Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Discriminante dos Subcorpos de Corpos Ciclotômicos de Condutores Potência de Um Primo Ímpar

por

Carlos Henrique Souza de Jesus

sob orientação do

Prof. Dr. Orlando Stanley Juriaans

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Março/2006
João Pessoa - Pb

Discriminante dos Subcorpos de Corpos Ciclotômicos de Condutores Potência de Um Primo Ímpar

por

Carlos Henrique Souza de Jesus

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Orlando Stanley Juriaans - IME-USP (Orientador)

Prof. Dr. José Gomes de Assis - UFPB

Prof. Dr. João Montenegro de Miranda - UEC

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Março/2006

Agradecimentos

- Ao professor Dr. Orlando Stanley Juriaans, da USP, pela orientação, pelos ensinamentos desde o curso de verão, e pelo privilégio que tive em ser seu orientando e tê-lo como crítico deste trabalho.

- Ao Professor Dr. João Lucas Marques Barbosa, da UFC, pelo total apoio no momento certo e por acreditar em meu potencial.

- Ao Professor Dr. João Marcos Bezerra do Ó, pela oportunidade única de crescimento acadêmico que me ofereceu.

- Ao Professor Dr. Roberto Callejas Bedregal, pelas importantes sujestões, pelos ensinamentos bem humorados e, acima de tudo, pelos frutíferos "momentos de loucura"das aulas de Álgebra Comutativa.

- Ao Professor Dr. Trajano Pires da Nóbrega Neto, da UNESP, pelas sugestões e colaboração virtual a mim dirigidas sem nenhuma obrigação ou vínculo institucional, sem ao menos me conhecer pessoalmente. Por me ajudar simplesmente pelo bem da Matemática.

- Ao Professor Dr. José Gomes de Assis, pela leitura crítica, sugestões e além disso, por saber ser amigo nas horas difíceis.

- Ao Professor Dr. Antônio Andrade e Silva, pela colaboração e ensinamentos durante todo o curso.

- Ao Professor Dr. João Montenegro de Miranda, da UFCE, pela leitura crítica e sugestões.

- Aos professores Doutores Everaldo Souto de Medeiros, Nelson Nery de Oliveira Castro, Rodrigo Ristow Montes e a todos os professores do programa de pós-graduação em Matemática da UFPB, que me proporcionaram a aquisição de um bem valoroso, porém pequeno: meu conhecimento matemático.

- A todos os colegas de mestrado, companheiros de luta, cito José "Shrek"Anderson, como representante dos alunos, que me proporcinaram a aquisição de um bem valoroso e grande: o binômio coleguismo-amizade.

- A meus colegas-amigos Reinaldo Marchi e Wilmar Vaz, pelo companherismo e parceria nos estudos, sem a qual colaboração provavelmente não obteríamos sucesso.

- Aos meus amigos paraibanos de fora da Matemática, Onildo de Souza Monteiro e Valentim Arash Carvalho Dana, pela atenção dispensada a mim, pelas atitudes e palavras que me conduziam à crença de que um dia o sertão vai virar mar.

- Ao Professor Geraldo Daltro Lopes da Silveira, da UFPA, pelo apoio imprescindível, interesse e incentivo para a realização deste curso, além de ter sido um dos melhores professores de Matemática que tive o prazer de ser aluno.

- Aos colegas da UFPA em Marabá, em especial ao coordenador do campus, professor Erivan Souza Cruz, pela compreensão e boa vontade dispensadas no sentido de me permitir uma maior dedicação a este curso.

- À Professora Andrea Cristina Santos de Jesus, da UFRN, pelo apoio permanente, incentivo a este projeto, colaboração positivista vizando o progresso pessoal, e pelo filho maravilhoso que me deu.

- À Dançarina Emanuela Silva do Livramento, por me valorizar acima do que eu realmente sou, pela presença de espírito e bom humor, e pelo filho maravilhoso que me deu.

- Aos meus irmãos Antônio e Luiz Henrique e minha mãe Maria Lídia, pelo apoio incondicional a mim dispensado, provando que só a distância não é suficiente para separar, nem o tempo o bastante para destruir.

- À memória de meu pai Arnaldo Pereira e minha avó Meiry, por estarem sempre presentes comigo no meu pensamento.

"As coisas encobertas são para o Senhor nosso Deus, porém as reveladas são para nós e para nossos filhos para sempre"...

Deuteronômio 29/29

Aos meus filhos
André e Emanuel Henrique.

Resumo

O discriminante de um corpo de números K tem aplicabilidade tecnológica, por isso vários estudiosos vêm se ocupando em seu cálculo, e certamente encontram dificuldade quando tentam determinar uma base integral para K. Se tal corpo K for abeliano, pode-se recorrer ao teorema de Kronecker-Weber que assegura que K está contido em alguma extensão ciclotômica $\mathbb{Q}(\zeta_m)$ e, neste caso, pode-se aplicar o teorema de Hasse para calcular o discriminante de K.

O resultado aqui obtido está restrito ao cálculo do discriminante de corpos de números, subcorpos de corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$, onde p é um primo ímpar. E para tal cálculo apresentamos uma fórmula em função do grau de K.

Abstract

The discriminant of a number field K has technological applicability and because of that, many researchers have being occupying themselves with its calculation, and certainly finding difficulties in determining an integral base for K. If such a field K is abelian, one can appeal to the Kronecker-Weber Theorem which assures that K is contained in a cyclotomic extension $\mathbb{Q}(\zeta_m)$ and, in this case, the Theorem of Hasse can be applied for evaluating the discriminant of K.

The result obtained here is restricted to calculation of the discriminant of number fields, subfields of cyclotomic fields $\mathbb{Q}(\zeta_{p^r})$, where p is an odd prime. And for such calculation a formula in function of K's degree is presented.

Notação

$\widehat{G}$ - Grupo do caracteres do grupo G.

$\langle g \rangle$ - Subgrupo gerado por g.

$\frac{\mathbb{Z}}{n\mathbb{Z}}$ - Anel dos inteiros módulo n.

$(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ - Grupo multiplicativo dos elementos inversíveis de $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

(a, b) - Máximo divisor comum de a e b.

$[a, b]$ - Mínimo múltiplo comum de a e b.

$\varphi(n)$ - Função de Euler.

K^* - Grupo cíclico multiplicativo do corpo K.

$K[x]$ - Anel dos polinômios sobre o corpo K.

$[L : K]$ - Grau da extenção L sobre K.

$(G : H)$ - Índice do subgrupo H em G.

$\mathbb{N}$ - Conjunto dos números naturais.

$\mathbb{Z}$ - Conjunto dos números inteiros.

$D(n)$ - Conjunto dos divisores de n.

$\equiv$ - Congruente.

$|$ - Divide.

$disc(K)$ - Discriminante do corpo K.

$Ker\varphi$ - Núcleo de φ.

$Im\varphi$ - Imagem de φ.

$\mathcal{T}_{L/K}(x)$ - Traço de x relativamente a L e K.

$\mathcal{N}_{L/K}(x)$ - Norma de x relativamente a L e K.

$det\ M$ - determinante da matriz M.

I_K - Anel dos inteiros de um corpo de números K.

$Gal(L/K)$ - Grupo de Galois de L sobre K.

X_K - Grupo dos caracteres associados a K.

f_χ - Condutor do caracter χ.

ζ_n - Raiz primitiva n-ésima da unidade.

$U_{(n)}$ - Conjunto das raízes n-ésimas da unidade.

$P_{(n)}$ - Conjunto das raízes primitivas n-ésimas da unidade.

$|A|$ - Cardinalidade do conjunto A.

$\mathbb{Q}(i)$ - Corpo de números gaussianos.

$\mathbb{Z}[\ i\ ]$ - Anel dos inteiros gaussianos.

Conteúdo

Introdução

"Que aqui não adentrem aqueles que não conhecem Geometria".

Inscrição de advertência afixada na entrada da academia de filosofia de Atenas, fundada por Platão no séc. IV a.C.

Os corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$, com p primo ímpar e r inteiro positivo, representam uma família na categoria dos corpos de números algébricos que permite o uso da Teoria de Galois no cálculo do discriminante, entre outros estudos aqui não abordados.

O parâmetro densidade de empacotamento esférico dos reticulados, subgrupos discretos do $\mathbb{R}^n$, depende do discriminante do corpo K, neste caso o volume da região fundamental, além da função traço relativo e da norma do ideal $\mathfrak{i}$, quando tal reticulado for a representação geométrica de um ideal ordinário $\mathfrak{i}$ do anel dos inteiros algébricos de um corpo de números K.

