_{11}x_2^2 = \pm 1$. O discriminante dessa forma quadrática é $D = (a_{22} - a_{11})^2 + 4\, a_{12}a_{21}$

Do fato que $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \sim_{Q} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ tiramos a conclusão de que $a_{11} + a_{22} = -1$ Da primeira equação temos que

$$a_{11}a_{22} - a_{12}a_{21} = 1 .$$

$$a_{11}^2 + a_{22}^2 + 2\, a_{11}a_{22} = 1.$$

Então

$$D = a_{22}^2 + a_{11}^2 - 2\, a_{11}a_{22} + 4\, a_{12}a_{21} =$$

$$= 1 - 2\, a_{11}a_{22} - 2\, a_{11}a_{22} + 4\, a_{12}a_{21} =$$

$$= 1 - 4\,(a_{11}a_{22} - a_{12}a_{21}) = 1 - 4 = -3$$

Toda forma quadrática sobre Z de discriminante -3 é equivalente a $\pm(x^2 + xy + y^2)$ (Ver [5] pag.135) e logo representa +1 ou (-1).

Deduzimos então que existem esses números x_1 e x_2, ou seja, $T \underset{Z}{\sim} U$.

d) $n = 4$. Temos aqui duas alternativas:

d_1) $s = 0$, $t = 2$ e então $r = 1$

d_2) $t = 0$, $s = 4$ e então $r = 3$ (caso real)

(d_1) Nesse caso sabemos que E e I' são $\mathbb{Q}$-equivalentes e de posto 1, então se deduz que são Z-equivalentes. O grupo de Galois, $Gal(\kappa,\mathbb{Q})$ neste caso pode ser Z_4 ou $Z_2 \times Z_2$; exemplos dessas possibilidades, estão dados por $\mathbb{Q}(\xi)$, onde ξ é uma raiz primitiva de ordem 5, da unidade e $\mathbb{Q}(\zeta)$, onde ζ é uma raiz primitiva de ordem 2^3 da unidade (Ver [15] pag.257).

(d_2) Aqui aparece um primeiro caso no qual $E \not\simeq_Z I' = I$. Construiremos dois exemplos, um no qual $E \simeq_Z I' = I$ e $Gal(\kappa,\mathbb{Q}) \cong Z/_{4Z}$ e outro no qual $E \not\simeq_Z I' = I$ e $Gal(\kappa,\mathbb{Q}) \cong Z/_{2Z} \times Z/_{2Z}$

LEMA II.5.1. Duas matrizes a coeficientes inteiros da forma :

$$A = \begin{pmatrix} -1 & a_{12} & a_{13} \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} -1 & b_{12} & b_{13} \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

são Z-equivalentes se e somente se $a_{12} - a_{13} \equiv b_{12} - b_{13} \pmod 2$

DEMONSTRAÇÃO

Seja $C = \begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix}$ tal que $z_{ij} \in Z$, $\det C = \pm 1$ e $AC = CB$.

Então, escrevendo o produto

$$\begin{pmatrix} -1 & a_{12} & a_{13} \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix} = \begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix}\begin{pmatrix} -1 & b_{12} & b_{13} \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

e calculando a primeira coluna de ambas matrizes produto tmos:

$$\begin{pmatrix} -z_{11} + a_{12}z_{21} + a_{13}z_{31} \\ -z_{31} \\ z_{21} \end{pmatrix} = \begin{pmatrix} -z_{11} \\ -z_{21} \\ -z_{31} \end{pmatrix} \quad \text{então}$$

$z_{21} = z_{31} = 0$. Como $\det C = \pm 1$, temos que $z_{11} = \pm 1$. Podemos supor $z_{11} = 1$. Temos também que $(A^2 + I)C = C(B^2 + I)$

$$A^2 + I = \begin{pmatrix} 2 & a_{13} - a_{12} & -(a_{12} + a_{13}) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{Temos então que:}$$

$$\begin{pmatrix} 2 & a_{13} - a_{12} & -(a_{12} + a_{13}) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & z_{12} & z_{13} \\ 0 & z_{22} & z_{23} \\ 0 & z_{32} & z_{33} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & z_{12} & z_{13} \\ 0 & z_{22} & z_{23} \\ 0 & z_{32} & z_{33} \end{pmatrix} \begin{pmatrix} 2 & b_{13} - b_{12} & -(b_{12} + b_{13}) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

A primeira linha dos produtos é igual a:

$$(2,\ 2 z_{12} + z_{22}(a_{13} - a_{12}) - z_{32}(a_{12} + a_{13}),\ 2 z_{13} + \\ + z_{23}(a_{13} - a_{12}) - z_{33}(a_{12} + a_{13}))$$

e $(2, b_{13} - b_{12}, -(b_{12} + b_{13}))$ respectivamente.

$$2 z_{12} + (a_{13} - a_{12}) z_{22} - (a_{12} + a_{13}) z_{32} = b_{13} - b_{12}$$

$$2 z_{13} + (a_{13} - a_{12}) z_{23} - (a_{12} + a_{13}) z_{33} = -(b_{12} + b_{13})$$

Se $2 | (a_{13} - a_{12}) \implies 2 | a_{13} + a_{12}$ logo $2 | b_{13} - b_{12}$.

Temos que

$$\begin{pmatrix} z_{22} & z_{32} \\ z_{23} & z_{33} \end{pmatrix} \begin{pmatrix} a_{13} - a_{12} \\ -(a_{12} + a_{13}) \end{pmatrix} = \begin{pmatrix} b_{13} - b_{12} - 2\, z_{12} \\ -(b_{12} + b_{13}) - 2\, z_{13} \end{pmatrix}$$

Como $\begin{pmatrix} z_{22} & z_{32} \\ z_{23} & z_{33} \end{pmatrix}$ é inversível, existem γ_{11}, γ_{12}, γ_{21}, $\gamma_{22} \in Z$ tais que

$$a_{13} - a_{12} = \gamma_{11}(b_{13}-b_{12}) - 2\gamma_{11}z_{12} - \gamma_{12}(b_{12}+b_{13}) - 2\gamma_{12}z_{13}$$

$$-(a_{13}+a_{12}) = \gamma_{21}(b_{13}-b_{12}) - 2\gamma_{21}z_{12} - \gamma_{22}(b_{12}+b_{13}) - 2\gamma_{22}z_{13}$$

Logo se $2|b_{13}-b_{12}$, então $2|a_{13}-a_{12}$. Então $A \underset{Z}{\sim} B$ implica que $a_{13} - a_{12} \equiv (b_{13} - b_{12}) \pmod 2$.

Falta provar a recíproca, ou seja que se $a_{13}-a_{12} \equiv (b_{13}-b_{12}) \pmod 2$, então $A \underset{Z}{\sim} B$.

Seja $C = \begin{pmatrix} 1 & z_{12} & z_{13} \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$ onde

$$z_{12} = \frac{1}{2}((b_{13} - b_{12}) + (a_{12} + a_{13}))$$

$$z_{13} = \frac{1}{2}(-(b_{12} + b_{13}) + (a_{13} - a_{12}))$$

Então $AC = CB$; z_{12} e z_{13} são inteiros pois :

$a_{13} - a_{12} \equiv (b_{13} - b_{12}) \pmod 2$

c.q.d.

LEMA II.5.2.

Seja G um grupo cíclico de ordem 4. Seja I = Ker ε a representação inteira associada ao ideal de aumentação. Então as representações inteiras de G que são equivalentes sobre $\mathbb{Q}$ com I, se partem em duas classes de equivalência sobre Z. Numa classe estão Ker ε e todas indecomponíveis (como ZG-módulos) na outra todas as decomponíveis.

DEMONSTRAÇÃO

Como o grupo G é um grupo cíclico de ordem 4, as representações de G ficam determinadas por matrizes $\tilde{A} = (a_{ij})_{\substack{1 \leq i \leq 3 \\ 1 \leq j \leq 3}}$ que verificam $\tilde{A}^4 = I$, $a_{ij} \in Z$, $\det \tilde{A} = \pm 1$.

Seja $G = \{1, \sigma, \sigma^2, \sigma^3\}$, Ker $\varepsilon = \{a_1(\sigma-1) + a_2(\sigma^2-1) + a_3(\sigma^3-1) \mid a_i \in Z\}$

Logo uma matriz associada a I, está dada por

$$\sigma(\sigma-1) = \sigma^2 - \sigma = -(\sigma-1) + (\sigma^2-1)$$
$$\sigma(\sigma^2-1) = \sigma^3 - \sigma = -(\sigma-1) + \qquad + (\sigma^3-1)$$
$$\sigma(\sigma^3-1) = 1 - \sigma = -(\sigma-1)$$

Ou seja que uma tal matriz é $B_0 = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

Se B_0 está dada na base canônica (e_1, e_2, e_3) consideramos a base

$$f_1 = e_1 - e_2 + e_3$$
$$f_2 = e_2$$
$$f_3 = e_3$$

Então

$B_0(f_1) = - f_1$

$B_0(f_2) = - f_1 - f_2 + 2 f_3$

$B_0(f_3) = - f_1 - f_2 + f_3$

Então

$$B_0 \underset{Z}{\sim} \begin{pmatrix} -1 & -1 & -1 \\ 0 & -1 & -1 \\ 0 & 2 & 1 \end{pmatrix} = B$$

Seja A_0 uma matriz arbitrária a coeficientes inteiros equivalente sobre $\mathbb{Q}$ com B.

$A_0 \underset{\mathbb{Q}}{\sim} B$, então $\chi_{A_0} = \chi_B = -(\lambda+1)(\lambda^2+1)$ (onde χ_A indicará no futuro o polinômio característico de A).

Então A_0 tem o valor próprio -1, ou seja $A_0 \underset{Z}{\sim} \begin{pmatrix} -1 & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix}$ (Ver Corolário I.6.1).

Seja $A' = \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix}$ e $B' = \begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}$

Sabemos que $-(\lambda+1)(\lambda^2+1) = (-1-\lambda)\chi_{A'} = -(\lambda+1)\chi_{B'}$. Logo $\chi_{A'} = \chi_{B'} = \lambda^2 + 1$

Então $A' \underset{Z}{\sim} B' \underset{Z}{\sim} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = C'$ (Ver Corolário I.6.2)

Em definitivo, temos que

$$A \underset{Z}{\sim} \begin{pmatrix} -1 & \tilde{a}_{12} & \tilde{a}_{13} \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} = \overline{A}$$

$$B \underset{Z}{\sim} \begin{pmatrix} -1 & \tilde{b}_{12} & \tilde{b}_{13} \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} = \overline{B}$$

Aplicando o Lema II.5.1. temos que $A_0 \underset{Z}{\simeq} \bar{B}$ se e somente se:

$\tilde{a}_{12} - \tilde{a}_{13} \equiv \tilde{b}_{12} - \tilde{b}_{13} \pmod 2$.

Para completar a demonstração do teorema só falta provar que $\bar{B}$ é indecomponível. Para isso precisamos saber como passar de B a $\bar{B}$.

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Então tomando

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \quad \text{temos que } C^{-1}BC = \bar{B}$$

$$C^{-1}BC = \begin{pmatrix} -1 & 0 & -1 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} = \bar{B}$$

Como consequência do Lema II.5.1. temos que $\bar{B} \underset{Z}{\not\simeq} \begin{pmatrix} -1 & 0 & -1 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$ ou seja, $\bar{B}$ não é decomponível.

c.q.d.

EXEMPLO II.5.1.

Seja $m = 2^4 = 16$, ζ uma raiz primitiva de ordem 2^4 de 1.

$[Q(\zeta):Q] = \phi(2^4) = 2^3 = 8$ (Onde ϕ é a função de Euler)

$\dim_{Q(\zeta+\zeta^{-1})} Q(\zeta) = 2$ pois $\zeta^2 - (\zeta+\zeta^{-1})\zeta + 1 = 0$

Então temos que $\dim_Q Q(\zeta+\zeta^{-1}) = 4$.

$$\begin{tikzcd} Q(\zeta) \arrow[dash, rd, "2"] \arrow[dash, d, "8"'] & \\ Q & Q(\zeta+\zeta^{-1}) \arrow[dash, l, "4"] \end{tikzcd}$$

$$\zeta + \zeta^{-1} = 2\cos \pi/8 = 2\sqrt{\frac{1+\cos\pi/4}{2}} =$$

$$= 2\sqrt{\frac{1+\frac{\sqrt{2}}{2}}{2}} = \sqrt{2+\sqrt{2}} = \alpha$$

$Irr(\zeta+\zeta^{-1},Q) = Irr(\alpha,Q) = x^4 - 4x^2 + 2$

Temos que as raízes de $Irr(\alpha,Q)$ são $x_1 = \sqrt{2+\sqrt{2}}$, $x_2 = -\sqrt{2+\sqrt{2}}$,

$x_3 = \sqrt{2-\sqrt{2}}$, $x_4 = -\sqrt{2-\sqrt{2}}$

$x_1x_3 = \sqrt{4-2} = \sqrt{2} = x_1^2 - 2$. Então $x_3 = x_1 - \dfrac{2}{x_1}$

$x_1^4 - 4x_1^2 + 2 = 0$, logo $-2/x_1 = x_1^3 - 4x_1$ então $x_3 = x_1^3 - 3x_1$

Seja $\sigma \in Gal(Q(\zeta+\zeta^{-1}),Q)$ $\sigma(x_1) = x_3$

É facil verificar que $\sigma(x_3) = x_2 = -x_1$

Temos então que $\sigma^4 = Id$ é o grupo de Galois $G=Gal(Q(\zeta+\zeta^{-1}),Q)$

$\cong Z/4Z$. $G = \{ 1, \sigma, \sigma^2, \sigma^3 \}$. Também poderíamos ter deduzido que $G \cong Z_{/4Z}$ usando [14] pag.599.

Os inteiros de $Q(\zeta+\zeta^{-1})$ são $Z[\zeta+\zeta^{-1}] = Z[\sqrt{2+\sqrt{2}}]$ pelo seguinte raciocínio. Sejam $\mathcal{O}$ os inteiros de $Q(\zeta+\zeta^{-1})$. É claro que:
$Z[\zeta+\zeta^{-1}] \subset \mathcal{O}$

Como os inteiros de $Q(\zeta)$ são $Z[\zeta]$ e $Z[\zeta]\cap Q(\zeta+\zeta^{-1})=Z[\zeta+\zeta^{-1}]$ se deduz que $Z[\zeta+\zeta^{-1}] = \mathcal{O}$

Um conjunto de inversíveis fundamentais de $\mathcal{O}$ está dado por

$$\varepsilon_1 = 1 + 2x_1 + x_1^2$$
$$\varepsilon_2 = 1 - 2x_1^2$$
$$\varepsilon_3 = -1 + 4x_1^2 + 2x_1^3$$

e seus inversos são

$$\varepsilon_1^{-1} = 11 - 14x_1 - 3x_1^2 + 4x_1^3$$
$$\varepsilon_2^{-1} = -7 + 2x_1^2$$
$$\varepsilon_3^{-1} = -1 + 4x_1^2 - 2x_1^3$$

$$\sigma(\varepsilon_1) = 5 - 6x_1 - x_1^2 + 2x_1^3$$
$$\sigma(\varepsilon_2) = -7 + 2x_1^2$$
$$\sigma(\varepsilon_3) = 15 - 20x_1 - 4x_1^2 + 6x_1^3$$

Uma verificação imediata nos permite comprovar que

$$\sigma(\varepsilon_1) = \varepsilon_1^{-1}\varepsilon_3$$
$$\sigma(\varepsilon_2) = \varepsilon_2^{-1}$$
$$\sigma(\varepsilon_3) = -\varepsilon_1^{-2}\varepsilon_2\varepsilon_3$$

Logo a representação E, pensada como representação matricial, pode ser dada pela matriz 3×3 a coeficientes inteiros unimodular

$$A = \begin{pmatrix} -1 & 0 & -2 \\ 0 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Provaremos que $A \underset{Z}{\sim} \mathrm{Ker}\ \varepsilon$ para isso a levaremos à forma

$$A \underset{Z}{\sim} \begin{pmatrix} -1 & \alpha_{12} & \alpha_{13} \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$ com $\alpha_{13} - \alpha_{12}$ ímpar (Ver Lema II.5.2.)

Fazendo a mudança de base $f_1 = e_2$, $f_2 = e_1$, $f_3 = e_3$ temos

$$A \underset{Z}{\sim} \begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & -2 \\ 0 & 1 & 1 \end{pmatrix} = A'$$

Seja agora

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 0 \end{pmatrix} \qquad C^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$C^{-1}A'C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & -2 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} -1 & -1 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

Como det $C = +1$

$$A \sim_Z \begin{pmatrix} -1 & -1 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$ logo pelo Lema II.5.2 temos que $A \sim_Z \operatorname{Ker} \varepsilon$.

EXEMPLO II.5.2.

Seja o polinômio $f(x) = x^4 - 5x^2 + 1$ as raízes desse polinômio são todas reais e iguais a $\alpha = \sqrt{\frac{5+\sqrt{21}}{2}}$, $\alpha^* = \sqrt{\frac{5-\sqrt{21}}{2}}$, $-\alpha$, $-\alpha^*$.

Como $\alpha\alpha^* = \sqrt{\frac{25-21}{4}} = 1$, $\alpha^* = \alpha^{-1}$. Consequentemente a extensão $K = Q(\sqrt{\frac{5+\sqrt{21}}{4}}) = Q(\alpha)$ é normal de grau 4 sobre Q.

Como $1 = 5\alpha^2 - \alpha^4$, $\alpha^{-1} = 5\alpha - \alpha^3$ ou seja que $\alpha^* = 5\alpha - \alpha^3$

Os automorfismos de K que deixam Q fixo são

$1 : \alpha \longrightarrow \alpha$

$\sigma : \alpha \longrightarrow \alpha^* = \alpha^{-1} = 5\alpha - \alpha^3 = \sqrt{\frac{5-\sqrt{21}}{4}}$

$\tau : \alpha \longrightarrow -\alpha = -\sqrt{\frac{5+\sqrt{21}}{4}}$

$\sigma\tau=\tau\sigma : \alpha \longrightarrow -\alpha^* = -\sqrt{\frac{5-\sqrt{21}}{4}} = -5\alpha + \alpha^3 = \alpha^{-1}$

É claro então que $\operatorname{Gal}(K,Q) \cong Z/_{2Z} \times Z/_{2Z}$. De acordo com [5], pag.200 os inteiros de K são exatamente os elementos do anel $Z[\alpha]$.

Cada automorfismo σ, τ, $\sigma\tau$ deixa fixo um subcorpo quadrático de K, logo para procurar inversíveis em K, os procuramos nesses corpos quadráticos.

Sejam F_τ, F_σ e $F_{\tau\sigma}$ os corpos fixos de σ, τ e $\sigma\tau$ respectivamente.

$F_\tau = Q(\sqrt{21})$ pois $\sqrt{21} = 2\alpha^2 - 5$ $\quad \tau(\sqrt{21}) = 2(\tau(\alpha))^2 - 5 = 2\alpha^2 - 5$.

$F_\sigma = Q(\sqrt{7}) = Q(\alpha+\alpha^*)$ pois $(\alpha+\alpha^*)^2 = \alpha^2 + \alpha^{*2} + 2 = \dfrac{5+\sqrt{21}}{2} +$

$+ \dfrac{5-\sqrt{21}}{2} + 2 = 7$ e $\sigma(\alpha+\alpha^*) = \sigma(\alpha) + \sigma(\alpha^*) = \alpha^* + \alpha$.

$F_{\sigma\tau} = Q(\sqrt{3}) = Q(\alpha-\alpha^*)$ pois $(\alpha-\alpha^*)^2 = \alpha^2 + \alpha^{*2} - 2 = 5 - 2 = 3$

$\sigma\tau(\alpha-\alpha^*) = \sigma\tau(\alpha-\sigma\alpha) = \sigma\tau\alpha - \tau\alpha = -\alpha^* + \alpha = \alpha - \alpha^*$

Consideremos então em $F_\sigma = Q(\sqrt{7})$ o inversível $\varepsilon_2 = 8 + 3\sqrt{7}$

$\varepsilon_2^{-1} = 8 - 3\sqrt{7}$

$\varepsilon_2 = 8 + 3(\alpha+\alpha^*) = 8 + 3(\alpha+5\alpha-\alpha^3) = 8 + 18\alpha - 3\alpha^3$

$\varepsilon_2^{-1} = 8 - 3(\alpha+\alpha^*) = 8 - 3(6\alpha-\alpha^3) = 8 - 18\alpha + 3\alpha^3$

Consideremos agora em $F_{\sigma\tau} = Q(\sqrt{3})$ o inversível $\varepsilon_3 = 2 + \sqrt{3}$

$\varepsilon_3^{-1} = 2 - \sqrt{3}$

$\varepsilon_3 = 2 + \sqrt{3} = 2 + (\alpha-\alpha^*) = 2 + (\alpha-5\alpha+\alpha^3) = 2 - 4\alpha + \alpha^3$

$\varepsilon_3^{-1} = 2 - \sqrt{3} = 2 - (\alpha-\alpha^*) = 2 - (\alpha-5\alpha+\alpha^3) = 2 + 4\alpha - \alpha^3$

Consideremos então em $Q(\alpha)$ o conjunto de inversíveis fundamentais $\quad \varepsilon_1 = \alpha$

$\varepsilon_2 = 8 + 18\alpha - 3\alpha^3 = 8 + 3(\alpha+\alpha^*)$

$\varepsilon_3 = 2 - 4\alpha + \alpha^3 = 2 + (\alpha-\alpha^*)$

Calcularemos agora a representação matricial de G associada a

E : $\sigma(\varepsilon_1) = \sigma(\alpha) = \alpha^{-1} = \varepsilon_1^{-1}$

$\sigma(\varepsilon_2) = \qquad = \varepsilon_2$ pois $\varepsilon_2 \in F_\sigma$

$\sigma(\varepsilon_3) = 2 + \sigma\alpha - \sigma\alpha^* = 2 + \alpha^* - \alpha = 2 - (\alpha - \alpha^*) = \varepsilon_3^{-1}$

$\tau(\varepsilon_1) = -\varepsilon_1$

$\tau(\varepsilon_2) = 8 + 3(\tau\alpha + \tau\alpha^*) = 8 - 3(\alpha+\alpha^*) = \varepsilon_2^{-1}$

$\tau(\varepsilon_3) = 2 - (\alpha - \alpha^*) \qquad = \varepsilon_3^{-1}$

Uma representação matricial associada a E é então

$$\sigma \longrightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \qquad \tau \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \qquad (*)$$

Calculemos agora uma representação matricial associada a I

$I = \{ a(\sigma-1) + b(\tau-1) + c(\sigma\tau-1) \mid a,b,c \in Z \}, \sigma^2 = 1 \ , \ \tau^2 = 1$

$\sigma\tau = \tau\sigma$

$\sigma(\sigma-1) = \sigma^2 - \sigma = 1 - \sigma = -(\sigma-1)$

$\sigma(\tau-1) = \sigma\tau - \sigma = \qquad = -(\sigma-1) \qquad + (\sigma\tau-1)$

$\sigma(\sigma\tau-1) = \tau - \sigma = \qquad = -(\sigma-1) + (\tau-1)$

$\tau(\sigma-1) = \tau\sigma - \tau \qquad = \qquad -(\tau-1) + (\sigma\tau-1)$

$\tau(\tau-1) = \qquad = \qquad -(\tau-1)$

$\tau(\sigma\tau-1) = \sigma - \tau \qquad = (\sigma-1) - (\tau-1)$

Uma representação matricial associada a I é então

$$\sigma \longrightarrow \begin{pmatrix} -1 & -1 & -1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad \tau \longrightarrow \begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix} \qquad (**)$$

As representações (*) e (**) são equivalentes sobre Q. Por outro lado provaremos diretamente que não existe $C = (z_{ij})$ com $\det C = \pm 1$, $z_{ij} \in Z$ tal que

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix} = \begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix}\begin{pmatrix} -1 & -1 & -1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Pois teríamos

$$\begin{pmatrix} -z_{11} & -z_{12} & -z_{13} \\ z_{21} & z_{22} & z_{23} \\ -z_{31} & -z_{32} & -z_{33} \end{pmatrix} = \begin{pmatrix} -z_{11} & -z_{11}+z_{13} & -z_{11}+z_{12} \\ -z_{21} & -z_{21}+z_{23} & -z_{21}+z_{22} \\ -z_{31} & -z_{31}+z_{33} & -z_{31}+z_{32} \end{pmatrix}$$

Da igualdade das segundas linhas tiramos que $z_{21} = 0$, $z_{22}=z_{23}$. das primeiras linhas $z_{12} = z_{11} - z_{13}$, das terceiras $z_{32}=z_{31} - z_{33}$.

Então

$$C = \begin{pmatrix} z_{11} & z_{11}-z_{13} & z_{13} \\ 0 & z_{23} & z_{23} \\ z_{31} & z_{31}-z_{33} & z_{33} \end{pmatrix}$$

$$\det C = \det\begin{pmatrix} z_{11} & z_{11}-2z_{13} & z_{13} \\ 0 & 0 & z_{23} \\ z_{31} & z_{31}-2z_{33} & z_{33} \end{pmatrix} = -z_{23}\det\begin{pmatrix} z_{11} & z_{11}-2z_{13} \\ z_{31} & z_{31}-2z_{33} \end{pmatrix}$$

$$= -z_{23}\det\begin{pmatrix} z_{11} & -2z_{13} \\ z_{31} & -2z_{33} \end{pmatrix} = 2z_{23}\det\begin{pmatrix} z_{11} & z_{13} \\ z_{31} & z_{33} \end{pmatrix} \neq \pm 1.$$

Em consequência $E \not\cong_Z \operatorname{Ker} \varepsilon$

Para o caso $n = 5$ e em geral $n = p$ com p primo, precisamos estudar melhor o problema de Z-equivalência de matrizes, com polinômio característico dado.

SEÇÃO II.6. A Z-EQUIVALÊNCIA DE MATRIZES

Duas matrizes A e $B \in M_n(Z)$ dizem-se Z-equivalentes $A \underset{Z}{\sim} B$ se existe $C \in M_n(Z)$, C unimodular tal que $A = C^{-1}BC$ (Ver [12] pag.49).

TEOREMA II.6.1.

Seja $A \in M_n(Z)$. Então A é Z-equivalente a uma matriz de blocos da forma

$$\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1p} \\ 0 & A_{22} & \cdots & A_{2p} \\ \vdots & & & \\ 0 & 0 & \cdots & A_{pp} \end{bmatrix}$$

Onde p é o número de fatores irredutíveis de χ_A sobre Q, e os $\chi_{A_{ii}}$ são irredutíveis sobre Q para $1 \leq i \leq p$. (χ_T indicará o polinômio característico da matriz T).

DEMONSTRAÇÃO

Faremos a demonstração por indução em p, onde p é o número de fatores irredutíveis mônicos de χ_A.

Se $p = 1$, não temos nada para demonstrar.

Suponhamos que o resultado está provado para toda matriz B com polinômio característico χ_B com menos de p fatores irredutíveis mônicos a coeficientes inteiros, e seja A uma matriz com p fatores irredutíveis mônicos a coeficientes inteiros, $A \in M_n(Z)$.

Seja g um fator irredutível fixo de χ_A • $\chi_A = g.h$

Seja θ uma raiz de g e seja $K = Q(\theta)$. Como g é irredutível, $\mathrm{gr}\, g = \dim_Q K = k$. Seja K^* o anel dos inteiros de K, e seja $\{\omega_1, \ldots, \omega_k\}$ uma base fundamental de K^* (i.e. todo $\alpha \in K^*$ se escreve como $\alpha = \sum_{i=1}^{k} z_i\omega_i$ com $z_i \in Z$ e $\omega_1, \ldots, \omega_k$ uma base de K sobre Q).