Os reticulados têm se mostrado bastante úteis em aplicações na teoria das comunicações, contudo reticulados de maior interesse são aqueles com maior densidade de empacotamento, o qual podemos obter formando o discriminante mínimo.

Empacotamento esférico é a disposição de esferas de mesmo raio no espaço euclidiano n-dimensional, de tal modo que a interseção de duas delas tenha no máximo um ponto. A forma de dispor essas esferas de modo a cobrir a maior parte do espaço, tem sido um desafio e mereceu citação de Hilbert no ano de 1900 como o 18^o problema de uma lista de desafios que ocuparam destaque no desenvolvimento das ciências ao longo de todo século XX e até hoje.

As pesquisas de base, em Matemática pura, apontam progressivamente para uma maior ligação com vários outros campos da ciência. Nosso trabalho, baseado no artigo *"On computing discriminants of subfields of* $\mathbb{Q}(\zeta_{p^r})$" publicado no *Journal of Number Theory 96/2002*, não foge desta linha e procura mostrar que processo foi utilizado na obtenção de um dos itens formador de um resultado importante da Teoria dos Números, o discriminante de corpos de números abelianos.

Corpos de números abelianos são extensões normais de $\mathbb{Q}$ com grupo de Galois abeliano que, segundo Kronecker e Weber, estão sempre contidos em algum corpo ciclotômico $\mathbb{Q}(\zeta_n)$.

O cálculo do discriminante de um corpo de números K, conforme sua definição original, depende do conhecimento de uma base integral do anel dos inteiros algébricos de K (I_K como $\mathbb{Z}$-módulo) e seu valor relativo, do conjunto das imersões de K no corpo dos números complexos.

Para corpos com condutor potência de um primo ímpar, ou seja, subcorpos de $\mathbb{Q}(\zeta_{p^r})$, devido a correspondência de Galois, o discriminante absoluto de K pode ser calculado em função do seu grau, aplicando a fórmula do condutor-discriminante. Este é o nosso resultado principal correspondente ao teorema 4.1.

Entretanto para alcançarmos este objetivo precisaremos de três lemas como pré-requisito e do teorema de Hasse. Estes resultados, compilados no terceiro capítulo e mais o lema do condutor, formam um preâmbulo para o cálculo do discriminante para o qual nos propomos.

No segundo capítulo, procuramos desenvolver resultados clássicos da teoria dos caracteres em grupos abelianos finitos, atenção especial dada ao estudo dos caracteres de Dirichlet, com destaque para o conceito de condutor de um caracter numérico.

As referências principais para os tópicos abordados nestes capítulos foram os livros [Was,Rib].

No primeiro capítulo apresentamos ao leitor alguns resultados indispensáveis para o entendimento dos elementos conceituais que compõem o título desta dissertação. Como a noção de corpos de números algébricos, com enfoque maior aos corpos ciclotômicos, qual o significado de condutor de um corpo abeliano, e o que é afinal o discriminante de um corpo de números e sua indissociada base integral. As principais referências utilizadas nesses capítulos, tanto no conteúdo quanto na notação foram [End1,Sam].

No apêndice A foi escrito um capítulo "zero", com o objetivo introdutório, constituído dos resultados básicos aplicados, vizando atender aos leitores sem formação em Teoria Algébrica dos Números, porém interessados num melhor entendimento das técnicas aqui abordadas, tal como a definição de inteiro algébrico, anel integralmente fechado, norma e traço relativos e polinômio característico. Iniciamos com uma apresentação das estruturas algébricas, com destaque para o grupo de Galois, grupo multiplicativo das unidades do anel dos inteiros módulo n e extensão galoisiana dos racionais.

Faremos uso exaustivo do anel $\mathbb{Z}$ como domínio principal integralmente fechado, bem como do seu corpo de frações $\mathbb{Q}$ e de $\mathbb{Z}$-módulos F.G., denotaremos por L o corpo de decomposição de um determinado polinômio ou para indicar um corpo ciclotômico em questão. L como extensão finita de $\mathbb{Q}$ estará sempre contido em $\mathbb{C}$.

K denotará qualquer subcorpo de L que contém $\mathbb{Q}$.

O anel dos inteiros algébricos será denotado por I_K, podendo ser um domínio fatorial não necessariamente euclidiano.

Enunciamos os atributos essenciais e específicos do anel dos inteiros de um corpo de números K de modo que o torne inconfundível com qualquer outro fecho, além das bases do método da Teoria dos Caracteres, a Teoria de Galois. As principais referências pesquisadas neste apêndice foram [Bha,End2,Rot,Lan,Ste].

Desta maneira tentamos tornar este trabalho enxuto, conciso, de fácil entendimento, e o mais auto-suficiente possível.

Capítulo 1

Corpos de Números Algébricos e Seu Principal Invariante

"Leiam, leiam Euler. Ele é nosso mestre em tudo".
Pierre de Laplace, séc. XVIII, recomendando Introdução à Análise Infinita a seus alunos.

Um corpo de números algébricos, ou simplesmente corpo de números é uma extensão finita do corpo dos números racionais. Corpos de números têm característica zero.

1.1 Corpos Quadráticos

Um corpo quadrático é uma extensão K de $\mathbb{Q}$ de grau dois.

Note que qualquer elemento $\alpha \in K/\mathbb{Q}$ é um elemento primitivo da extensão K. De fato, $1 < [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [K : \mathbb{Q}] = 2$, decorre que $K = \mathbb{Q}(\alpha)$.

Os elementos $1,\ \alpha$ formam uma base desta extensão e $F_{\alpha,K\mathbb{Q}} = P_{\alpha|\mathbb{Q}}$ é um polinômio em $\mathbb{Q}[x]$ de grau dois.

Todo corpo quadrático possui um elemento primitivo distinguido da forma $\sqrt{d}$, univocamente determinado a menos de sinal, onde $d \in \mathcal{D}$ é um número inteiro livre de quadrados, isto é, $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, onde os $p_{i's}$ são números primos e $\alpha_i \in \{0, 1\}$. Seja $\mathcal{D} = \{d \in \mathbb{Z} \setminus \{0, 1\} \ ; 1 \neq c^2 \nmid d, \ \ c \in \mathbb{Z}\}$ conjunto dos números inteiros livres de quadrados, e considere $\mathcal{Q} = \{K \ ; \ \mathbb{Q} \subseteq K \subseteq \mathbb{C} \ \ e \ \ [K : \mathbb{Q}] = 2\}$ conjunto dos corpos quadráticos de $\mathbb{Q}$.

Para cada número inteiro livre de quadrados, temos um único corpo quadrático correspondente, e reciprocamente. Ou seja, A aplicação $f : \mathcal{D} \to \mathcal{Q}$, dada por $f(d) = \mathbb{Q}(\sqrt{d})$ é bijetiva.

Diremos que um corpo quadrático $K = \mathbb{Q}(\sqrt{d})$ é;

a) Real, ou seja $K \subseteq \mathbb{R}$, quando $d > 0$;

b) Imaginário, quando $d < 0$.

Sabemos que todo domínio fatorial é integralmente fechado em seu corpo de frações, no entanto o anel I_K é integralmente fechado em K, mas não é um domínio fatorial, pois para $K = \mathbb{Q}(\sqrt{-5})$ o domínio $\mathbb{Z}[\sqrt{-5}]$ não é fatorial.

Mencionamos, neste contexto que, para qualquer corpo de números algébricos K, o anel I_K será fatorial;

a) se, e somente se I_K for um domínio principal;

b) se, e somente se o seu número de classes n_K for igual a 1.

Definição 1.1 *Um domínio R é euclidiano, se existir uma aplicação*

$$\varepsilon : R \setminus \{0\} \to \mathbb{N}$$

com as seguintes propriedades:

i) $b|a$ *implica* $\varepsilon(b) \leq \varepsilon(a), \quad a, b \in R \setminus \{0\}$;

ii) $\exists\exists!\ q, r \in R$, *tais que* $a = bq + r$, *com* $r = 0$ *ou* $\varepsilon(r) < \varepsilon(b)$

Portanto, todo DE, domínio euclidiano, é principal e, daí, fatorial.