O sistema $(A-\theta I)x = 0$ tem alguma solução em K^n (pois $\det(A-\theta I) = X_A(\theta) = g(\theta)h(\theta) = 0$). Multiplicando uma solução fixa por um inteiro adequado podemos achar $x \in K^{*n}$ que verifica $Ax=\theta x$. Seja agora uma matriz $C \in M_{n,k}(Z)$ tal que $x = C\omega$ com $\omega = \begin{pmatrix}\omega_1\\ \vdots \\ \omega_k\end{pmatrix}$ e seja $B \in M_{k,k}(Z)$ tal que $\theta\omega = B\omega$

Então

$A C\omega = Ax = \theta x = \theta C\omega = CB\omega$ então como os ω_i são linearmente independentes sobre Z, dessa igualdade deduzimos que

$$AC = CB \qquad (a)$$

Seja agora $r \leq k \leq n$ o posto de C. Existem matrizes U e V unimodulares tais que $V \in M_{k,k}(Z)$, $U \in M_{n,n}(Z)$, $S \in M_{r,r}(Z)$ tais que

$$C = U \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} V \qquad (b)$$

com $\begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} \in M_{n,k}(Z)$

Seja agora $U^{-1}AU = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}$ (c)

com $A_1 \in M_{r,r}(Z)$

Temos que

$$U^{-1}AC = U^{-1}CB = \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} VB \quad \text{(aplicando (a) e (b)),} \quad e,$$

$$U^{-1}AC = U^{-1}AUU^{-1}C = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix} \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} V \quad \text{(aplicando (c) e (b)).}$$

Temos então que

$$\begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} VB = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix} \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} V$$

Ou seja chamando $VB = \begin{bmatrix} T_1 & T_2 \\ T_3 & T_4 \end{bmatrix}$ e $V = \begin{bmatrix} V_1 & V_2 \\ V_3 & V_4 \end{bmatrix}$

temos que

$$\begin{bmatrix} s & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} T_1 & T_2 \\ T_3 & T_4 \end{bmatrix} = \begin{bmatrix} A_1S & 0 \\ A_3S & 0 \end{bmatrix} \begin{bmatrix} V_1 & V_2 \\ V_3 & V_4 \end{bmatrix}$$

Ou seja que $A_3SV_1 = 0$ como S e V são inversíveis deduzimos que $A_3 = 0$

Provaremos agora que $X_{A_1} = g$

$$\begin{bmatrix} A_1 & A_2 \\ 0 & A_4 \end{bmatrix} \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} V = \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} VB$$

Aplicando esse igualdade ao vetor ω temos se $V\omega = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ que:

$$\begin{bmatrix} A_1 & A_2 \\ 0 & A_4 \end{bmatrix} \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} V(\theta\omega) = \theta \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Então temos que

$$A_1 S\alpha = \theta S\alpha \qquad (d)$$

Por outro lado $S\alpha \neq 0$ pois se $S\alpha = 0 \Rightarrow \alpha = 0$. Então

$V\omega = \begin{bmatrix} 0 \\ \beta \end{bmatrix}$. Usando (b) temos que $x = C\omega = U \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \beta \end{bmatrix} = 0$.

Então $X_{A_1}(\theta) = 0$. Temos que $X_A = X_{A_1} X_{A_4} = gh$, g irredutível.

Se $g \not| X_{A_1}$ existem polinômios R e S tais que $Rg + S X_{A_1} = 1$,

mas $g(\theta) = X_{A_1}(\theta) = 0$. Então g / X_{A_1}. Mas $gr(g) = gr(X_{A_1})$ então $g = X_{A_1}$.

X_{A_1} é irredutível mônico a coeficientes inteiros. Por indução se deduz o resultado do teorema.

c.q.d.

Agora estamos em condições de demonstrar um resultado sobre a Z-equivalência de matrizes em Z com polinômio característico (e minimal) irredutível sobre Q.

TEOREMA II.6.2.

Existe só um número finito de classes de equivalência de matrizes $A \in M_n(Z)$ tais que $f(A) = 0$, onde f é um polinômio mônico de grau n, com coeficientes inteiros, irredutível sobre Q. O número de classes de equivalência é o mesmo que o número de classes de ideais do anel $Z[\theta]$ onde θ é uma raiz arbitrária de f.

DEMONSTRAÇÃO

Seja θ uma raiz fixa de f.

Seja A uma matriz que verifica $f(A) = 0$, $A \in M_n(Z)$

Se χ_A e m_A indicam o polinômio característico e minimal A, temos que $\chi_A = m_A = f$ (como $f(A) = 0$ deduzimos que m_A/f; mas como f é irredutível $m_A = f/\chi_A$, e gr f = gr $\chi_A = n$ então $m_A = \chi_A = f$).

Seja $R = Z[\theta]$ e seja K = corpo de frações de R.

O sistema $(A - \theta I)x = 0$ tem solução não trivial em K^n e logo em R^n, pois $\det(A-\theta I) = \chi_A(\theta) = f(\theta) = 0$.

Seja $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ com $x_i \in R$, uma tal solução.

Seja agora $S_x = Z[x_1,\ldots,x_n] \subset R$. Veremos que S_x é um ideal de R. Evidentemente é um subgrupo abeliano de R. Como $\theta x = Ax$, $\theta S_x \subseteq S_x$ e como $R = Z[\theta]$, é claro que $RS_x \subset S_x$, ou seja, S_x ideal de R.

O que acontece se mudarmos o vetor próprio ? . Procuramos ver que relação existe entre S_x e S_y onde x e y verificam ambos $Ax = \theta x$, $Ay = \theta y$, $x,y \in R^n$. Como f é irredutível se deduz que a raiz θ, de f é simples. Daí sai imediatamente que: $\dim_K \mathrm{Ker}(A-\theta I) = 1$. Em consequência éxistem α e $\beta \in R$ tais que $\alpha x = \beta y$, então $\alpha S_x = \beta S_y$, ou seja, que S_x e S_y estão na mesma classe de ideais de R (Ver I.1.).

Dessa forma definimos uma correspondência entre as matrizes $A \in M_n(Z)$ que verificam $f(A) = 0$ e as classes de ideais de $R = Z[\theta]$, onde θ é uma raiz fixada de f.

Essa correspondência passa ao quociente módulo a relação de Z-equivalência de matrizes de $M_n(Z)$. Se $B = UAU^{-1}$ com U unimodular. Se $Ax = \theta x$ com $x \in R^n$, então $BUx = \theta Ux$ com $Ux \in R^n$. Logo os ideais S_x e $S_{Ux} \subset R$ coincidem (passamos de uma base de um a uma base de outro por uma matriz unimodular a coeficientes inteiros).

Seja agora $\mathcal{J}$ uma classe de ideais de R. Seja S um ideal de R, $S \subset R$, $S \in \mathcal{J}$.

Podemos achar elementos $x_1, \ldots, x_n \in R$ tais que $Z[x_1,\ldots,x_n] = R$. (Seja $x_1 \ldots x_r$ uma base de S -sobre Z- com $r < n$.

$$\theta x_i = \tilde{a}_{i1}x_1 + \quad + \tilde{a}_{ir}x_r \quad \text{então} \quad \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = (\tilde{A}-\theta I) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}$$

como os x_i não não nulos $\det(\tilde{A}-\theta I) = 0$. Então $\operatorname{gr} \operatorname{Irr}(\theta, Q) \leq r < n$, e isso é absurdo).

Seja agora $A \in M_n(Z)$ tal que $\theta x = Ax$ onde $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Daí deduzimos que $f(A)x = f(\theta)x = 0$ e como os $x_1 \ldots x_n$ são linearmente independentes sobre Z, vamos ter que $f(A) = 0$.

Seja agora um outro ideal T de R, $T \subset R$, $T \in \mathcal{J}$. Escrevemos $T = Z[y_1,\ldots,y_n]$ e vamos ter outra matriz B, tal que $\theta y = By$. Além disso existem $\alpha, \beta \in R$ tais que $\alpha S = \beta T$. Então $(\beta y_1, \ldots, \beta y_n)$ e $(\alpha x_1,\ldots,\alpha x_n)$ são ambas bases de $\alpha S = \beta T$. Em consequência existe uma matriz unimodular $U \in M_n(Z)$, tal que $\beta y = U\alpha x$.

Temos então que $\beta By = \theta\beta y = \theta U\alpha x = \alpha U\theta x = \alpha UAx$.

Mais $\beta By = B\beta y = BU\alpha x$. Então $UAx = BUx$, mas U é inversível, logo $(U^{-1}BU-A)x = 0$. Como $x_1, \ldots, x_n$ são linearmente independentes sobre Z, deduzimos que $A = U^{-1}BU$.

Pela forma em que definimos as correspondências anteriores é claro que são uma inversa da outra .

c.q.d.

Demonstraremos agora como corolários, duas propriedades anteriormente usadas.

COROLÁRIO II.6.1.

Seja $A \in M_n(Z)$ que possui um valor próprio inteiro $a \in Z$, então A é equivalente sobre Z a uma matriz cuja primeira coluna é $\begin{pmatrix} a \\ \vdots \\ 0 \end{pmatrix}$

DEMONSTRAÇÃO

Seja X_A o polibômio característico de A.

Então $X_A = (x-a)\ p_2(x) \ldots p_r(x)$ onde os p_i são irredutíveis sobre Q. Pelo Teorema II.6.1. temos que A é equivalente sobre Z a uma matriz da forma

$$\begin{bmatrix} A_{11} & A_{12} & \ldots & A_{1r} \\ 0 & A_{22} & \ldots & A_{2r} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & & A_{rr} \end{bmatrix} \quad \text{com } X_{A_{ii}} = p_i \text{ se } i \geq 2$$

$X_{A_{11}} = (x - a)$. Então A_{11} é uma matriz escalar $A_{11} = (a)$.

c.q.d.

COROLÁRIO II.6.2.

Todas as matrizes $A \in M_2(Z)$ que verificam $A^2 + I = 0$ são Z-equivalentes.

DEMONSTRAÇÃO

$f(x) = x^2 + 1$ é Q-irredutível, o anel $Z[i]$ (onde $i^2 = -1$) é um anel euclidiano, logo principal, logo o número de classes de ideais é 1.

c.q.d.

SEÇÃO II.7. O CASO DE UMA EXTENSÃO CÍCLICA

Seja K uma extensão cíclica dos racionais (ou seja, Gal(K,Q) é um grupo cíclico).

Seja n = ordem do grupo de Galois. Seja h(n) = número de classes de ideais de $Q(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade (Ver [3] pag.325). No caso em que n é primo e h(p) = 1 podemos assegurar a Z equivalência de E e I'.

Neste teorema daremos uma demonstração diferente da demonstração do [2] onde utiliza um teorema de Reiner e Diederichsen sobre a estrutura dos ZG-módulos onde G é cíclico de ordem primo (Ver [4] pag.503).

TEOREMA II.7.1.

Seja K uma extensão cíclica de Q, onde $|Gal(K,Q)| = p$ e $h(p)=1$ (p número primo). Então $E \cong I'$ como ZG-módulos.

DEMONSTRAÇÃO

Sejam A e B representações matriciais associadas a E e I' respectivamente. Ou seja, A e B são $A,B : G \longrightarrow M_r(Z)$. Para dar A e B basta conhecer as matrizes A(g) e B(g) onde g é um gerador do grupo cíclico G.

Seja $A(g) = A_0$, $B(g) = B_0$, $A_0, B_0 \in M_r(Z)$.

Sabemos que $A_0 \sim_Q B_0$ pelo teorema II.3.1. Precisamos provar que $A_0 \sim_Z B_0$. Do fato que $A_0 \sim_Q B_0$ se deduz que $X_{A_0} = X_{B_0} = f$.

Para aplicar o Teorema II.6.2. precisamos calcular X_{B_0}.

Temos duas possibilidades:

(a) p = 2. Nesse caso r = 1 ou r = 0. A segunda alternativa cai fora de nosso interesse. Podemos supor então que a extensão é real e r = 1. Nesse caso (o caso de posto 1) a Q-equivalência obviamente implica a Z-equivalência.

(b) p ímpar. Nesse caso a extensão deve ser real, ou seja $I' = I$.

$I = \{ a_1(\sigma-1) + a_2(\sigma^2-1) + \dots + a_{p-1}(\sigma^{p-1}-1) \mid a_i \in Z \}$

$G = \{ 1, \sigma, \dots, \sigma^{p-1} \}$

$$\sigma(\sigma-1) = \sigma^2 - \sigma = -(\sigma-1) + (\sigma^2-1)$$

$$\sigma(\sigma^2-1) = \sigma^3 - \sigma = -(\sigma-1) + \dots + (\sigma^3-1)$$

$$\vdots$$

$$\sigma(\sigma^j-1) = \sigma^{j+1} - \sigma = -(\sigma-1) + \dots\dots + (\sigma^{j+1}-1)$$

$$\vdots$$

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

Podemos supor que

$$B_0 = \begin{pmatrix} -1 & -1 & \dots & -1 \\ 1 & 0 & & . \\ 0 & 1 & & . \\ \vdots & \vdots & & \vdots \\ 0 & 0 & 1 & 0 \end{pmatrix}$$. Então é claro que $X_{B_0} = \Phi_p$,

onde Φ_p é o p-ésimo polinômio ciclotônico , ou seja,

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

É um fato bem conhecido que Φ_p é irredutível sobre Q.

Então tanto A_0 como B_0 verificam o p-ésimo polinômio ciclotônico. Elas são também matrizes $A_0, B_0 \in M_{p-1}(Z)$. Em consequência como estamos trabalhando nas hipóteses de que $h(p) = 1$, $A_0 \sim_Z B_0$, como consequência do Teorema II. 6.2.

c.q.d.

Este resultado nos permite liquidar o problema da Z-equivalência para todas as extensões cíclicas de ordem primo $\underline{p}$ dos racionais com $p \leq 19$. Ou seja, para os primos 2, 3, 5, 7, 11, 13, 17, 19 que são os únicos primos menores que 100 para os quais $h(p) = 1$.

Não é sabido se existem um número finito ou infinito de primos p, para os quais $h(p) = 1$.

No caso de um grupo cíclico de ordem primo arbitrário, podemos assegurar que as representações dadas pelas matrizes A_0 e B_0 (como antes), verificam ambas o polinômio $\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1$ e uma dela tem uma matriz associada da forma

$$B_0 = \begin{pmatrix} -1 & -1 & \dots & -1 \\ 1 & 0 & & . \\ 0 & 1 & & . \\ \vdots & \vdots & & \vdots \\ 0 & 0 \,..\, 1 & & 0 \end{pmatrix}$$

Podemos então identificar a classe de ideais de $Z[\zeta]$ (com $\zeta^p = 1$, $\zeta \neq 1$), com a qual a classe das matrizes Z equivalentes com B_0 está em correspondência biunívoca.

Resolveremos o problema da Z-equivalência de A_0 com B_0 se pudermos comprovar que a classe de ideais que corresponde a A_0 coincide com a classe de ideais (conhecida) que corresponde a B_0. Nesse sentido podemos enunciar o seguinte teorema.

TEOREMA II.7.2.

Seja K uma extensão cíclica de ordem primo, de Q ($\dim_Q K = p$) $p>2$. A representação E é isomorfa sobre ZG com $I' = I$ se e somente se a classe de ideais de $Z[\zeta]$ (ζ raiz primitiva de ordem p de 1) associada a E de acordo com o Teorema II.6.2., contém a $Z[\zeta]$. Em outras palavres, se essa classe de ideais consta só de ideais principais.

DEMONSTRAÇÃO

De acordo com o teorema II.6.2 basta provar que a classe de ideais de $Z[\zeta]$ associada com I é a classe dos ideais principais. Sabemos que I está determinado (ver demonstração do Teorema II.7.1.) pela matriz

$$B_0 = \begin{pmatrix} -1 & -1 & \dots & -1 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots 1 & 0 \end{pmatrix}$$

Um vetor próprio correspondente ao vetor próprio ζ dessa matriz é

$$x = \begin{pmatrix} \zeta^{p-2} \\ \zeta^{p-3} \\ \vdots \\ \zeta \\ 1 \end{pmatrix} \quad \text{pois}$$

$$\begin{pmatrix} -1 & -1 & \dots & -1 \\ 1 & 0 & \dots & 0 \\ . & 1 & & . \\ \vdots & \vdots & & . \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \zeta^{p-2} \\ \zeta^{p-3} \\ \vdots \\ \zeta \\ 1 \end{pmatrix} = \zeta \begin{pmatrix} \zeta^{p-2} \\ \zeta^{p-3} \\ \\ \zeta \\ 1 \end{pmatrix}$$

como se comprova imediatamente dado que:

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

Olhando para a demonstração do Teorema II.6.2. observamos que a classe de ideais de $Z[\zeta]$ associada com I é a classe de ideais que contém $Z[1,\zeta,\zeta^2,\ldots,\zeta^{p-2}]$, ou seja a classe dos ideais principais.

c.q.d.

C A P Í T U L O   III

SEÇÃO III.1   CORPOS CICLOTÔMICOS

Seja p um primo arbitrário e seja ξ uma raiz primitiva de ordem p^a, de 1 $(p > 2)$.

O polinômio ciclotômico $\Phi_{p^a}(X) = Irr(\xi, Q)$ se escreve como

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

Também sabemos $\dim_Q Q(\xi) = gr(\Phi_{p^a}(X)) = \phi(p^a) = p^{a-1}(p-1)$ onde ϕ é a função de Euler.

Sabemos também que $\Phi_{p^a}(X) = \prod_{(i,p^a)=1} (X - \xi^i)$ onde (m,n) indica o máximo divisor comum entre m e n.

Fazendo na equação anterior $X = 1$ temos

$$p = \prod_{(i,p^a)=1} (1 - \xi^i)$$

Indicaremos com $\mathcal{O}$ o conjunto dos inteiros de $Q(\xi)$. Se $(i,p^a) = 1$ então $(1 - \xi^i)$ e $(1 - \xi)$ são associados em $\mathcal{O}$ pois

$$\frac{1 - \xi^i}{1 - \xi} = 1 + \xi + \ldots + \xi^{i-1} \in \mathcal{O}.$$

Se escolhemos j e ℓ, tais que $ji + \ell p^a = 1$ $(\xi^i)^j = \xi$ então

$$\frac{1-\xi}{1-\xi^i} = \frac{1-(\xi^i)^j}{1-\xi^i} = 1+\xi^i+\ldots+\xi^{(j-1)i} \in \mathcal{O}.$$

Como $(\{i: (i,p^a) = 1\}) = \phi(p^a) = p^{a-1}(p-1)$, temos que $p = \varepsilon(1-\xi)^{p^{a-1}(p-1)}$ com ε inversível em $\mathcal{O}$.

Seja agora um primo P de $Q(\xi)$ que está sobre p.

$$\nu_P(p) = e = \nu_P(\varepsilon(1-\xi)^{p^{a-1}(p-1)}) = p^{a-1}(p-1)\ \nu_P(1-\xi)$$

onde $\underline{e}$ é o índice de ramificação de P, e ν_P indica a valorização P-ádica associada ao primo P.

Dessa igualdade deduzimos que $\nu_P(1-\xi) \neq 0$ e que $e \geq p^{a-1}(p-1)$. Como $p^{a-1}(p-1) = \dim_Q Q(\xi)$, deduz-se que $e = p^{a-1}(p-1)$ e que $\nu_P(1-\xi) = 1$.

Sabemos que (ver I.1) se $P_1,\ldots,P_t$ são primos de $Q(\xi)$ que estão sobre p, e $\underline{e}_i$ e $\underline{f}_i$ são seus respectivos índices de ramificação e graus de inércia, então

$$\sum_{i=1}^{t} e_i\ f_i = p^{a-1}(p-1) = \dim_Q\ Q(\xi).$$

Como $e_i = p^{a-1}(p-1)$ para todo $i = 1,\ldots,t$ temos que $t = 1$, ou seja

$$p = P^{p^{a-1}(p-1)}$$

Usaremos também no futuro o fato que

$$\{1,\xi,\ldots,\xi^{p^{a-1}(p-1)-1}\}$$

é uma base fundamental de $Q(\xi)$ sobre Q. (ver [3] pg.327)

No caso $a=1$, precisaremos conhecer o discriminante do corpo $Q(\xi)$. Se D = discriminante de $Q(\xi)$, usando a base fundamental $\{\xi,\xi^2,\ldots,\xi^{p-1}\}$ temos que $D = \det((Tr(\xi^{i+j})_{1\leq i,j\leq p-1}))$. Se $s \not\equiv 0 \pmod p$ o polinômio $Irr(\xi^s,Q) = X^{p-1}+X^{p-2}+\ldots+X+1$ então $Tr(\xi^s) = -1$.

Se $s \equiv o \pmod p$ $\xi^s = 1$. Então $Tr(\xi^s) = \dim_Q Q(\xi) = p-1$. Definitivamente, temos que

$$D = (-1)^{\frac{p-1}{2}}\, p^{p-2} \quad \text{se} \quad p > 2.$$

No caso $p = 2$, alguns resultados anteriores são válidos.

Seja ξ uma raiz de ordem 2^a de 1. Suponhamos $a > 1$. (o caso $a = 1$ carece de interesse)

$$\Phi_{2^a}(X) = Irr(\xi,Q) = X^{2^{a-1}} + 1, \quad \dim_Q Q(\xi) = 2^{a-1}$$

Como antes temos que 2 se ramifica totalmente em $Q(\xi)$.

$$2 = P^{2^{a-1}}.$$

Também podemos provar que uma base fundamental de $Q(\xi)$ está dada por $\{1,\xi,\ldots,\xi^{2^{a-1}-1}\}$.

SEÇÃO III.2 ESTUDO DE UMA EXTENSÃO PARTICULAR

Seja p, um primo arbitrário e seja K um corpo de números algébricos que contém todas as raízes p-ésimas de 1. Seja $\alpha \in K$ e consideremos L = corpo de decomposição do polinômio $x^p-\alpha$. Vamos supor também que α é inversível em K. (α inteiro em K)

Vamos provar o seguinte: L é uma extensão abeliana de K e em K os únicos primos de K que eventualmente se ramificam são aqueles que estão sobre p $\in$ Q.

Seja $w_o \in L$ um elemento que verifica $w_o^p = \alpha$. As raízes da equação $x^p - \alpha = 0$ são $\{w_o, w_o\,\xi, \ldots, w_o\,\xi^{p-1}\}$ onde ξ é uma raiz p-ésima primitiva de um.

É claro que $L = K(w_o)$. Os automorfismos de L estão determinados por seu valor em w_o. Então $\forall\, \sigma \in Gal(L,K)$ $\sigma(w_o) = \xi^{n(\sigma)} w_o$.

Temos então uma aplicação

$$n: Gal(L,K) \longrightarrow F_p \qquad (F_p = \text{grupo cíclico de ordem } p)$$

É fácil verificar que n é um homomorfismo do grupo multiplicativo Gal(L,K) no grupo aditivo F_p.

Se $n(\sigma) = 0$ $\sigma(w_o) = w_o$ então $\sigma = Id_L$. Então n é injetora. Em consequência o grupo Gal(L,K) é isomorfo a F_p ou trivial (isso acontece se $w_o \in K$).

Se a extensão é trivial (L = K) nenhum primo de K se ramifica em L.

No caso em que a extensão não é trivial temos que Gal(L,K) é isomorfo a F_p. Logo a extensão L é abeliana e $\dim_K L = p$.

Provaremos que nesse caso os únicos primos que eventualmente se ramificam são aqueles que estão sobre p.

Para isso calcularemos o discriminante da extensão $\begin{smallmatrix} L \\ | \\ K \end{smallmatrix}$.

Seja uma base $x_1 \ldots x_p$ arbitrária de L sobre K. Indicaremos com $\Delta(x_1 \ldots x_p)$ ao discriminante dessa base.

$$\Delta(1, w_o, \ldots, w_o^{p-1}) = \prod_{0 \le i < j \le p-1} (w_o^{(i)} - w_o^{(j)})^2$$

onde $w_o^{(i)}$ e $w_o^{(j)}$ indicam os conjugados de w_o.

Então

$$\Delta(1,w_0,\dots,w_0^{p-1}) = \prod_{0\leq i<j\leq p-1} (w_0\ \xi^i - w_0\ \xi^j)^2 =$$

$$= \prod_{0\leq i<j\leq p-1} w_0^2(\xi^i - \xi^j)^2 = w_0^r \cdot \prod_{0\leq i<j\leq p-1} (\xi^i - \xi^j)^2.$$

Nessa expressão aparece o discriminante do corpo ciclotômico p-ésimo. Então (ver seção III.1):

$$\Delta(1,w_0,\dots,w_0^{p-1}) = w_0^r(-1)^{\frac{p-1}{2}}\ p^{p-2} \quad \text{se} \quad p>2$$

Seja agora $x_1,\dots,x_p$ uma base fundamental de L sobre K. Nesse caso $w_0^i = \sum_j u_{ij}\ x_j$ com u_{ij} inteiros em K.

Se $U = (u_{ij})$ temos que

$$\Delta(1,w_0,\dots,w_0^{p-1}) = (\det U)^2\ \Delta(x_1 \dots x_{p-1}) \qquad \text{(ver seção I.1)}$$

Os únicos primos de K que dividem $\Delta(1,w_0,\dots,w_0^{p-1})$ são aqueles que dividem p, então os únicos primos de K que dividem $\Delta(x_1,\dots,x_{p-1})$ são aqueles que dividem p.

Pelo teorema de Dedekind (ver pg. 161 [15]) os únicos primos de K que eventualmente se ramificam em L são aqueles que dividem p.

No caso $p=2$, se consideramos em L a base $(1,\sqrt{\alpha})$ observamos que:

$$\Delta(1,\sqrt{\alpha}) = 4\alpha$$

Temos então o mesmo resultado.

SEÇÃO III.3 ANÁLISE P-ÁDICO

Seja k um corpo com uma valorização discreta ν com respeito à qual é completo. (Ver [3] pg.253)

PROPRIEDADE III.3.1 A série $\sum\limits_{n=0} a_n$ $a_n \in k$ converge se e somente se $\nu(a_n) \longrightarrow 0$.

PROPRIEDADE III.3.2 Seja a série $\sum\limits_{i,j=1} a_{ij}$, e as séries $\sum\limits_{i=1}^{\infty} (\sum\limits_{j=1}^{\infty} a_{ij})$ e $\sum\limits_{j=1}^{\infty} (\sum\limits_{i=1}^{\infty} a_{ij})$. Se para todo $N > 0$ existe só um número finito de pares (i,j) tais que $\nu(a_{ij}) \geq N$, então a série dupla converge e as séries iteradas também e

$$\sum_{i,j=1}^{\infty} a_{ij} = \sum_{i=1}^{\infty} (\sum_{j=1}^{\infty} a_{ij}) = \sum_{j=1}^{\infty} (\sum_{i=1}^{\infty} a_{ij})$$

PROPRIEDADE III.3.3 O conjunto dos $x \in k$ para os quais a série $\sum\limits_{n} a_n x^n$ converge é da forma $\{x \mid \nu(x) \geq \mu\}$ para algum $\mu \in Z$.

PROPRIEDADE III.3.4 Sejam $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$ $g(y) = \sum\limits_{n=1}^{\infty} b_n y^n$. Se a f converge para $\{x \mid \nu(x) \geq \mu\}$ e a g para $y_0 \in k$ tal que $\nu(b_m y_0^m) \geq \mu$ $\forall$ $m \geq 1$ então a série $F(y)$ obtida substituindo formalmente a g na f converge para $y_0 \in k$, e ainda mais $F(y_0) = f(g(y_0))$.

Seja agora a seguinte situação: K um corpo de números algébricos e $p \in Q$ um primo. P um primo de K que está sobre p.

Seja ν_P a valorização P-ádica de K. Seja $e = \nu_P(p)$ = índice de ramificação de P. Seja D_P o anel da valorização ν_P. E seja π um elemento primo do anel D_P. Seja K_P o completamen to de K com respeito a valorização ν_p. Seja Q_p o corpo dos números p-ádicos.

Sejam em K_p as séries

$$\exp x = 1 + x + \ldots + \frac{x^n}{n!} + \ldots$$

$$\lg(1+x) = x - x^2/2 + x^3/3 + \ldots + (-1)^{n-1}\, x^n/n$$

É claro que $\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots$, onde $[\alpha]$ indica a parte inteira de α. Então $\nu_p(n!) = e(\left[\frac{n}{p}\right] + \ldots) < en \sum\limits_{k=1} \frac{1}{p^k} = \frac{en}{p-1}$. Então temos que

$$\nu_p(\frac{x^n}{n!}) > n(\nu_p(x) - \frac{e}{p-1}).$$

Então se $\nu_p(x) > \frac{e}{p-1}$ a série exp x converge.