De fato, dado um ideal não-nulo $\mathfrak{a}$ de R, existe $b \in \mathfrak{a} \setminus \{0\}$, tal que $\varepsilon(b)$ seja minimal em $\{\varepsilon(a) \ ; a \in \mathfrak{a} \setminus \{0\}\}$.
Para qualquer $a \in \mathfrak{a}$, sejam $q, r \in R$, tais que $a = bq + r$ e $r = 0$ ou $\varepsilon(r) < \varepsilon(b)$,
como $r = a - bq \in \mathfrak{a}$, pois $bq + r \in \mathfrak{a}$,
veja $r \in \mathfrak{a}$, mas $\varepsilon(r) \not< \varepsilon(b)$, pois $\varepsilon(b)$ é mínimo,
daí $r = 0$ e $a = bq \in < b >$, concluimos que $\mathfrak{a} = < b >$ é principal.
Assim, R é um domínio principal, logo fatorial.

Diagrama de ordenação dos domínios

Exemplos de domínios euclidianos;

a) $\mathbb{Z}$, anel dos inteiros, com a aplicação $\varepsilon = |\ |$, valor absoluto.

$$\varepsilon : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$$

$$a \rightsquigarrow |a|$$

b) $K[x]$, anel dos polinômios sobre um corpo K qualquer, com a aplicação $\varepsilon = \partial$, grau do polinômio.

$$\varepsilon : K[x] \setminus \{0\} \to \mathbb{N}$$

$$f \rightsquigarrow \partial f$$

c) Em alguns casos, I_K, anel dos inteiros algébricos sobre o corpo quadrático $K = \mathbb{Q}(\sqrt{d})$, com a aplicação $\varepsilon = |\mathcal{N}_{K|\mathbb{Q}}(\ )|$, norma absoluta (a norma será sempre não-negativa quando $d < 0$).

$$\varepsilon : \ I_K \setminus \{0\} \to \mathbb{N}$$

$$\alpha \rightsquigarrow |\mathcal{N}_{K|\mathbb{Q}}(\alpha)|$$

Para I_K ser um domínio de fatoração única é suficiente, mas não é necessário que ele seja euclidiano.

Observação 1.2 *Em relação ao exemplo c), a propriedade ii da definição 1.1 é satisfeita apenas quando* $d \in \{-1,-2,-3,-7,-11\} \cup \{2,3,5,7,11,13,17,19,21,29,33,37,41,57,73\}$*, ou seja, temos 21 casos em que* $I_{\mathbb{Q}(\sqrt{d})}$ *é um DE em relação à norma absoluta. E não se sabe se existem outros* $d \in \mathcal{D}$ *tais que o domínio indicado seja euclidiano em relação a uma função* ε *diferente da norma absoluta.*

Um exemplo importante de DE é $\mathbb{Z}[\,i\,]$ o anel dos inteiros de Gauss o qual é igual ao anel $I_{\mathbb{Q}(i)}$ dos inteiros algébricos do corpo de números gaussianos, onde $i = \sqrt{-1}$.

Lema 1.3 $\mathbb{Z}[\,i\,]$ *é euclidiano em relação à norma* $\mathcal{N}_{\mathbb{Q}(i)/\mathbb{Q}}$.

Prova.

Dados os elementos $\alpha, \beta \in \mathbb{Z}[\,i\,]$, existem $u, v \in \mathbb{Q}$, tais que $\alpha\beta^{-1} = u + vi$, fazendo $\mathcal{N}_{\mathbb{Q}(i)|\mathbb{Q}} = \mathcal{N}$, temos $\mathcal{N}(\alpha\beta^{-1}) = \mathcal{N}(\alpha)\mathcal{N}(\beta^{-1}) = \mathcal{N}(u+vi)$.

Sendo $d = -1$, $\mathcal{N}(x) \geq 0, \forall\, x$, logo $\beta|\alpha$ implica $\mathcal{N}(\beta) \leq \mathcal{N}(\alpha)$.

Agora, existem $m, n \in \mathbb{Z}$, tais que $|u-m| \leq \dfrac{1}{2}$ e $|v-n| \leq \dfrac{1}{2}$, isto é, $m = [u], n = [v]$. Então temos que existem únicos $m+ni, \rho \in \mathbb{Z}[\,i\,]$, tais que $\alpha = \beta(m+ni) + \rho$, onde $\rho = 0$ ou $\mathcal{N}(\rho) < \mathcal{N}(\beta)$.
De fato, $\rho = \alpha - \beta(m+ni)$, mas

$$\alpha = (u+vi)\beta \Rightarrow \rho = \beta(u+vi) - \beta(m+ni) \Rightarrow \rho = \big((u-m)+(v-n)i\big)\beta \Rightarrow$$

$$\mathcal{N}(\rho) = \mathcal{N}((u-m)+(v-n)i)\mathcal{N}(\beta) \Rightarrow \mathcal{N}(\rho) = \mathcal{N}((u-m)^2+(v-n)^2)\mathcal{N}(\beta),$$

como $|u-m|\,,\ |v-n| \leq \dfrac{1}{2} \Rightarrow (u-m)^2, (v-n)^2 \leq \dfrac{1}{4} \Rightarrow 0 < ((u-m)^2+(v-n)^2) < 1$, daí $\mathcal{N}(\rho) < \mathcal{N}(\beta)$. ■

1.2 Corpos Ciclotômicos

Considere e o elemento neutro de um grupo multiplicativo G. Dado um elemento $a \in G$, se $a^m \neq e$, $\forall\, m \in \mathbb{N} \setminus \{0\}$, diremos que a tem ordem infinita.

Se existir um número inteiro $m > 0$, tal que $a^m = e$, diremos que a tem período m ou ordem m, quando m for o menor inteiro satisfazendo essa condição. Para qualquer $0 \neq \alpha \in \mathbb{C}$, denotamos por $\mathrm{o}(\alpha)$ a ordem de α no grupo multiplicativo $\mathbb{C}^*$.

Diremos que $\alpha \in \mathbb{C}^*$ é uma raiz n-ésima da unidade em $\mathbb{C}$, quando $\alpha^n = 1$. Assim, uma raiz n-ésima da unidade é um inteiro algébrico em $\mathbb{C}$, raiz do polinômio $x^n - 1$.

O conjunto das raízes n-ésimas da unidade forma um grupo cíclico multiplicativo de ordem n, denotado por $U_n(\mathbb{C})$, ou simplesmente $U_{(n)}$.

$\mathbb{C}^*$ não é cíclico, mas todo subgrupo finito de $\mathbb{C}^*$ é da forma $U_{(n)}$. Um gerador deste grupo é chamado de raiz primitiva n-ésima da unidade e é denotado por ζ_n, ou simplesmente ζ. O número complexo ζ_n^m é uma raiz primitiva n-ésima da unidade se, e

somente se $mdc(m,n)=1$, portanto o número de raízes primitivas n-ésimas da unidades é $\varphi(n)$, onde φ é a função φ de Euler. Ou seja, o conjunto das raízes primitivas n-ésimas da unidade em $\mathbb{C}$ tem ordem $\varphi(n)$ e é denotado por $P_n(\mathbb{C})$, ou simplesmente $P_{(n)}$.

Observemos que a existência de uma raiz primitiva n-ésima da unidade pertencente a um corpo algebricamente fechado $\Omega \supseteq L$ é garantida por que a característica do corpo de decomposição L de x^n-1, que é um corpo de números, não divide n, isto é, $P_n(\Omega) \neq \phi \Leftrightarrow car(L) \nmid n$, o que é trivial quando $car(L)=0$.

O conjunto das raízes primitivas n-ésimas da unidade, também um subconjunto dos inteiros algébricos em $\mathbb{C}$, é constituido das raízes distintas do polinômio minimal de ζ_n, $P_{\zeta_n/\mathbb{Q}} = \prod_{(i,\ j)=1} (x-\zeta_n^j) \in \mathbb{Z}[x]$, conhecido como n-ésimo polinômio ciclotômico, e denotado por Φ_n.

O n-ésimo polinômio ciclotômico Φ_n é um polinômio mônico em $\mathbb{Z}[x]$ de grau $\varphi(n)$ e irredutível em $\mathbb{Q}[x]$.

Temos que $x^n-1 = \prod_{d|n} \Phi_d$, pois $U_{(n)} = \bigcup_{d|n} U_{(d)}$.

Se $n=p$, um número primo, temos $p-1$ raízes primitivas n-ésimas da unidade e portanto a única raiz p-ésima da unidade que não é primitiva é 1.

Desta forma, $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$.