Reciprocamente se $\nu_p(x) \leq \frac{e}{p-1}$

$$\nu_p(\frac{x^n}{n!}) = n\ \nu_p(x) - \nu_p(n!)$$

Fazendo $n = p^s$

$$\nu_p(n!) = e(p^{s-1} + p^{s-2} + \ldots + 1) = e\ \frac{p^s-1}{p-1} = \frac{e(n-1)}{p-1}$$

$$\nu_p(\frac{x^n}{n!}) = n\ \nu_p(x) - \frac{e(n-1)}{p-1} = n(\nu_p(x) - \frac{e}{p-1}) + \frac{e}{p-1} \leq \frac{e}{p-1}$$

Então a série exp x não converge.

Em consequência o conjunto de convergência da série exp está dado por $\{x\colon \nu_p(x) \geq \kappa\}$ onde $\kappa = \left[\frac{e}{p-1}\right] + 1$.

Vamos estudar o conjunto de convergência da série $\log(1+x)$. Se $\nu_p(x) \leq 0$ $\quad \nu_p(\frac{x^n}{n}) = n\ \nu_p(x) - \nu_p(n) \leq 0$; logo a série $\lg(1+x)$ não converge.

Se $\nu_p(x) \geq 1$ e $n = p^a n_1$ com $(n_1, p) = 1$ temos que

$$\lg n = a \lg p + \lg n_1 \geq a \lg p \quad (*)$$

Então

$$\nu_p\left(\frac{x^n}{n}\right) = n\,\nu_p(x) - \nu_p(n) = n\,\nu_p(x) - ea \geq n\,\nu_p(x) - e\,\frac{\lg n}{\lg p} \geq$$

$$\geq n - e\,\frac{\lg n}{\lg p} = n\left(1 - \frac{e}{n}\,\frac{\lg n}{\lg p}\right).$$

Como $\frac{\lg n}{n} \longrightarrow 0$ $n \longrightarrow \infty$ temos que $\nu_p\left(\frac{x^n}{n}\right) \longrightarrow \infty$ se $n \longrightarrow \infty$. Então $\lg(1+x)$ converge se e somente se $\nu_p(x) \geq 1$.

Shja $A = \{\varepsilon \in K_p :\ \varepsilon \equiv 1 \pmod{\pi}\}$ então o conjunto de convergência da série $\lg z$ é exatamente A.

Temos então que $\lg : A \longrightarrow K_p$.

Analogamente se $B = \{x \in K_p :\ \nu_p(x) \geq k\}$ temos que

$$\exp : B \longrightarrow K_p.$$

Queremos estudar a validez num corpo completo das propriedades usuais da série lg e exp.

É fácil provar que se $\varepsilon_1, \varepsilon_2 \in A$ então $\lg(\varepsilon_1\varepsilon_2) = \lg \varepsilon_1 + \lg \varepsilon_2$; isso é consequência das propriedades formais da série lg.

Em geral não podemos garantir que $\lg \varepsilon$ seja um elemento de $\mathcal{O}_p$. $\mathcal{O}_p$ são os inteiros de K_p.

Vamos achar um subconjunto de A para o qual as imagens do lg estão dentro de B, e ainda mais $\exp \lg \varepsilon = \varepsilon$.

TEOREMA III.3.1 A aplicação $x \longrightarrow \exp x$ é um isomorfismo do grupo aditivo B no grupo multiplicativo

$$A_\kappa = \{\varepsilon \in A: \ \varepsilon \equiv 1 \pmod{\pi^\kappa}\}.$$

O isomorfismo inverso está dado por $\varepsilon \longrightarrow \lg \varepsilon$. $\kappa = \left[\frac{e}{p-1}\right] + 1.$

DEMONSTRAÇÃO

Seja $x \in B$, queremos provar que $\exp x \in A_\kappa$, ou seja que

$$\nu_p(\exp x - 1) \geq \kappa$$

Ou seja, basta provar que $\nu_p(\frac{x^n}{n!}) \geq \kappa \quad \forall\ n \geq 1$ com $\nu_p(x) \geq \kappa$.

Seja s tal que $p^s \leq n < p^{s+1}$

$$\nu_p(\frac{x^n}{n!}) - \kappa = n\ \nu_p(x) - \nu_p(n!) - \kappa \geq$$

$$\geq (n-1)\kappa - e(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^s}\right])$$

Mas

$$\left[\frac{n}{p}\right] + \ldots + \left[\frac{n}{p^s}\right] \leq \frac{n}{p} + \frac{n}{p^2} + \ldots + \frac{n}{p^s} = \frac{n}{p}(1 + \frac{1}{p} + \ldots + \frac{1}{p^{s-1}})$$

Então

$$\left[\frac{n}{p}\right] + \ldots + \left[\frac{n}{p^s}\right] \leq \frac{n}{p}(\frac{\frac{1}{p^s} - 1}{\frac{1}{p} - 1}) = \frac{n}{p}\ \frac{p^s-1}{p-1}\ \frac{p}{p^s} = \frac{n}{p^s}\ \frac{p^s-1}{p-1}$$

Como $\kappa \geq \frac{e}{p-1}$ temos que (se $n \geq 1$)

$$\nu_p(\frac{x^n}{n!}) - \kappa \geq \frac{(n-1)e}{p-1} - \frac{en}{p^s}\ \frac{p^s-1}{p-1} = \frac{e}{p-1}\ (\frac{n}{p^s} - 1) \geq 0$$

Temos provado então que $x \longrightarrow \exp x: B \longrightarrow A_\kappa$.

Utilizando a Propriedade III.3.4 temos que $\lg \exp x = x$ $\forall\ x \in A_\kappa$ (isso é consequência de que a série obtida substituindo $\exp x$ em $\lg \varepsilon$ formalmente, dá a identidade).

Também temos que $\exp(x+y) = \exp x \circ \exp y$.

Queremos provar agora que $\varepsilon \longrightarrow \lg \varepsilon : A_\kappa \longrightarrow B$, ou seja que se x é tal que $\nu_p(x) \geq \kappa$ $\quad \nu_p(\frac{x^n}{n}) \geq \kappa$. $\forall\ n \geq 1$.

Se $n = 1$ a propriedade se verifica trivialmente.

Em geral consideremos duas possibilidades

(a) $1 \leq n \leq p-1$

$$\nu_p(\frac{x^n}{n}) = n\ \nu_p(x) - \nu_p(n) = n\ \nu_p(x) \geq \nu_p(x) \geq \kappa$$

(b) $n \geq p \geq 2$

A igualdade (*) assegura que:

$$\nu_p(n) \leq e\ \frac{\lg n}{\lg p}$$

Então:

$$\nu_p(\frac{x^n}{n}) - \kappa \geq (n-1)\kappa - e\ \frac{\lg n}{\lg p} = (n-1)(\left[\frac{e}{p-1}\right] + 1) - e\ \frac{\lg n}{\lg p}$$

Então:

$$\nu_p(\frac{x^n}{n}) - \kappa > (n-1)\ \frac{e}{p-1} - e\ \frac{\lg n}{\lg p} = \frac{e(n-1)}{\lg p}\ \left[\frac{\lg p}{p-1} - \frac{\lg n}{n-1}\right] \geq 0$$

pois a função $\frac{\lg t}{t-1}$ é decrescente se $t \geq 2$.

Também se verifica que $\forall\ \varepsilon \in A_\kappa$ $\quad \exp \lg \varepsilon = \varepsilon$. c.q.d.

Procuraremos agora os zeros do lg. (ver [6] pg.258)

TEOREMA III.3.2

Seja a aplicação $\lg: A \longrightarrow K_p$, então $\lg \varepsilon = 0$ implica que existe p^s com $s \geq 0$ que verifica $\varepsilon^{p^s} = 1$.

DEMONSTRAÇÃO

Se $\nu_p(\varepsilon-1) \geq \kappa$. Como $1 \in A_\kappa$, $\lg 1 = 0$ (por definição), e a função lg é injetora em A_κ, resulta que $\varepsilon = 1$.

Provaremos que se $\nu_p(\varepsilon-1) \geq 1$ existe s tal que $\nu_p(\varepsilon^{p^s}-1) \geq \kappa$, então como de $\lg \varepsilon = 0$ se deduz $\lg \varepsilon^{p^s} = 1$, pela observação anterior temos que $\varepsilon^{p^s} = 1$.

Seja $x_s = \varepsilon^{p^s} - 1$, então

$$x_{s+1} = \varepsilon^{p^{s+1}} - 1 = (x_s+1)^p - 1 = \binom{p}{1}x_s + \binom{p}{2}x_s^2 + \ldots + \binom{p}{p}x_s^p$$

(onde $\binom{p}{j}$ indica o número combinatório)

$$\nu_P\left(\binom{p}{j}\right) = \nu_P(p!) - \nu_P((p-j)!) - \nu_P(j!) =$$

$$= e(\nu_p(p!) - \nu_p((p-j)!) - \nu_p(j!))$$

Então

$$\nu_P\left(\binom{p}{j}\right) = \begin{cases} e & 0 < j \neq p \\ 0 & j = p \end{cases}$$

Em consequência

$\nu_P(x_{s+1}) \geq \min\{e+\nu_P(x_s), e+2\nu_P(x_s), \ldots, e+(p-1)\nu_P(x_s), p\nu_P(x_s)\}$

Então $\nu_P(x_{s+1}) > \nu_P(x_s)$. Então existe s tal que $\nu_P(x_s) \geq \kappa$.

c.q.d.

SEÇÃO III.4 A APLICAÇÃO λ

Seja $\begin{smallmatrix} K \\ | \\ Q \end{smallmatrix}$ uma extensão algébrica normal finita, seja p um elemento primo de Q e seja $G = \mathrm{Gal}(K,Q)$. Seja P um elemento primo de K que está sobre Q. Temos a seguinte situação

$$\begin{array}{ccc} \mathcal{O} \subset K & \xrightarrow[\tau_P]{} & K_P \supset \mathcal{O}_P \\ | & & | \\ Z \subset Q & \longrightarrow & Q_p \supset Z_p \end{array}$$

onde $\mathcal{O}$ são os inteiros de K, K_P e Q_p os completamentos de K e Q um respeito às valorizações P e p-ádicas respectivamente. Z_p os inteiros p-ádicos e $\mathcal{O}_P$ os inteiros P-ádicos, τ_P a inclusão canônica.

Uma generalização natural dos resultados do Cap.II nos levaria a procurar um Z_p G-morfismo entre os Z_p G-módulos $E \otimes_Z Z_p$ e $\underset{P/p}{\oplus} \mathcal{O}_P$.

A estrutura de Z_p G-módulo de $E \otimes_Z Z_p$ é a natural.

A estrutura de Z_p G-módulo de $\underset{P/p}{\oplus} \mathcal{O}_P$ é a seguinte: se $(a_P)_{P/p} \in \underset{P/p}{\oplus} \mathcal{O}_P$ e $\sigma \in G$ $\sigma\circ(a_P)_{P/p} = (\tilde{\sigma}(a_{\sigma^{-1}(P)}))_{P/p}$, onde $\tilde{\sigma}: \mathcal{O}_{\sigma^{-1}(P)} \longrightarrow \mathcal{O}_P$ é o único Z_p-morfismo que faz o diagrama abaixo comutativo

$$\begin{array}{ccc} \sigma : \mathcal{O} & \longrightarrow & \mathcal{O} \\ {\scriptstyle \tau_{\sigma^{-1}(P)}} \downarrow & & \downarrow {\scriptstyle \tau_P} \\ \mathcal{O}_{\sigma^{-1}(P)} & \xrightarrow{\tilde{\sigma}} & \mathcal{O}_P \end{array}$$

No futuro usaremos a mesma notação para σ e $\tilde{\sigma}$.

No capítulo II construimos um QG-morfismo de $E \otimes_Z Q$ usando o lg. Agora faremos uma coisa parecida para construir um morfismo de $E \otimes_Z Z_p$ usando lg P-ádico. Para isso precisamos resolver alguns problemas técnicos que tem origem no fato de não ser possível definir o logarítmo P-ádico em qualquer elemento de U.

Seja como antes U o grupo dos inversíveis de $\mathcal{O}$, e C o subgrupo das raízes da unidade de K.

Seja $E_p = U^{(N-1)p^t}$ onde N indica a norma absoluta de um ideal primo P, que está sobre p, e t é o menor inteiro que verifica $p^t > e \geq 1$, sendo e = índice de ramificação de P.

LEMA III.4.1

$E_p \cong U/C = E$ como ZG-módulos.

DEMONSTRAÇÃO

Seja α: $U \longrightarrow E_p \subset U$ definida assim

$$\alpha(x) = x^{(N-1)p^t}$$

É claro que α é um homomorfismo sobrejetor de U em E_p considerados como módulos sobre ZG.

É claro também que o $\operatorname{Ker} \alpha \subset C$.

Seja $z \in C$ queremos provar que $z^{(N-1)p^t} = 1$. Seja $w = \#(C)$ (cardinalidade do C). Então $w = w_0\, p^a$ onde $p \nmid w_0$. Queremos provar que $w/(N-1)p^t$ ou seja $w_0/(N-1)$ e $a \leq t$.

Seja $Q(\xi) \subset K$ onde ξ é uma raiz primitiva de ordem p^a de 1. $\dim_Q Q(\xi) = p^{a-1}(p-1)$. Como p se ramifica totalmente em $Q(\xi)$ (ver III.1) $e_{Q(\xi),Q} = p^{a-1}(p-1)/e_{K,Q} = e$. Ou seja que $p^{a-1}(p-1)/e < p^t$ ou seja $p^{a-1}(p-1) < p^t$, então $a \leq t$.

Seja agora $\Gamma = \{\gamma \mid \gamma^n = 1$ com $(n,p) = 1\} \subset \mathbb{C}$. Então $\#(\Gamma) = w_0$.

Seja ϕ: $\Gamma \longrightarrow (\mathcal{O}/P)^*$ definida assim:

$$\phi(\gamma) = \gamma + P.$$

ϕ é um morfismo injetor. Se $\gamma + P = 1 + P$ com $\gamma \neq 1$, acontece que $\gamma^{n-1} + \gamma^{n-2} + \ldots + 1 = 0$. Como $\gamma^k \equiv 1 \pmod P$ resulta que $n \equiv 0 \pmod P$, ou seja P/n. Mas por hipótese o máximo divisor comum entre n e p, é 1. Então resulta que ϕ é injetora.