Os seis primeiros polinômios ciclotômicos são;

$$\Phi_1 = x-1,\ \ \Phi_2 = x+1,\ \Phi_3 = x^2+x+1,$$
$$\Phi_4 = x^2+1,\ \Phi_5 = x^4+x^3+x^2+x+1 \text{ e } \Phi_6 = x^2-x+1.$$

Uma curiosidade notável diz respeito aos coeficientes dos 104 primeiros polinômios ciclotômicos que estão todos em $\{-1,0,1\}$. Agora, para $n \geq 105$ os coeficientes explodem, isto é, ocorrem coeficientes arbitrariamente grandes em $\mathbb{Z}$. Uma outra, diz respeito à alternância do sinal de seus termos, ou seja, $\Phi_{2n}(x) = \Phi_n(-x)$, mas só no caso de n ser ímpar.

Definição 1.4 *Diremos que L é o n-ésimo corpo ciclotômico se L é resultante da adjunção de $\mathbb{Q}$ e uma raiz primitiva n-ésima da unidade, $L=\mathbb{Q}(\zeta_n)$.*

O isomorfismo do grupo $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+\right)$ sobre $U_{(n)}$, definido por $a+n\mathbb{Z} \rightsquigarrow \zeta^a$

induz uma bijeção entre o grupo das unidades do anel $\frac{\mathbb{Z}}{n\mathbb{Z}}$ e $P_{(n)}$.

Daí o grau $[L:K]$, igual à ordem de $Aut(L/K)$, é um divisor de $\varphi(n)$, onde K é um corpo intermediário entre L e $\mathbb{Q}$.

Teorema 1.5 *Seja $L=K(\zeta)$, sendo $\zeta \in \mathbb{C}$ uma raiz primitiva n-ésima da unidade. Então L é uma extensão galoisiana de K, cujo grupo de Galois $Aut(L/K)$ é canonicamente isomorfo a um subgrupo de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$. Em particular, $Aut(L/K)$ é um grupo abeliano e sua ordem divide $\varphi(n)$.*

No caso em que $K = \mathbb{Q}$, vale o seguinte:

Teorema 1.6 *Seja $\zeta \in \mathbb{C}$ uma raiz primitiva n-ésima da unidade. Então $L = \mathbb{Q}(\zeta)$ é uma extensão galoisiana de $\mathbb{Q}$, cujo grupo de Galois $Aut(L/\mathbb{Q})$ é canonicamente isomorfo a $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$, e portanto abeliano de ordem $\varphi(n)$.*

Assim, concluimos que além de $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +) \simeq U_{(n)}$, temos o isomorfismo $Aut(L/\mathbb{Q}) \simeq (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$.

Obviamente $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ é abeliano, mas nem sempre é cíclico.
Prova-se que $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ será cíclico se, e somente se $n = 2, 4, p^r$ ou $2p^r$, para p primo ímpar, veja [Rib] cap. 3 Ex.1.

Considere o corpo L, tal que $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$, com $[L : \mathbb{Q}] < \infty$.
$U_n(L) = \{\zeta \in L \,; \zeta^n = 1\}$ o conjunto das raízes em L do polinômio $x^n - 1$.
$P_n(L) = \{\zeta \in L \,; o(\zeta) = n\}$ o conjunto das raízes primitivas n-ésimas da unidade em L.

O grupo de todas as raízes da unidade em $L, U(L)$, que é a união dos grupos $U_n(L)$, onde $n \in \mathbb{N} \setminus \{0\}$, é finito e coincide com o subgrupo de torção de L^*, isto é,

$$|U(L)| = |\bigcup_{n\geq 1} U_n(L)| = |T(L^*)| = |\{\alpha \in I_L; \quad |\sigma_1(\alpha)| = \cdots = |\sigma_n(\alpha)| = 1\}| < \infty,$$

onde $\sigma_1, \ldots, \sigma_n$ são isomorfismos de L em $\mathbb{C}$.

Vamos determinar sua ordem no caso do n-ésimo corpo ciclotômico.

Seja $\zeta \in \mathbb{C}$ uma raiz primitiva n-ésima da unidade e $L = \mathbb{Q}(\zeta)$ o n-ésimo corpo ciclotômico. Então $U(L)$ tem ordem n, se n for par ou $U(L)$ tem ordem $2n$, se n for ímpar.

Escrevendo $\mathcal{T}$ e $\mathcal{N}$ no lugar de $\mathcal{T}_{L/\mathbb{Q}}$ e $\mathcal{N}_{L/\mathbb{Q}}$, temos para $j = 1, 2, \ldots, p-1$ que

Proposição 1.7 *Sejam ζ uma raiz primitiva p-ésima da unidade, e p é um número primo. Temos que;*

$$\begin{array}{lll} \mathcal{T}(\zeta^j) = -1 & \mathcal{T}(\zeta^j - 1) = -p & \mathcal{T}(1 - \zeta^j) = p \\ \mathcal{N}(\zeta^j) = 1 & \mathcal{N}(\zeta^j - 1) = p & \mathcal{N}(1 - \zeta^j) = p \ , \end{array}$$

A seguir estudaremos o anel I_L dos inteiros algébricos do corpo ciclotômico L, restringindo-nos, entretanto, ao caso em que n é um primo ímpar.

Sendo $L = \mathbb{Q}(\zeta)$, onde, ζ é uma raiz primitiva p-ésima da unidade, temos que $[L : \mathbb{Q}] = p-1$ e $1, \zeta, \ldots, \zeta^{p-2}$ formam uma base da extensão L de $\mathbb{Q}$ e que $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ são as raízes do p-ésimo polinômio ciclotômico $\Phi_p = x^{p-1} + \cdots + x + 1$.

O grupo de Galois $Aut(L/\mathbb{Q})$ consiste dos $p-1$ automorfismo $\sigma_1, \sigma_2, \ldots, \sigma_{p-1}$, sendo σ_j univocamente determinado por $\sigma_j(\zeta) = \zeta^j, \;\; j = 1, 2, \ldots, p-1$, em particular σ_1 é a identidade de L.

Podemos então demonstrar que o $\mathbb{Z}$-módulo I_L é livre.

Teorema 1.8 *$1, \zeta, \ldots, \zeta^{p-2}$ formam uma base do $\mathbb{Z}$-módulo I_L.*

Prova.

$1, \zeta, \ldots, \zeta^{p-2}$ são linearmente independentes sobre $\mathbb{Z}$, pois o são sobre $\mathbb{Q}$. Obviamente $\mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{p-2} \subseteq I_L$. Portanto basta provar $\supseteq$.

Seja $\alpha \in I_L$, isto é $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, com $a_0, a_1, \ldots, a_{p-2} \in \mathbb{Q}$.

Mostraremos primeiro que $a_0 \in \mathbb{Z}$. Note que

$$\begin{aligned}\alpha(1-\zeta) &= a_0(1-\zeta) + a_1\zeta(1-\zeta) + \cdots + a_{p-2}\zeta^{p-2}(1-\zeta) \\ &= a_0(1-\zeta) + a_1(\zeta - \zeta^2) + \cdots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1}) \\ &= a_0(1-\zeta) + \sum_{j=1}^{p-2} a_j(\zeta^j - \zeta^{j+1}) \qquad \text{aplica} \qquad \mathcal{T}_{L/\mathbb{Q}} = \mathcal{T}\ .\end{aligned}$$

$$\mathcal{T}(\alpha(1-\zeta)) = \mathcal{T}(a_0(1-\zeta)) + \mathcal{T}(\sum_{j=1}^{p-2} a_j(\zeta^j - \zeta^{j+1})).$$

Note que

$$\mathcal{T}(\sum_{j=1}^{p-2} a_j(\zeta^j - \zeta^{j+1})) = \sum_{j=1}^{p-2} \mathcal{T}(a_j(\zeta^j - \zeta^{j+1})) = \sum_{j=1}^{p-2} a_j\mathcal{T}(\zeta^j - \zeta^{j+1})$$

e que $\mathcal{T}(\zeta^j - \zeta^{j+1}) = \mathcal{T}(\zeta^j) - \mathcal{T}(\zeta^{j+1}) = -1 - (-1) = 0$, ou seja,

$$\mathcal{T}(\alpha(1-\zeta)) = \mathcal{T}(a_0(1-\zeta))$$

e

$$\mathcal{T}(\alpha(1-\zeta)) = a_0\mathcal{T}(1-\zeta) \stackrel{p/1.7}{=} a_0 p. \ . \tag{1.1}$$

Por outro lado, temos que

$$\mathcal{T}(\alpha(1-\zeta)) = \sum_{j=1}^{p-1} \sigma_j(\alpha(1-\zeta)), \quad \text{def. traço}$$

$$\sigma_j(\alpha(1-\zeta)) = \sigma_j(\alpha - \alpha\zeta) = \sigma_j(\alpha) - \sigma_j(\alpha\zeta) = \sigma_j(\alpha) - \sigma_j(\alpha)\sigma_j(\zeta)$$

$$= \sigma_j(\alpha)(1-\zeta^j) \Rightarrow \mathcal{T}(\alpha(1-\zeta)) = \sum_{j=1}^{p-1} \sigma_j(\alpha)(1-\zeta^j) \tag{1.2}$$

De (1.1) e (1.2)

$$pa_0 = \sum_{j=1}^{p-1} \sigma_j(\alpha)(1-\zeta^j) \in (1-\zeta)I_L \cap \mathbb{Z} = p\mathbb{Z} \Rightarrow a_0 \in \mathbb{Z}.$$

Supondo por indução que $a_1, \ldots, a_j \in \mathbb{Z}$, para algum $j \in \{1, 2, \ldots, p-2\}$, mostraremos que $a_j \in \mathbb{Z}$. De fato, multiplicando α por ζ^{p-j}, obtemos que

$$\alpha\zeta^{p-j} = a_j + a_{j+1}\zeta + a_{j+2}\zeta^2 + \cdots + a_{p-2}\zeta^{p-2-j} + a_0\zeta^{p-j} + a_1\zeta^{p-j+1} + \cdots + a_{j-1}\zeta^{p-1}.$$

Seja o p-ésimo polinômio ciclotômico $\Phi_p = x^{p-1} + \cdots + x + 1$ cujas raízes são as $p-1$ raízes primitivas p-ésimas da unidade, logo $\zeta_p = \zeta$ é uma delas,

assim $1 + \zeta + \zeta^2 + \cdots + \zeta^{p-2} + \zeta^{p-1} = 0 \Rightarrow \zeta^{p-1} = -1 - \zeta - \zeta^2 - \cdots - \zeta^{p-2}$ e

$\alpha\zeta^{p-j} = a_j + a_{j+1}\zeta + \cdots + a_{p-2}\zeta^{p-2-j} + a_0\zeta^{p-j} + a_1\zeta^{p-j+1} + \cdots + a_{j-1}(-1-\zeta-\zeta^2-\cdots-\zeta^{p-2})$

$\alpha\zeta^{p-j} = (a_j - a_{j-1}) + (a_{j+1} - a_{j-1})\zeta + (a_{j+2} - a_{j-1})\zeta^2 + \cdots + (a_{j+p-3} - a_{j-1})\zeta^{p-3} +$

$(a_{j+p-2} - a_{j-1})\zeta^{p-2}$, com $b_i = (a_{j+i} - a_{j-1}) \in \mathbb{Q}$ e $i \in \{1, 2, \ldots, p-3, p-2\}$

e como $\alpha\zeta^{p-j} \in I_L$, resulta que $a_j - a_{j-1} \in \mathbb{Z}$.

Portanto, $a_j = (a_{j+i} - a_{j-1}) + a_{j+1} \in \mathbb{Z}$, daí concluimos que $a_1, \ldots, a_{p-2} \in \mathbb{Z}$,

logo $\alpha \in \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{p-2} \Rightarrow I_L \subseteq \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{p-2}$ ■

Vimos assim que o anel dos inteiros de $\mathbb{Q}(\zeta)$ é $\mathbb{Z}[\zeta]$ e um resultado devido a Krummer afirma que toda unidade desse anel é o produto de um inteiro racional não-nulo com uma potência de ζ.

Mencionamos sem demonstração que o teorema 1.8 se generaliza ao n-ésimo corpo ciclotômico, para qualquer $n > 1$. De fato, este corpo tem $1, \zeta, \ldots, \zeta^{\varphi(n)-1}$ como base (veremos mais adiante como base integral), sendo ζ uma raiz primitiva n-ésima da unidade.

Proposição 1.9 *Seja $L = \mathbb{Q}(\zeta)$, com ζ uma raiz primitiva n-ésima da unidade*

a) $\alpha = \zeta + \zeta^{-1}$ e $K = \mathbb{Q}(\alpha)$ é o subcorpo maximal real de L;

b) O anel dos inteiros algébricos de K é $\mathbb{Z}[\alpha]$;

c) $1, \alpha, \ldots, \alpha^{\frac{\varphi(n)}{2}-1}$ formam uma base de K.

O seguinte teorema diz respeito à unicidade do subcorpo intermediário K.

Teorema 1.10 *Sejam p um número primo e $\zeta \in \mathbb{C}$ uma raiz primitiva p-ésima da unidade, tal que $L = \mathbb{Q}(\zeta)$ é o corpo de decomposição de $x^p - 1 \in \mathbb{Q}[x]$. Além disso, seja $\bar{g} = [g]_p$ uma raiz primitiva mod.p, isto é, $\bar{g}$ é um gerador do grupo multiplicativo $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$. Então*

a) O grau da extensão L de $\mathbb{Q}$ é $n = p-1$, e os elementos ζ^{g^i}, $i = 0, 1, \ldots, p-2$ formam uma base de L sobre $\mathbb{Q}$;

b) O grupo de Galois $Gal(L/\mathbb{Q})$ é gerado pelo automorfismo de L, dado por $\sigma(\zeta) = \zeta^g$, este automorfismo satisfaz, $\sigma(\zeta^{g^i}) = \zeta^{g^{i+1}}$ e $\sigma^k(\zeta^{g^i}) = \zeta^{g^{i+k}}$, para todo i,k onde esses índices devem ser lido mod.n;

c) Seja d um divisor de n e seja $e = \frac{n}{d}$, então existe um único corpo intermediário K_d, tal que $[K_d : \mathbb{Q}] = d$ e este corpo é dado por $K_d = \mathbb{Q}(\omega_0) = \cdots = \mathbb{Q}(\omega_{d-1})$, onde $\omega_k = \zeta^{g^k} + \zeta^{g^{k+d}} + \zeta^{g^{k+2d}} + \cdots + \zeta^{g^{k+(e-1)d}}$ é a soma dos ζ^{g^i}, com $i \equiv k(mod.d)$. O número de ω_k é chamado de e-período de grau de L sobre $\mathbb{Q}$, pois cada ω_k consiste exatamente de e somas.

Tal resultado, a unicidade do grau do corpo intermediário K de uma extensão ciclotômica p-ésima de $\mathbb{Q}$, viabilizará o cálculo do discriminante mais adiante.

1.3 Corpos de Números abelianos

Um resultado fundamental envolvendo corpos ciclotômicos e o conceito de corpos de números abelianos, devido a Kronecker e Weber, é o seguinte:

Teorema 1.11 *Seja K uma extensão finita e abeliana dos racionais (isto é, galoisiana com grupo de Galois abeliano). Então K está contido em algum corpo ciclotômico.*

A importância desse resultado reside no fato de que se o corpo K for abeliano podemos aplicar o teorema de Hasse para calcular o discriminante absoluto de K.

1.4 Bases Integrais

Todo corpo de números K possui uma base integral. Ou equivalentemente, seu anel dos inteiros algébricos I_K é um $\mathbb{Z}$-módulo livre. Isso pode ser provado juntando a proposição 1.12 com os teoremas 1.25 , 1.8 e A.2 , e com um sistema de imersões desses $\mathbb{Z}$-módulos livres no $\mathbb{Q}$-espaço vetorial.

Um sistema $(\alpha_1, \ldots, \alpha_n)$ de inteiros algébricos formará uma base da extensão K de $\mathbb{Q}$ se o discriminante desse sistema, além de ser não-nulo, não for divisível por nenhum quadrado $1 \neq c^2 \in \mathbb{Z}$, e tal discriminante terá o menor valor absoluto dentre todos dos sistemas de I_K^n.

Qualquer uma das bases do $\mathbb{Z}$-módulo I_K é chamada base integral de K.

Uma base integral de K é também uma base de K sobre $\mathbb{Q}$ como espaço vetorial já que tem $[K : \mathbb{Q}]$ elementos linearmente independentes.

No entanto, a recíproca não é verdadeira, isto é, nem toda base de K sobre $\mathbb{Q}$, como espaço vetorial, contida em I_K, é uma base integral.

Por exemplo, no caso do corpo de números $K = \mathbb{Q}(\sqrt{13})$,temos que $\{1, \sqrt{13}\}$ é uma base de $\mathbb{Q}(\sqrt{13})$ sobre $\mathbb{Q}$ formada por elementos inteiros algébricos, entretanto, não é uma base integral, pois o discriminante da dupla $(1, \sqrt{13})$, pela observação 1.26, é diferente do discriminante de K. Uma base integral de K, neste caso é $\left\{1, \frac{1+\sqrt{13}}{2}\right\}$.