Daí temos que $\#(\Gamma)/\#(\mathcal{O}/P)^* = N-1$. (ver seção I.1)

<u>c.q.d.</u>

Agora temos que $E_p \subset U \subset \mathcal{O}$, e podemos trabalhar em E_p

com o logarítmo P-ádico que é injetor.

LEMA III.4.2

$lg_p \circ \tau_p : E_p \longrightarrow \mathcal{O}_p$ é uma função injetora.

DEMONSTRAÇÃO

Após o Teorema III.3.1 basta provar que $\nu_p(w-1) \geq \left[\frac{e}{p-1}\right] + 1 = \kappa$, para todo $w \in E_p$. Seja $w = u^{(N-1)p^t}$ com $u \in U$, e seja $x = u^{(N-1)}$.

Do fato de $(\mathcal{O}/P)^*$ ter N-1 elementos, deduz-se que $u^{N-1} \equiv 1 \pmod{P}$. Existe então α tal que $\nu_p(\alpha) \geq 0$ e $x = 1 + \alpha\pi$ (onde π é um elemento de K tal que $\nu_p(\pi) = 1$).

Então temos que $w-1 = x^{p^t} - 1 = (1+\alpha\pi)^{p^t} - 1$

$$\nu_p(w-1) = \nu_p((1+\alpha\pi)^{p^t} - 1) = \nu_p\left(\sum_{i=1}^{p^t} \binom{p^t}{i}(\alpha\pi)^i\right)$$

Provaremos que para todo $i \geq 1$ acontece que

$$\nu_p\left(\binom{p^t}{i}(\alpha\pi)^i\right) > \frac{e}{p-1}$$

Se $i = p^t$ $\quad \nu_p((\alpha\pi)^{p^t}) \geq p^t > e \geq \frac{e}{p-1}$.

Se $i < p^t$ $\quad \nu_p\left(\binom{p^t}{i}(\alpha\pi)^i\right) = \nu_p\left(\binom{p^t}{i}\right) + i\nu_p(\alpha\pi) \geq \nu_p\left(\binom{p^t}{i}\right) + 1$

agora se $i \neq p^t$ $\quad p/\binom{p^t}{i}$ então:

$$\nu_p\left(\binom{p^t}{i}\right) \geq \nu_p(p) = e$$

Em consequência se $i < p^t$

$$\nu_p\left(\binom{p^t}{i}(\alpha\pi)^i\right) \geq e + 1 > \frac{e}{p-1}$$

c.q.d.

Podemos agora então definir um Z_p G-homomorfismo

$$\lambda_{K,p}: E_p \otimes_Z Z_p \longrightarrow \bigoplus_{P/p} \mathcal{O}_P \qquad (1)$$

da seguinte forma: sejam $w \in E_p$ e $\alpha \in Z_p$

$$\lambda_{K,p}(w \otimes \alpha) = (\alpha\, lg_P\, \tau_P\, w)_{P/p}$$

onde τ_P indica a inclusão canônica $K \xhookrightarrow{\tau_P} K_P$ e lg_P o logaritmo em K_P. É óbvio que $\lambda_{K,p}$ é um Z_p-morfismo. Precisamos provar que comuta com a multiplicação por um elemento de G, ou seja

$$\lambda_{K,p}(\sigma(w \otimes \alpha)) = \sigma\, \lambda_{K,p}(w \otimes \alpha).$$

Por um lado

$$\lambda_{K,p}(\sigma(w \otimes \alpha)) = \lambda_{K,p}(\sigma(w) \otimes \alpha) = (\alpha\, lg_P\, \tau_P\, \sigma w)_{P/p}.$$

Por outro lado

$$\alpha \cdot \lambda_{K,p}(w \otimes \alpha) = \sigma \circ (\alpha\, lg_P\, \tau_P\, w)_{P/p} =$$

$$= (\sigma(\alpha\, lg_{\sigma^{-1}(P)}\, \tau_{\sigma^{-1}(P)}\, w))_{P/p} = (\alpha\, \sigma(lg_{\sigma^{-1}(P)}\, \tau_{\sigma^{-1}P}\, w))_{P/p}$$

Como temos que o diagrama seguinte comuta

$$\begin{tikzcd}
\mathcal{O}_{\sigma^{-1}(P)} \arrow[d, "\sigma"] & E_p \arrow[l, "lg_{\sigma^{-1}P} \circ \tau_{\sigma^{-1}P}"'] \arrow[d, "\sigma"] \\
\mathcal{O}_P & E_p \arrow[l, "lg_P \circ \tau_P"']
\end{tikzcd}$$

temos que $\sigma(lg_{\sigma^{-1}(P)}\, \tau_{\sigma^{-1}P}\, w) = lg_P\, \tau_P\, \sigma w$.

Em consequência: $\lambda_{K,p}(\sigma(w \otimes \alpha)) = \sigma\, \lambda_{K,p}(w \otimes \alpha)$.

Seja agora $r_{K,p} = \text{posto}_{Z_p}(\lambda(E_p \otimes_Z Z_p))$.

Sabemos que $\text{posto}_{Z_p}(E_p \otimes_Z Z_p) = \text{posto}_Z E_p = \text{posto}_Z E = r$

r = número de dirichlet de K sobre Q.

É claro então que $r \geq r_{K,p}$.

Estudar a injetividade de $\lambda_{K,p}$ é equivalente a estudar em que casos acontece a igualdade $r_{K,p} = r$. Veremos a relação de $r_{K,p}$ com o posto do regulador p-ádico.

No futuro indicaremos $\lambda_{K,p} = \lambda_p$ e $r_{K,p} = r_p$.

SEÇÃO III.5 O REGULADOR P-ÁDICO

Na mesma situação que na seção III.4 consideremos um primo fixo P_0, que está sobre p.

Seja $u_1,\ldots,u_r$ uma Z-base de E_p.

DEFINIÇÃO III.5.1 Chama-se matriz regulador p-ádico de K a uma matriz $R_p \in M_{n,r}(\mathcal{O}_{P_0})$ definida assim:

$$R_p = \begin{pmatrix} lg_{P_0} \tau_{P_0} \sigma_1 u_1 , & lg_{P_0} \tau_{P_0} \sigma_1 u_2 , & \ldots , & lg_{P_0} \tau_{P_0} \sigma_1 u_r \\ lg_{P_0} \tau_{P_0} \sigma_2 u_1 , & lg_{P_0} \tau_{P_0} \sigma_2 u_2 , & \ldots , & lg_{P_0} \tau_{P_0} \sigma_2 u_r \\ lg_{P_0} \tau_{P_0} \sigma_n u_1 , & lg_{P_0} \tau_{P_0} \sigma_n u_2 , & \ldots , & lg_{P_0} \tau_{P_0} \sigma_n u_r \end{pmatrix}$$

onde $\{\sigma_1 \ldots \sigma_n\} = Gal(K,Q)$.

DEFINIÇÃO III.5.2

$$\tilde{r}_p = \text{posto}_{K_{P_0}} R_p$$

Provaremos que $\tilde{r}_p$ é exatamente igual a r_p. Ou seja que a injetividade da transformação λ_p, fica controlada pela matriz regulador p-ádico. No Capítulo II provamos que a aplicação $\phi: E \otimes_Z Q \longrightarrow QG$ é injetora dado que o posto do regulador coincide com o posto de E. Na situação atual o problema da injetividade de λ_p é um problema em aberto, em particular a pergunta de se $r_p = r$ para toda K extensão abeliana de Q e para todo p primo, foi formulada por Leopoldt em [9].

TEOREMA III.5.1

$$\tilde{r}_p = r_p$$

DEMONSTRAÇÃO

Vamos supor que as colunas

$$x_i = \begin{pmatrix} \lg_{p_o} \tau_{p_o} \sigma_1 u_i \\ \vdots \\ \lg_{p_o} \tau_{p_o} \sigma_n u_i \end{pmatrix} \qquad \text{com} \quad 1 \leq i \leq \tilde{r}_p$$

são base (sobre K_{p_o}) das colunas de R_p.

Vamos provar nesse caso que os elementos $\lambda_p(u_1 \otimes 1),\ldots$ $\ldots,\lambda_p(u_{\tilde{r}_p} \otimes 1)$ são linearmente independentes sobre Z_p.

Se existem $\alpha_1,\ldots,\alpha_{\tilde{r}_p} \in Z_p$ tais que

$$\sum_{i=1}^{\tilde{r}_p} \alpha_i \lambda_p(u_i \otimes 1) = 0.$$

Temos que, multiplicando por $\sigma \in G$

$$\sigma \circ \sum_{i=1}^{\tilde{r}_p} \alpha_i \lambda_p(u_1 \otimes 1) = 0 = \sum_{i=1}^{\tilde{r}_p} \alpha_i \lambda_p(\sigma(u_i) \otimes 1)$$

Então para todo $\sigma \in G$ vale

$$0 = \sum_{i=1}^{\tilde{r}_p} \alpha_i \lg_{p_o} \tau_{p_o} \sigma u_i$$

Ou seja que as colunas da matriz regulador, verificam:

$$\sum_{i=1}^{\tilde{r}_p} \alpha_i x_i = 0$$

e isso é absurdo, a menos que $\alpha_i = 0 \quad i = 1 \dots \tilde{r}_p$.

Daí que $\{\lambda_p(u_i \otimes 1)\}_{1 \leq i \leq \tilde{r}_p}$ são linearmente independentes sobre Z_p. Seja agora $i > \tilde{r}_p$, como os $x_i \quad i = 1, \dots, \tilde{r}_p$, são base das colunas de R_p, existem $\beta_j \in K_{P_0}$, com $1 \leq j \leq \tilde{r}_p$, de modo que para todo $\sigma \in G$ se verifica

$$1g_{P_0} \; \tau_{P_0} \; \sigma \; u_i = \sum_{j=1}^{\tilde{r}_p} \beta_j \; 1g_{P_0} \; \tau_{P_0} \; \sigma \; u_j \qquad (2)$$

Seja agora $G_{P_0} = \{\rho \in G: \rho(P_0) = P_0\}$.

Seja $\rho \in G_{P_0}$, pelas observações da seção III.4 resulta que

$$\rho \; 1g_{P_0} \; \tau_{P_0} \; \sigma \; u_i = 1g_{\rho(P_0)} \; \tau_{\rho(P_0)} \; \rho \; \sigma \; u_i = 1g_{P_0} \; \tau_{P_0} \; \rho \; \sigma \; u_i$$

Então:

$$\rho \; 1g_{P_0} \; \tau_{P_0} \; \sigma \; u_i = 1g_{P_0} \; \tau_{P_0} \; \rho \; \sigma \; u_i = \sum_{j=1}^{\tilde{r}_p} \beta_j \; 1g_{P_0} \; \tau_{P_0} \; \rho \; \sigma \; u_j$$

Aplicando agora ρ na igualdade (2) temos que

$$\rho(1g_{P_0} \; \tau_{P_0} \; \sigma \; u_i) = \rho\Big(\sum_{j=1}^{\tilde{r}_p} \beta_j \; 1g_{P_0} \; \tau_{P_0} \; \sigma \; u_j\Big) =$$

$$= \sum_{j=1}^{\tilde{r}_p} \rho(\beta_j) \; 1g_{P_0} \; \tau_{P_0} \; \rho \; \sigma \; u_j$$

Comparando as duas últimas expressões e observando que fixando ρ e variando σ obtemos todos os elementos de G, temos que

$$\sum_{j=1}^{\tilde{r}_p} \rho(\beta_j) \; x_j = \sum_{j=1}^{\tilde{r}_p} \beta_j \; x_j .$$

Resulta então que $\forall \; \rho \in G_{P_0} \quad \rho(\beta_j) = \beta_j$.

Usando a teoria de Hilbert (ver [15] pg.175, Proposição 4-10-5) deduzimos que $\beta_j \in Q_p$.

Temos então a igualdade (2) com $\beta_j \in Q_p$.

Seja agora $\theta \in G$ arbitrário e apliquemos θ na igualdade (2).

$$\theta(lg_{P_0}\ \tau_{P_0}\ \sigma\ u_i) = lg_{\theta(P_0)}\ \tau_{\theta(P_0)}\ \theta\ \sigma\ u_i =$$

$$= \theta\Big(\sum_{j=1}^{\tilde{r}_p} \beta_j\ lg_{P_0}\ \tau_{P_0}\ \sigma\ u_j\Big) = \sum_{j=1}^{\tilde{r}_p} \beta_j\ lg_{\theta(P_0)}\ \tau_{\theta(P_0)}\ \theta\ \sigma\ u_j$$

Seja agora P/p arbitrário e seja θ tal que $\theta(P_0) = P$. A igualdade anterior vale para todo σ em particular para $\sigma = \theta^{-1}$, teremos então que:

$$lg_P\ \tau_P\ u_i = \sum_{j=1}^{\tilde{r}_p} \beta_j\ lg_P\ \tau_P\ u_j \qquad i > \tilde{r}_p \qquad \beta_j \in Q_p$$

Em consequência os vetores $\lambda_p(u_1 \otimes 1), \ldots, \lambda_p(u_{\tilde{r}_p} \otimes 1), \lambda_p(u_i \otimes 1)$ são linearmente dependentes sobre Q_p, então

$$\text{pôsto}_{Z_p}(\lambda_p(E_p \otimes_Z Z_p)) = \tilde{r}_p.$$

<u>c.q.d.</u>

SEÇÃO III.6 ALGUNS RESULTADOS PARCIAIS

TEOREMA III.6.1 Se $r \geq 2 \implies r_p \geq 2$

DEMONSTRAÇÃO

Se $r_p < 2$, considerando a linha da matriz R_p que corresponde ao elemento $Id \in Gal(K,Q)$, teríamos $\forall\ \sigma \in G$ e $\forall\ i$, $1 \leq i \leq r$ que existem números $\beta(\sigma) \in K_{P_0}$ tais que

$$lg_{P_0}\ \tau_{P_0}\ \sigma\ u_i = \beta(\sigma)\ lg_{P_0}\ \tau_{P_0}\ u_i$$

Aplicando a propriedade multiplicativa da função logarítmo (teorema III.3.1) concluimos que para todo $\sigma \in G$ e $\forall\, u \in E_p$ vale

$$lg_{P_0}\ \tau_{P_0}\ \sigma\, u = \beta(\sigma)\ lg_{P_0}\ \tau_{P_0}\ u$$

Seja m = ordem σ e $\sigma \neq Id$

$$lg_{P_0}\ \tau_{P_0}\ \sigma^2\, u = \beta(\sigma)\ lg_{P_0}\ \tau_{P_0}\ \sigma\, u = [\beta(\sigma)]^2\ lg_{P_0}\ \tau_{P_0}\ u$$

$$lg_{P_0}\ \tau_{P_0}\ u = lg_{P_0}\ \tau_{P_0}\ \sigma^m\, u = [\beta(\sigma)]^m\ lg_{P_0}\ \tau_{P_0}\ u$$

Definitivamente $[\beta(\sigma)]^m = 1$. Ou seja que $\beta(\sigma)$ é algébrico sobre Q. Então usando o teorema de Mahler [10], que generaliza o 7º problema de Hilbert ao caso p-ádico, deduzimos que $\beta(\sigma)$ deve ser racional. Então $\beta(\sigma) = \pm 1 = \varepsilon$. Em consequência

$$lg_{P_0}\ \tau_{P_0}\ \sigma\, u = lg_{P_0}\ \tau_{P_0}\ u^{\varepsilon}$$

usando o lema III.4.2 deduzimos que:

$$\sigma\, u = u^{\varepsilon}, \quad \text{para todo} \quad u \in E_p.$$

Então os ZG-submódulos cíclicos de E_p, tem posto 1 sobre Z, mas isso claramente está em contradição com o Teorema II.4.1 exceto no caso $r = 1$. c.q.d.