A seguinte proposição afirma ser livre os submódulos de um $\mathbb{Z}$-módulo livre.

Proposição 1.12 *Seja M um $\mathbb{Z}$-módulo livre de posto n, e N um submódulo de M de posto $q \leq n$. Então;*

a) N também é um $\mathbb{Z}$-módulo livre.

b) Existem uma base $\{\beta_1, \ldots, \beta_n\}$ de M e elementos $a_1, \ldots, a_q \in \mathbb{Z}\backslash\{0\}$, com $a_1|a_2|\ldots|a_q$, tais que $a_1\beta_1, a_2\beta_2, \ldots, a_q\beta_q$ formam uma base de N.

c) Chamando $\{\varepsilon_1, \ldots, \varepsilon_q\}$ de base de N, e os inteiros $r_i \in a_i\mathbb{Z}, i = 1, \ldots, q$ e $r_{q+1}, \ldots, r_n \in \mathbb{Z}$ temos que os isomorfismos

$$\prod_{i=1}^{n} \mathbb{Z}_i \longrightarrow M, \text{ dado por } (r_1, r_2, \ldots, r_n) \rightsquigarrow (r_1\beta_1 + r_2\beta_2 + \cdots + r_n\beta_n) \text{ e}$$

$$\prod_{i=1}^{q} \mathbb{Z}_i \longrightarrow N, \text{ dado por } (r_1, \ldots, r_q) \rightsquigarrow (r_1\varepsilon_1 + \cdots + r_q\varepsilon_q)$$

induzem o isomorfismo $\frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_q\mathbb{Z}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n-q} \longrightarrow \frac{M}{N}$, daí uma classe $\bar{x} \in \frac{M}{N}$ se escreve na forma $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_q, x_{q+1}, \ldots, x_n)$

Proposição 1.13 *Seja M um $\mathbb{Z}$-módulo gerado por n elementos, $M = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$. Então existem $r, s \in \mathbb{N}$, com $r + s \leq n$ e elementos $a_1, \ldots, a_r \in \mathbb{Z}\backslash\{-1, 0, 1\}$, tais que $a_1|a_2|\ldots|a_r$ e M seja isomorfo ao $\mathbb{Z}$-módulo $\frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_r\mathbb{Z}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{s}$*

Proposição 1.14 *Seja K uma extensão finita de $\mathbb{Q}$ de grau n.*
Então:
a) O $\mathbb{Z}$-módulo I_K tem posto n.
b)Para todo anel S entre K e $\mathbb{Z}$, as seguintes condições são equivalentes;
i)$S \subseteq I_K$
ii)S é um $\mathbb{Z}$-módulo livre de posto $q \leq n$
iii)S é um $\mathbb{Z}$-módulo F.G.
No caso em que $K = Q(S)$, S é um $\mathbb{Z}$-módulo livre de posto n.

Prova. a) Pelo teorema 1.25, I_K está entre dois $\mathbb{Z}$-módulos livres de posto n, portanto tem posto n

b) *i)* $\Rightarrow$ *ii)*
Ainda por 1.25, S é um submódulo de um $\mathbb{Z}$-módulo livre de posto n, portanto, a afirmação resulta do item a da proposição 1.12, S também é um $\mathbb{Z}$-módulo livre de posto $q \leq n$.

ii) $\Rightarrow$ *iii)* imediato.

iii) $\Rightarrow$ *i)* como S é um $\mathbb{Z}$-módulo F.G. e $S \subset K \Rightarrow S \subseteq I_K$, pelo corolário A.26
■

Proposição 1.15 *Seja $[K : \mathbb{Q}] = n$. Para qualquer subanel S de K, as seguintes condições são equivalentes;*

i)$S \subseteq I_K$ *e* $K = Q(S)$

ii) S *é um* $\mathbb{Z}$*-módulo livre de posto* n*.*

Os subaneis S de I_K que satisfazem as condições equivalentes da prop. 1.15, são chamados as "ordens"de K e I_K de "ordem máxima"de K.

Entre as ordens de K distingüem-se os anéis $\mathbb{Z}[\alpha]$, onde $\alpha \in I_K$ é um elemento primitivo da extensão K de $\mathbb{Q}$.

1.5 Discriminantes

O principal invariante dos corpos de números algébricos é assim definido:

Definição 1.16 *Seja* K *uma extensão finita de grau* n *do corpo dos racionais. Para qualquer* n*-upla* $(\alpha_1, \ldots, \alpha_n) \in K^n$*, o Discriminante do Sistema* $(\alpha_1, \ldots, \alpha_n)$ *é o elemento de* $\mathbb{Q}$ *dado por*

$$disc\ _{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = det(\mathcal{T}_{K/\mathbb{Q}}(\alpha_i\alpha_j)) \in \mathbb{Q}, com \quad i, j \in \{1, 2, \ldots, n\}.$$

Observação 1.17 *Escrevendo* $\mathcal{T}$ *no lugar de* $\mathcal{T}_{K/\mathbb{Q}}$*,*

$$a\ matriz \begin{pmatrix} \mathcal{T}(\alpha_1\alpha_1) & \mathcal{T}(\alpha_1\alpha_2) & \cdots & \mathcal{T}(\alpha_1\alpha_n) \\ \mathcal{T}(\alpha_2\alpha_1) & \mathcal{T}(\alpha_2\alpha_2) & \cdots & \mathcal{T}(\alpha_2\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \mathcal{T}(\alpha_n\alpha_1) & \mathcal{T}(\alpha_n\alpha_2) & \cdots & \mathcal{T}(\alpha_n\alpha_n) \end{pmatrix} é\ simétrica.$$

Observação 1.18 *Se a* n*-upla* $(\alpha_1, \ldots, \alpha_n)$ *for uma base integral da extensão* K *de* $\mathbb{Q}$*, o discriminante desse sistema é sempre não nulo. E tal discriminante é dito o discriminante do corpo* K*, denotado por* $disc(K)$*.*

Se um elemento $\gamma_i \in K$ é escrito como combinãção linear de $\alpha_j's \in K$, com $i, j \in \{1, 2, \ldots, n\}$, os discriminantes dos sistemas $(\gamma_1, \ldots, \gamma_n)$ e $(\alpha_1, \ldots, \alpha_n)$ diferem por um fator quadrático, ou melhor

Proposição 1.19 *Para* $i = 1, 2, \ldots, n$*, seja* $\gamma_i = \sum_{j=i}^{n} a_{ij}\alpha_j$*, onde* $a_{ij} \in \mathbb{Q}$*. Então*

$$disc\ _{K/\mathbb{Q}}(\gamma_1, \ldots, \gamma_n) = det^2(a_{ij}) disc\ _{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$$

Prova.

$$\begin{cases} \gamma_1 = a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n \\ \gamma_2 = a_{21}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \\ \gamma_n = a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + a_{nn}\alpha_n \end{cases}$$

de $\gamma_r = \sum_{i=1}^{n} a_{ri}\alpha_i$, $\gamma_s = \sum_{j=1}^{n} a_{sj}\alpha_j$, o produto $\gamma_r\gamma_s = \sum_{i=1}^{n} a_{ri}\alpha_i \sum_{j=1}^{n} a_{sj}\alpha_j = \sum_{i,j=1}^{n} a_{ri}\alpha_i a_{sj}\alpha_j$

daí $\mathcal{T}_{K/\mathbb{Q}}(\gamma_r\gamma_s) = \mathcal{T}_{K/\mathbb{Q}}(\sum_{i,j=1}^{n} a_{ri}\alpha_i a_{sj}\alpha_j) = \sum_{i,j=1}^{n} \mathcal{T}_{K|\mathbb{Q}}(a_{ri}\alpha_i a_{sj}\alpha_j) = \sum_{i,j=1}^{n} a_{ri}\mathcal{T}_{K/\mathbb{Q}}(\alpha_i\alpha_j)a_{js}$.
Agora fazendo variar r e s entre 1 e n, $1 \leq r, s \leq n$ temos desse somatório 2 matrizes

$(a_{ri}) = A$ e $(a_{js}) = A^t$, daí $\mathcal{T}_{K|\mathbb{Q}}(\gamma_r\gamma_s) = A\mathcal{T}_{K|\mathbb{Q}}(\alpha_i\alpha_j)A^t$

$$det(\mathcal{T}_{K/\mathbb{Q}}(\gamma_r\gamma_s)) = det(A\mathcal{T}_{K/\mathbb{Q}}(\alpha_i\alpha_j)A^t) = det(A)det(\mathcal{T}_{K/\mathbb{Q}}(\alpha_i\alpha_j))det(A^t) =$$

$$= det^2(A)det(\mathcal{T}_{K/\mathbb{Q}}(\alpha_i\alpha_j)),$$

fazendo $A = a_{ij}$, temos

$$disc\ _{K/\mathbb{Q}}(\gamma_1, \ldots, \gamma_n) = det^2(a_{ij})disc\ _{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n).$$

■

Da Proposição 1.19, concluímos que se $\gamma_1, \ldots, \gamma_n$ e $\alpha_1, \ldots, \alpha_n$ forem bases de $K/\mathbb{Q}$, então a matriz mudança de base (a_{ij}) é invertível, e portanto seu determinante é invertível, isto é, $det(a_{ij}) \neq 0$.

Sejam $\sigma_1, \ldots, \sigma_n$ n $\mathbb{Q}$-isomorfismos distintos de K em $\mathbb{C}$, então para quaisquer $\alpha_1, \ldots, \alpha_n \in K$ temos que:

Proposição 1.20 $disc\ _{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = det^2(\sigma_i(\alpha_j)_{1\ \leq\ i,j\ \leq\ n})$

Prova.

$$\mathcal{T}_{K/\mathbb{Q}}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

Sejam $A^t = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \end{pmatrix}$ e $A = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$,

então

$$A^tA = \begin{pmatrix} \sum_{i=1}^{n} \sigma_i(\alpha_1)\sigma_i(\alpha_1) & \sum_{i=1}^{n} \sigma_i(\alpha_1)\sigma_i(\alpha_2) & \cdots & \sum_{i=1}^{n} \sigma_i(\alpha_1)\sigma_i(\alpha_n) \\ \sum_{i=1}^{n} \sigma_i(\alpha_2)\sigma_i(\alpha_1) & \sum_{i=1}^{n} \sigma_i(\alpha_2)\sigma_i(\alpha_2) & \cdots & \sum_{i=1}^{n} \sigma_i(\alpha_2)\sigma_i(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{i=1}^{n} \sigma_i(\alpha_n)\sigma_i(\alpha_1) & \sum_{i=1}^{n} \sigma_i(\alpha_n)\sigma_i(\alpha_2) & \cdots & \sum_{i=1}^{n} \sigma_i(\alpha_n)\sigma_i(\alpha_n) \end{pmatrix},$$

ou seja, $A^tA = \begin{pmatrix} \mathcal{T}(\alpha_1\alpha_1) & \mathcal{T}(\alpha_1\alpha_2) & \cdots & \mathcal{T}(\alpha_1\alpha_n) \\ \mathcal{T}(\alpha_2\alpha_1) & \mathcal{T}(\alpha_2\alpha_2) & \cdots & \mathcal{T}(\alpha_2\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \mathcal{T}(\alpha_n\alpha_1) & \mathcal{T}(\alpha_n\alpha_2) & \cdots & \mathcal{T}(\alpha_n\alpha_n) \end{pmatrix}$ e portanto

$det(A^tA) = (det(A))^2 = det^2(\sigma_i(\alpha_j)) = det(\mathcal{T}(\alpha_i\alpha_j)) = disc\ _{K/\mathbb{Q}}(\alpha_1, \alpha_2, ..., \alpha_n)$ ■

Este resultado garante que o discriminante do corpo de números algébricos $K = \mathbb{Q}(\alpha)$ coincida com o discriminante do polinômio característico do elemento primitivo α em relação à extensão $K/\mathbb{Q}$, assim o discriminante do sistema $(1, \alpha, \ldots, \alpha^{n-1})$ e do polinômio $F_{\alpha,\ K/\mathbb{Q}}$ não diferem.

Proposição 1.21 *Para qualquer $\alpha \in K$, temos que*

$$disc\ _{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = disc(F_{\alpha,\ K/\mathbb{Q}}) = (-1)^{\binom{n}{2}}\mathcal{N}_{K/\mathbb{Q}}(F'_{\alpha,\ K/\mathbb{Q}}(\alpha))$$

Proposição 1.22 *Sejam $\beta_1, \ldots, \beta_n \in K$. Teremos que $disc_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) \neq 0$ se, e somente se $\beta_1, \ldots, \beta_n$ formarem uma base da extensão K de $\mathbb{Q}$.*

Usando 1.22, mostra-se que toda base da extensão K de $\mathbb{Q}$ possui uma base dual, e isto será consequência do seguinte:

Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de $K/\mathbb{Q}$, então existe um único elemento $\alpha \in K$, tal que $\mathcal{T}_{K/\mathbb{Q}}(\alpha\beta_i) \in \mathbb{Q}$, para $i = 1, 2, \ldots, n$.

Usaremos este fato para mostrar que cada base $\{\beta_1, \ldots, \beta_n\}$ de $K/\mathbb{Q}$ corresponde a uma outra base $\{\beta'_1, \ldots, \beta'_n\}$ também de $K/\mathbb{Q}$, tal que $\mathcal{T}_{K/\mathbb{Q}}(\beta_j\beta'_i) = \delta_{ij}$,
justificando por que todo elemento $\alpha \in K$ se escreve univocamente como sendo

$$\alpha = \sum_{i=1}^{n} \mathcal{T}_{K/\mathbb{Q}}(\alpha\beta_i)\beta'_i \quad ou \quad \alpha = \sum_{i=1}^{n} \mathcal{T}_{K/\mathbb{Q}}(\alpha\beta'_i)\beta_i.$$

Assim $\{\beta'_1, \ldots, \beta'_n\}$ é a base dual de $\{\beta_1, \ldots, \beta_n\}$ e reciprocamente.

Lema 1.23 *Suponhamos que $\{\beta_1, \ldots, \beta_n\}$ seja uma base da extensão K de $\mathbb{Q}$. Para quaisquer $c_1, \ldots, c_n \in \mathbb{Q}$, existe um único $\alpha \in K$, tal que $\mathcal{T}_{K/\mathbb{Q}}(\beta_i\alpha) = c_i, \quad i = 1, 2, \ldots, n$*

Proposição 1.24 *Para cada base $\{\beta_1, \ldots, \beta_n\}$ da extensão K de $\mathbb{Q}$, existe uma única base $\{\beta'_1, \ldots, \beta'_n\}$ desta extensão, tal que $\mathcal{T}_{K/\mathbb{Q}}(\beta_i\beta'_j) = \delta_{ij}, \quad i, j \in \{1, 2, \ldots, n\}$.*

$$\mathcal{T}_{K|\mathbb{Q}}(\beta_i\beta'_j) = \delta_{ij} \Leftrightarrow \sum_{i,j=1}^{n} \sigma_i(\beta)\sigma_j(\beta') = 0\ ou\ 1$$

Observamos que uma base $\beta_1, \ldots, \beta_n$ deste tipo pode ser obtida multiplicando uma base arbitrária por um certo elemento $t \in \mathbb{Z} \setminus \{0\}$ eliminando denominadores, uma vez que, pelo teorema A.29 $K = Q(I_K)$.

Tal base é dita dual, visto que existem, pelo lema 1.23, $\mathcal{T}_{K/\mathbb{Q}}(\beta_i\alpha) \in \mathbb{Q}$, tais que qualquer $\alpha \in K$, pode ser escrito univocamente na forma

$$\alpha = \mathcal{T}_{K/\mathbb{Q}}(\beta_1\alpha)\beta'_1 + \mathcal{T}_{K/\mathbb{Q}}(\beta_2\alpha)\beta'_2 + \cdots + \mathcal{T}_{K/\mathbb{Q}}(\beta_n\alpha)\beta'_n$$

O próximo teorema nos mostra que I_K, está entre dois $\mathbb{Z}$-módulos livres, M, M', sendo o primeiro gerado por uma base $\beta_1, \ldots, \beta_n \in I_K$ da extensão $K/\mathbb{Q}$ e o segundo por sua base dual $\beta'_1, \ldots, \beta'_n$.

Teorema 1.25 *Suponhamos que $\beta_1, \ldots, \beta_n \in I_K$ formem uma base da extensão K de $\mathbb{Q}$ e $\beta'_1, \ldots, \beta'_n$ sua base dual. Então temos que $M \subseteq I_K \subseteq M'$, onde $M = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$ e $M' = \mathbb{Z}\beta'_1 + \cdots + \mathbb{Z}\beta'_n$ são $\mathbb{Z}$-módulo livres com bases $\beta_1, \ldots, \beta_n$ e $\beta'_1, \ldots, \beta'_n$ respectivamente.*

Prova. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de $K/\mathbb{Q}$, então $\beta_1, \ldots, \beta_n$ são LI sobre $\mathbb{Q}$, e consequentemente, $\beta_1, \ldots, \beta_n$ são LI sobre $\mathbb{Z}$, portanto $\beta_1, \ldots, \beta_n$ formam uma base para M.