Na demonstração do teorema anterior foi essencial o fato de que $\beta(\sigma)$ fosse multiplicativa em relação à variável $\sigma \in G$. Nossa intenção é generalizar esse raciocínio, para isso precisamos, dada uma combinação linear $\sum_{\sigma \in G} a(\sigma)\ lg_{P_0}\ \tau_{P_0}\ \sigma\, u_i = 0$ que os $a(\sigma)$ se comportem razoavelmente com respeito a multiplicação em G. Para isso precisaremos um resultado sobre os idempotentes centrais, queremos expressá-los em função dos caracteres do grupo. (ver teorema (33.8) pg.236 [4])

LEMA III.6.1

Seja P_0 um primo fixo de K que está sobre p e seja Ω um fecho algébrico de K_{P_0}. Vamos supor que $G = Gal(K,Q)$ é um grupo abeliano. Suponhamos também que a extensão K/Q é real. Então se $r_p < r = n-1$ existe um carácter $x \in \hat{G}$ tal que

$$\sum_{\sigma \in G} x(\sigma)\ lg_{P_0}\ \tau_{P_0}\ \sigma\ u_i = 0$$

e x não é o carácter identicamente igual a 1.

$$(\hat{G} = \{x:\ G \longrightarrow \Omega:\ x(g_1 g_2) = x(g_1)\ x(g_2)\})$$

DEMONSTRAÇÃO

Seja a matriz R_p^t matriz transposta do regulador p-ádico. Podemos pensar R_p^t como uma transformação linear

$$R_p^t:\ \Omega^n \longrightarrow \Omega^r = \Omega^{n-1}$$

Seja $N = \{(\alpha_\sigma)_{\sigma \in G} \mid \alpha_\sigma \in \Omega \ \sum_{\sigma \in G} \alpha_\sigma\ lg_{P_0}\ \tau_{P_0}\ \alpha\ u = 0 \quad \forall\ u \in E_p\}$.

É claro que $\dim_\Omega N + \dim_\Omega(R_p^t(\Omega^n)) = n$.

Mas $\dim_\Omega R_p^t(\Omega^n) = r_p \leq n-2$ então temos que $\dim_\Omega N \geq 2$.

Seja agora no anel de ΩG o seguinte ideal:

$$V(G) = \{\sum_{\sigma \in G} \alpha_\sigma\ \sigma \mid \sum_{\sigma \in G} \alpha_\sigma\ lg_{P_0}\ \tau_{P_0}\ \sigma\ u = 0 \quad \forall\ u \in E_p\}$$

Verificaremos que V(G) é um ideal

Se $\theta \in G$ e $\sum_{\sigma \in G} \alpha_\sigma\ \sigma \in V(H)$

$$\theta \circ \sum_{\sigma \in G} \alpha_\sigma\ \sigma = \sum_{\sigma \in G} \alpha_\sigma\ \theta\ \sigma = \sum_{\sigma \in G} \alpha_{\theta^{-1}\sigma}\ \sigma$$

Precisamos verificar então que

$$\sum_{\sigma \in G} \alpha_{\theta^{-1}\sigma} \, 1g_{p_o} \, \tau_{p_o} \, \sigma \, u = 0 \quad \forall \, u \in E_p$$

Mas se consideramos $u = \theta^{-1} v$ com $v \in E_p$ temos que

$$\sum_{\sigma \in G} \alpha_{\theta^{-1}\sigma} \, 1g_{p_o} \, \tau_{p_o} \, \sigma \, \theta^{-1} \, v = \sum_{\sigma \in G} \alpha_{\theta^{-1}\sigma} \, 1g_{p_o} \, \tau_{p_o} \, \theta^{-1} \, \sigma \, v =$$

$$= \sum_{\rho \in G} \alpha_\rho \, 1g_{p_o} \, \tau_{p_o} \, \rho \, v = 0$$

e essa igualdade vale para todo $v \in E_p$.

Como ΩG é semi-simples e abeliano $V(G) = \Omega \, G \, e_1 \oplus \ldots\ldots \oplus \Omega \, G \, e_t$ onde os e_i são idempotentes ortogonais primitivos. Pelo teorema 33.8 da pg.236 de [4] temos que

$$e_j = \frac{1}{|G|} \sum_{\sigma \in G} x^j(\sigma) \, \sigma .$$

Como $e_j \in V(G)$ os caracteres x^j associados a e_j verificam

$$\sum_{\sigma \in G} x^j(\sigma) \, 1g_{p_o} \, \tau_{p_o} \, \sigma \, u_i = 0$$

Se o único carácter que verifica a igualdade anterior é o carácter identicamente igual a 1, teremos que:

$$V(G) = \Omega \, G \, e_1 \quad \text{onde} \quad e_1 = \frac{1}{|G|} \sum_{\sigma \in G} \sigma .$$

Mas $\Omega \, G \, e_1 = \Omega \, e_1$, pois $\tau \, e_1 = e_1 \quad \forall \, \tau \in G$.

Em consequência se $(a_\sigma)_{\sigma \in G} \in N$ resulta que:

$$\sum_{\sigma \in G} a_\sigma \, \sigma \in V(G).$$

Então $\sum_{\sigma \in G} a_\sigma \, \sigma = \alpha \, e_1 \quad \alpha \in \Omega$, em consequência temos que se $(a_\sigma)_{\sigma \in G} \in N \Longrightarrow a_\sigma = \frac{\alpha}{|G|} \quad \forall \, \sigma$. Daí sai que $\dim_\Omega N = 1$ absurdo.

c.q.d.

Podemos agora demonstrar o seguinte resultado.

TEOREMA III.6.2

Seja K uma extensão de Q abeliana real tal que

$$G = Gal(K,Q)$$

é um grupo de expoente m, com $m \leq 4$ ou $m = 6$. Então $r_p = r = n-1$.

DEMONSTRAÇÃO

Deduzimos (aplicando o lema III.6.1) que existe um carácter $x \in \hat{G}$ não identicamente 1 que verifica

$$\sum_{\sigma \in G} x(\sigma)\ lg_{p_0}\ \tau_{p_0}\ \sigma u = 0 \quad \forall\ u \in E_p.$$

Como os polinômios ciclotômicos ϕ_1, ϕ_2, ϕ_3, ϕ_4, ϕ_6, tem grau menor ou igual a 2 e o grupo G tem expoente ≤ 4 ou 6; resulta que $x(\sigma)^m = 1$ com $m \leq 4$ ou 6, de onde se deduz que $x(\sigma)$ está contido, para todo σ, numa extensão F de Q de grau ≤ 2.

Estudaremos então dois casos diferentes

a) $x(\sigma) \in Q \quad \forall\ \sigma \in G$

Como sempre acontece que $\sum_{\sigma \in G} lq_{p_0}\ \tau_{p_0}\ \sigma u = 0$ (isso é consequência de que $\prod_{\sigma \in G} \sigma u = N_{K/Q}\ u = +1$ pois

$$N_{K/Q}\ u = (N_{K,Q}(\varepsilon))^{(N-1)p^t} = (\pm 1)^{(N-1)p^t} = 1,$$

sendo $u = \varepsilon^{(N-1)p^t}$.) temos que

$$\sum_{\sigma \in G \setminus \{1\}} (x(\sigma)-1)\ lq_{p_0}\ \tau_{p_0}\ \sigma u = 0 \quad \forall\ u \in E_p.$$

Daí deduzimos que existem inteiros $a(\sigma)$ não todos nulos tais que

$$lq_{p_0}\ \tau_{p_0}\ (\prod_{\sigma \in G \setminus \{1\}} (\sigma u)^{a(\sigma)}) = 0$$

Como em E_p o $lg_{p_o} \circ \tau_{p_o}$ é uma função injetora, temos que:

$$(*) \quad \prod_{\sigma \in G \setminus \{1\}} (\sigma u)^{a(\sigma)} = 0 \quad \forall\ u \in E_p.$$

Sabemos (Teorema II.4.1) que existe $u \in E_p$ tal que $\text{posto}_Z ZGu = r = n-1$, mas isso é contraditório com (*) pois sabemos que existe algum $\sigma_0 \in G \setminus \{1\}$ tal que $a(\sigma_0) \neq 0$.

b) Existe δ inteiro sobre Q tal que $\delta \notin Q$

$$x(\sigma)-1 = a(\sigma) + b(\sigma)\delta \quad \text{com} \quad a(\sigma), b(\sigma) \in Z.$$

Como antes deduzimos que

$$lg_{p_o}\ \tau_{p_o} \left(\prod_{\sigma \in G \setminus \{1\}} \sigma(u)^{a(\sigma)} \right) = -\delta\ lg_{p_o}\ \tau_{p_o} \left(\prod_{\sigma \in G \setminus \{1\}} \sigma(u)^{b(\sigma)} \right) \quad (*)$$

igualdade que vale para todo $u \in E_p$.

Se $a(\sigma) = 0 \quad \forall\ \sigma \in G \setminus \{1\}$ teríamos (dado que $\delta \neq 0$) que $lg_{p_o}\ \tau_{p_o} \left(\prod_{\sigma \in G \setminus \{1\}} \sigma(u)^{b(\sigma)} \right) = 0$ e como na parte (a) deduzimos que $b(\sigma) = 0 \quad \forall\ \sigma \in G \setminus \{1\}$ mas isso é absurdo pois o carácter x não é identicamente 1.

Existe então σ_0: $a(\sigma_0) \neq 0$ e também σ_1: $b(\sigma_1) \neq 0$. Mas nesse caso estaríamos em contradição com o teorema de Mahler [10] pois o quociente de dois logarítmos de números algébricos p-ádicos seria algébrico não racional.

<u>c.q.d.</u>

OBSERVAÇÃO 1 O teorema anterior pode ser provado em hipóteses mais gerais, p.ex.; no caso que K seja tal que o subcorpo maximal real de K seja uma extensão abeliana com grupo de Galois de expoente ≤ 4 ou 6.

Isso é consequência de que se K_1 e o corpo maximal real e $K_1 \neq K$. Então $n = \dim_Q K$ é par e $\frac{n}{2} = \dim_Q K_1$. Nesse caso se chamarmos r_K e r_{K_1} os números de Dirichlet de K e K_1 teremos que $r_K = r_{K_1} = \frac{n}{2} - 1$. Como pelo teorema III.6.2 $r_{K_1,p} = r_{K_1}$ e não é difícil de provar que $r_{K_1,p} = r_{K,p}$; teremos que $r_{K,p} = r_K$.

OBSERVAÇÃO 2

O teorema III.6.2 também poderia ser demonstrado (dessa forma foi provado em [1]) usando um resultado de Minkowski [11] sobre inversíveis numa extensão galoisiana dos racionais (ver [1])

OBSERVAÇÃO 3

Vamos considerar uma valorização não trivial dos racionais que indicaremos com $| \ |$. ($| \ |$ pode ser arquimediana ou não arquimediana). Seja Ω um fecho algébrico do completamento de Q com respeito à valorização $| \ |$. Seja A = fecho algébrico de Q em Ω. Sejam $\alpha_i \in A$ $i = 1 \ldots n$ tais que o logarítmo dos α_i esteja definido. (No caso de que a valorização seja arquimediana o logarítmo é o logarítmo usual, e no caso não arquimediano o logarítmo é o logarítmo p-ádico)

CONJECTURA: Se $\lg \alpha_i$ $i = 1 \ldots n$ são linearmente dependentes sobre A então são linearmente dependentes sobre Q.

No caso $n = 2$ e $| \ |$ arquimediana é o 7º problema de Hilbert. No caso $n = 2$ e $| \ |$ não arquimediana é o teorema de Mahler [10]. Nenhum outro caso é conhecido.

Se a conjectura fosse verdadeira para todo n, então $r_{K,p} = r_K$ para toda extensão K abeliana de Q e para todo primo racional $p \in Q$.

Da mesma forma que na observação 1, podemos supor que a extensão K de Q é abeliana real.

Se $r_{K,p} < n-1 = r$ usando o lema III.6.1 mostramos a existência de um carácter x que verifica

$$\sum_{\sigma \in G} x(\sigma)\ \lg_{p_o}\ \tau_{p_o}\ \sigma u = 0 \quad \forall\ u \in E_p\ ,$$

e de modo que x não é identicamente igual a 1.

Vamos supor que $x(\sigma) : \sigma \in G\}$ gera um corpo F. Seja $t = \dim_Q F$. (os elementos $x(\sigma)$ são todos algébricos sobre Q pois $x(\sigma)^m = 1$ onde $m = o(\sigma)$).

Seja $\{x_1, \ldots, x_t\}$ uma base integral de F sobre Q. Existem então inteiros $a_1(\sigma), \ldots, a_t(\sigma)$ tais que

$$x(\sigma) - 1 = a_1(\sigma)\ x_1 + \ldots + a_t(\sigma)\ x_t \quad a_i(\sigma) \in Z \quad i = 1, \ldots, t,\ \sigma \in G.$$

Temos então que

$$x_1\ \lg_{p_o}\ \tau_{p_o} \prod_{\sigma \in G \setminus \{1\}} \sigma(u)^{a_1(\sigma)} + \ldots + x_t\ \lg_{p_o}\ \tau_{p_o} \prod_{\sigma \in G \setminus \{1\}} \sigma(u)^{t(\sigma)} = 0$$

Existem então racionais (ou inteiros) $n_1, \ldots, n_t$ tais que

$$\lg_{p_o}\ \tau_{p_o} \prod_{\sigma \in G \setminus \{1\}} \sigma(u)^{b(\sigma)} = 0$$

onde $b(\sigma) = n_1\ a_1(\sigma) + \ldots + n_t\ a_t(\sigma) \quad b(\sigma) \in Z$.

Como antes usando o resultado de Minkowski mencionado, [11], ou o teorema II.4.1, deduzimos que $b(\sigma) = 0$ para todo σ.

Mas isso é absurdo pois se $n_1 \neq 0$ temos que

$$a_1(\sigma) = -\frac{n_2}{n_1}\ a_2(\sigma) + \ldots - \frac{n_t}{n_1}\ a_t(\sigma)$$

Então

$$x(\sigma) - 1 = a_2(\sigma)(- \frac{n_2}{n_1} x_1 + x_2) + \ldots + a_t(\sigma)(- \frac{n_t}{n_1} x_1 + x_t)$$

Nesse caso $\dim_Q F$ não seria t.

SEÇÃO III.7 UM CASO ESPECIAL RESOLVIDO POR MÉTODOS ALGÉBRICOS

TEOREMA III.7.1 Seja p um primo regular, a um inteiro positivo, ξ, uma raiz primitiva p^a-ésima da unidade e $K = Q(\xi)$. Então $r_p = r$.

DEMONSTRAÇÃO

$E_p = U^{(N-1)p^t}$ com $N = N(P)$ P ideal primo que está sobre p, e t é o menor inteiro que verifica $p^t > e = p^{a-1}(p-1)$.

Na seção III.1 provamos que $P = (1-\xi)\mathcal{O}$ (onde $\mathcal{O}$ são os inteiros de K.). Então $N(P) = N(1-\xi)$. Na seção III.1 também provamos que:

$$p = (1-\xi)^{p^{a-1}(p-1)}\varepsilon.$$

Em consequência $N(p) = (N(1-\xi))^{p^{a-1}(p-1)}$. Mas como $p \in Q$

$$N(p) = p^{p^{a-1}(p-1)}.$$

Em definitivo temos que $N(P) = p$. Sabemos também (seção III.1) que $e = p^{a-1}(p-1)$ então o menor inteiro que verifica $p^t > p^a - p^{a-1}$ é a. Então $E_p = U^{(N-1)p^t} = U^{(p-1)p^a}$.

Sabemos que $r_p \leq r$, vamos supor que $r_p < r$.

Se $v_1, \ldots, v_r$ são um sistema de inversíveis fundamentais de $\mathcal{O}$, então $v_1^{(p-1)p^a}, \ldots, v_r^{(p-1)p^a}$ são uma base de E_p sobre Z. Seja $u_i = v_i^{(p-1)p^a}$. Se $r_p < r$ existem $\alpha_i \in Z_p$ não todos nulos tais que:

$$(1) \qquad \sum_{i=1}^{r} \alpha_i \; lg_p \; \tau_p \; u_i = 0 \qquad \text{para todo} \quad P/p.$$

Como Z_p é um anel local podemos supor que $\alpha_1 = 1$.

Chamaremos $w_i = v_i^{p-1}$, então $w_i^{p^a} = u_i$.

Nos elementos w_i podemos definir lg_p pois $\nu_p(w_i - 1) \geq 1$. Isso é consequência de que $\#((\mathcal{O}/P)^*) = N(P) - 1 = p-1$. Então $(v_i + P)^{p-1} = 1 + P$, ou seja $w_i \quad 1 \pmod P$)

Temos então substituindo em (1) que:

$$(2) \qquad \sum_{i=1}^{r} \alpha_i \; lg_p \; \tau_p \; u_i = p^a \sum_{i=1}^{r} \alpha_i \; lg_p \; \tau_p \; w_i = 0$$

Temos agora a dificuldade de que não sabemos se

$$lg_p \; \tau_p \; w_i \in D_p$$

onde D_p e o anel da valorização ν_p em K_p.

Existe um $b \geq 0$ tal que

$$(3) \quad p^b \; lg_p \; \tau_p \; w_i \in p^2 \; D_p \qquad \text{para} \qquad i = 1 \ldots r.$$

Os elementos α_i da relação (2) são de Z_p mas existem $a_i \in Z$ tais que

$$(4) \qquad a_i \equiv \alpha_i \; (\text{mod } p^b \; Z_p) \qquad i = 1 \ldots r$$

Temos então que

$$lg_p \; \tau_p \; [w_1 \prod_{i=2}^{r} w_i^{a_i}] =$$

$$= lg_p \; \tau_p \; w_1 + \sum_{i=2}^{r} a_i \; lg_p \; \tau_p \; w_i = \sum_{i=2}^{r} (a_i - \alpha_i) \; lg_p \; \tau_p \; w_i$$

Essa última expressão por (4) e (3) está em $p^2 \; D_p$.

Temos então que

$$(5) \qquad lg_p\ \tau_p\ [w_i \prod_{i=2}^{r} w_i^{a_i}] = p^2 x \qquad \text{com} \quad x \in D_p$$

Temos que $p^2x = p(px) = lg\{(\exp(px))^p\}$ pois $lg \exp px = px$ dado que $\nu_p(px) \geq \kappa$.

Neste caso $\kappa = \left[\frac{e}{p-1}\right] + 1 = \left[\frac{p^{a-1}(p-1)}{p-1}\right] + 1 = p^{a-1} + 1$

$$\nu_p(px) = e + \nu_p(x) \geq e = p^{a-1}(p-1) \geq p^{a-1} + 1 \qquad \text{se} \quad p \neq 2$$

No caso $p = 2$ em (3) devemos substituir $p^2\ D_p$ por $2^3\ D_p$. Em (5) teríamos a validez da igualdade com $x \in p\ D_p$.

Nesse caso

$$\nu_p(px) = e + \nu_p(x) \geq 2\ e = 2\ 2^{a-1} = 2^a \geq 2^{a-1} + 1 = \kappa$$

Chamando então $y = \exp(px)$ temos que $y \in D_p$ (seção III.3). Em definitivo temos que se

$$z = \tau_p\ (w_1 \prod_{i=2}^{r} w_i^{a_i}) \qquad z_0 = w_1 \prod_{i=2}^{r} w_i^{a_i} \qquad lg_p\ z = lg_p\ y^p$$

Existe então pelo teorema III.3.2 γ raiz da unidade em K_p tal que

$$(6) \qquad \gamma z = y^p \qquad \text{com} \qquad \gamma^{p^s} = 1$$

Acontece que as raízes da unidade de ordem uma potência de p em K_p são da forma $\tau_p\ \eta$ com η raiz da unidade em K. Seja γ uma raiz da unidade de ordem p^ν com $\nu > a$ temos a seguinte situação

$$\begin{array}{ccccc}
\tilde{P} & & Q(\gamma) & \longrightarrow & [Q(\gamma)]_{\tilde{P}} \\
| & & | & & | \\
P & & Q(\xi) & \longrightarrow & [Q(\xi)]_P \\
| & & | & & | \\
p & & Q & \longrightarrow & Q_p
\end{array}$$

Como $p = P^n$ e $p = \tilde{P}^r$ existe um único divisor primo de $Q(\gamma)$ que está sobre P.

Consideremos $Irr(\gamma, Q(\xi))$, esse polinômio como polinômio a coeficientes em $[Q(\xi)]_P$ se fatoriza em tantos fatores irredutíveis como divisores de $Q(\gamma)$ estão sobre P. Temos então que

$$Irr(\gamma, Q(\xi)) = (\beta(x))^m \quad \text{onde} \quad \beta = Irr(\gamma, [Q(\xi)]_P)$$

(para o anterior ver teorema 3 pg.271 [3])

Mas como $\gamma \in [Q(\xi)]_P$ temos que $\beta(x) = x - \gamma$. Então

$$Irr(\gamma, Q(\xi)) = (x-\gamma)^m,$$

em consequência $\gamma \in Q(\xi)$.

Temos então que $\gamma = \tau_P(\eta)$ $\eta = \xi^i$. Ou seja que a igualdade (6) se transforma em

$$(7) \qquad \tau_P(\xi^i z_0) = y^p \quad \text{com} \quad y \in D_P$$

Queremos provar que $y = \tau_P\, y_0$ com $y_0 \in K = Q(\xi)$.

Consideremos o polinômio $f(x) = x^p - \xi^i z_0$.

Seja L = corpo de partição de f sobre K.

Sabemos pelos resultados da seção III.2 que os primos de K que não estão sobre p, não se ramificam em L. Sabemos também que a extensão L de K é abeliana.

Então o único primo de K que poderia ramificar-se em L é P. Veremos que P também não se ramifica.

Seja w_0 uma raiz arbitrária de f. Sabemos que $L = K(w_0)$. Se $w_0 \in K$ não temos nada para demonstrar.

Em caso contrário temos que $P = \tilde{P}_1^{e_1} \ldots \tilde{P}_t^{e_t}$ onde $\tilde{P}_i$ são primos de L que estão sobre P, e $\tilde{P}_i$ corresponde a um fator irredutível de $x^p - \xi^i z_0$ sobre K_P (teorema 3 pg.271 [3]).

Em K_p o polinômio $x^p - \xi^i z_o$ se fatoriza totalmente, então $t = p$, na decomposição anterior.

Agora sabemos que $\sum_{i=1}^{p} e_i f_i = \dim_K L = p$ então $e_i = 1$ $i = 1 \dots p$. Aplicando agora um resultado da teoria de corpos de classes de Hilbert (teorema 131 pg.191 [8]) temos que $[L:K]/h$.

Como $p \nmid h$ (no caso $a = 1$ é a definição de primo regular, no caso $a > 1$ é um teorema de Iwasawa [7]) e $[L:K] = p$ ou 1, temos que $[L:K] = 1$. Ou seja que (7) se transforma em $\xi^i z_o = \alpha^p$ com $\alpha \in K$

$$\xi^i z_o = \xi^i (w_1 \prod_2^r w_i^{a_i}) = \xi^i (v_1 \prod_2^r v_i^{a_i})^{p-1} = \alpha^p \quad \alpha \text{ inversível de } K$$

Então

$$\xi^{i'} z_o \in U^p \qquad U = \text{inversíveis de } K$$

Passando à última igualdade ao quociente módulo as raízes de unidade temos

$$(\tilde{v}_1 \prod_2^r \tilde{v}_i^{a_i})^{p-1} \in (U/C)^p = E^p \qquad E = U/C$$

Como $\ell = \tilde{v}_1 \prod_2^r \tilde{v}_i^{a_i} \in E$ por construção, temos que

$$\tilde{v}_1 \prod_2^r \tilde{v}_i^{a_i} \in E^p$$

Como os $v_1, \dots, v_r$ são um conjunto de inversíveis **fundamentais**, os $\tilde{v}_1, \dots, \tilde{v}_r$ são uma base de E, logo

$$\tilde{v}_1 \prod_2^r \tilde{v}_i^{a_i} = (\prod_{j=1}^r \tilde{v}_j^{b_j})^p$$

ou seja que $1 = b_j\, p$ absurdo.

<u>c.q.d.</u>

B I B L I O G R A F I A

[1] *JAMES AX* "ON THE UNITS OF AN ALGEBRAIC NUMBER FIELD" Illinois J. of Mathematics Vol.9 Nº4 (1965) pg.584-589.

[2] *JAMES AX* "THE GALOIS ACTION ON THE UNITS" Preprint do artigo anterior.

[3] *Z.I.BOREVICH* and *I.R.SHAFAREVICH* "NUMBER THEORY" Academic Press.

[4] *C.CURTIS* and *I.REINER* "REPRESENTATION THEORY OF FINITE GROUPS AND ASSOCIATIVE ALGEBRAS" New York, Interscience.

[5] *B.N.DELONE* and *D.K.FADDEEV* "THE THEORY OF IRRATIONALITIES OF THE THIRD DEGREE" Translations of Mathematical Monographs. Volume 10.

[6] *H.HASSE* "ZAHLENTHEORIE" Akademie - Verlag, Berlin, 1949.

[7] *K.IWASAWA* "A NOTE ON CLASS NUMBERS OF ALGEBRAIC NUMBER FIELDS" Abh. Math. Sem. Univ. Hamburg, 20 (1956), 257-258.

[8] *GERALD J. JANUSZ* "ALGEBRAIC NUMBER FIELDS". Academic Press.

[9] *H.W. LEOPOLDT* "ZUR ARITHMETIC IN ABELSCHEN ZAHLENKÖRPERN" J.Reine Angew. Math., 209 (1962) 54-71.

[10] *K.MAHLER* "ÜBER TRANSZENDENTE P-ADISCHE ZAHLEN" Com positio Math. 2 (1935), 259-275.

[11] *H.MINKOWSKI* "ZUR THEORIE DER EINHEITEN IN DEN ALGEBRAI SCHE ZAHLKÖRPERN" Göttiner Nachrichten, 1900, p.90.

[12] *M.NEWMAN* "INTEGRAL MATRICES" Academic Press

[13] *C.POLCINO* "SOBRE AS UNIDADES DE ANÉIS DE GRUPOS" Dissertação de Mestrado. IMEUSP.

[14] *S.WARNER* "MODERN ALGEBRA" Prentice-Hall, inc.

[15] *E.WEISS* "ALGEBRAIC NUMBER THEORY" Mac Graw - Hill Book Company, Inc.