$\{\beta'_1, \ldots, \beta'_n\}$ base dual de $\{\beta_1, \ldots, \beta_n\}$, isto é, $K = \mathbb{Q}\beta'_1 + \cdots + \mathbb{Q}\beta'_n \Rightarrow \beta'_1, \ldots, \beta'_n$ são LI sobre $\mathbb{Z}$. Portanto $\beta'_1, \ldots, \beta'_n$ formam uma base para M' e $M = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n \subseteq I_K$ evidentemente, pois $\beta_1, \ldots, \beta_n \in I_K$.
falta mostrar que, $I_K \subseteq M'$.

Pela proposição 1.24, todo $\alpha \in I_K \subseteq K$ se escreve como $\alpha = \sum_{j=1}^{n} \mathcal{T}(\beta_j \alpha)\beta'_j$.

Note que $\alpha, \beta_j \in I_K$, logo $\alpha\beta_j \in I_K$ e que $\mathcal{T}_{K/\mathbb{Q}}(\beta_j\alpha) \in \mathbb{Z}$ (p/ A.32 item a),

como $\alpha \in I_K$ e $\alpha = \sum_{j=1}^{n} \mathcal{T}(\beta_j \alpha)\beta'_j$ e $\alpha \in \mathbb{Z}\beta'_1 + \cdots + \mathbb{Z}\beta'_n$, isto é, $\alpha \in M'$ e portanto $I_K \subseteq M'$. ■

Para quaisquer $\alpha_1, \ldots, \alpha_n \in I_K$, o $disc_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. Particularmente, o discriminante de um corpo de números é um número inteiro racional.

Observação 1.26 *O ideal de $\mathbb{Z}$ gerado pelo conjunto $\{disc_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n);\ \alpha_1, \ldots, \alpha_n \in I_K\}$ é chamado de Ideal Discriminante de $I_K/\mathbb{Z}$ e é denotado por $\mathfrak{d}_{I_K/\mathbb{Z}}$. Agora se $\{\beta_1, \ldots, \beta_n\}$ for uma base do $\mathbb{Z}$-módulo I_K, isto é, $I_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$, o ideal discriminante é gerado por $disc_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$. Além disso, o discriminante de qualquer sistema $(\alpha_1, \ldots, \alpha_n) \in I_K^n$ satisfaz $disc(\alpha_1, \ldots, \alpha_n) = a^2 disc(K)$, com $a \in \mathbb{Z}$, e tal sistema será uma base de I_K se $a^2 = 1$.*

Afirmação 1.27 *Seja $S \subseteq I_K$. Para todas as bases $\beta_1, \ldots, \beta_n$ do $\mathbb{Z}$-módulo S, os discriminantes $disc_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$ coincidem.*

Em particular, os discriminantes de todas as bases integrais de K são iguais.

De fato, pela observação 1.26 o quociente dos discriminantes de duas bases quaisquer do $\mathbb{Z}$-módulo S é invertível e é um quadrado em $\mathbb{Z}$, logo igual a um.

$$\frac{\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)}{\mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)} = a^2 = 1 \Rightarrow \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$$

Os discriminantes das bases do anel dos inteiros algébricos são invariantes, independentemente da escolha dessas bases. Daí a afirmação que o discriminante de K é único.

Definição 1.28 *Dizemos que $t_\alpha \in \mathbb{N}$ é o índice de α, quando*

$$disc_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = t_\alpha^2 disc(K)$$

Proposição 1.29 *Seja $\alpha \in I_K$ um elemento primitivo de $K/\mathbb{Q}$, então $t_\alpha = (I_K : \mathbb{Z}[\alpha])$ é o índice de $\mathbb{Z}[\alpha]$ em I_K, considerados como grupos aditivos.*

Prova. Como $\mathbb{Z}[\alpha]$ é um submódulo do $\mathbb{Z}$-módulo livre I_K e ambos têm posto n, concluimos da prop. 1.12 que existe uma base $\varepsilon_1, \ldots, \varepsilon_n$ de I_K e elementos $t_1, \ldots, t_n \in \mathbb{Z}$ tais que $t_1\varepsilon_1, \ldots, t_n\varepsilon_n$ formam uma base de $\mathbb{Z}[\alpha]$

Pela proposicão 1.13, temos que;

$$\frac{I_K}{\mathbb{Z}[\alpha]} \cong \frac{\mathbb{Z}}{t_1\mathbb{Z}} \times \frac{\mathbb{Z}}{t_2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{t_n\mathbb{Z}}$$

$$\left|\frac{I_K}{\mathbb{Z}[\alpha]}\right| = \left|\frac{\mathbb{Z}}{t_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{t_n\mathbb{Z}}\right| = |t_1 \cdots t_n| \Leftrightarrow (I_K : \mathbb{Z}[\alpha]) = |t_1 \cdots t_n| = t_\alpha$$

Por outro lado concluimos da afirmação 1.27 que:

$$disc_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = disc_{K/\mathbb{Q}}(t_1\varepsilon_1, \ldots, t_n\varepsilon_n)$$

Observe que

$$\begin{cases} t_1\varepsilon_1 = t_1\varepsilon_1 + 0\varepsilon_1 + 0\varepsilon_2 \cdots + 0\varepsilon_n \\ t_2\varepsilon_2 = 0\varepsilon_1 + t_2\varepsilon_2 + \cdots + 0\varepsilon_n \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ t_n\varepsilon_n = 0\varepsilon_1 + 0\varepsilon_2 + \cdots + t_n\varepsilon_n \end{cases}$$

Da prop. 1.19 temos,

$$disc_{K/\mathbb{Q}}(t_1\varepsilon_1, \ldots, t_n\varepsilon_n) = \begin{vmatrix} t_1 & 0 & 0 & 0 \\ 0 & t_2 & 0 & 0 \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & t_n \end{vmatrix}^2 disc_{K/\mathbb{Q}}(\varepsilon_1, \ldots, \varepsilon_n)$$

$= (t_1 t_2 \cdots t_n)^2 disc_{K/\mathbb{Q}}(\varepsilon_1, \ldots, \varepsilon_n)$
$= |t_1 t_2 \cdots t_n|^2 d_K$, como $|t_1 \cdots t_n| = t_\alpha = (I_K : \mathbb{Z}[\alpha])$

$\Rightarrow disc_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha_{n-1}) = t_\alpha^2 d_K \Leftrightarrow t_\alpha = 1 \Rightarrow I_K = \mathbb{Z}[\alpha]$. ■

Concluimos de 1.29 que K possui uma base integral da forma $1, \alpha, \ldots, \alpha^{n-1}$ quando $t_\alpha = 1$.

Sempre que tivermos o anel I_K na forma $\mathbb{Z}[\alpha]$, teremos $\{1, \alpha, \ldots, \alpha^{n-1}\}$ como base integral de K. Nem sempre existe uma base integral da forma $1, \alpha, \ldots, \alpha^{n-1}$, onde α é o elemento primitivo.

Condição necessária e suficiente para a existência de uma base integral desse tipo serão dadas na seguinte proposição:

Proposição 1.30 *Seja* $[K:\mathbb{Q}]=n$. *Para qualquer* $\alpha \in I_K$, *as seguintes condições são equivalentes;*

i) $I_K = \mathbb{Z}[\alpha]$

ii) $1, \alpha, \ldots, \alpha^{n-1}$ *formam uma base integral de* K

iii) $d_K = \mathrm{disc}_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1})$

Sendo $\{\beta_1, \ldots, \beta_n\}$ uma base do $\mathbb{Z}$-módulo I_K, o discriminante do corpo K $\mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$ é também denotado por d_K.

Definição 1.31 *Chamamos de divisor não essencial de discriminante e denotamos por* d_{NED} *o número inteiro positivo*

$$d_{NED} = mdc\{t_\alpha \ ; \ \alpha \in I_K\}$$

O seguinte exemplo, devido a Dedekind, mostra que existe um corpo cúbico K, tal que $t_\alpha \neq 1 (I_K \neq \mathbb{Z}[\alpha])$, para todo elemento primitivo $\alpha \in I_K$ e mesmo sendo o *mdc* d_{NED} diferente de 1.

Exemplo 1.32 [*Rib*] *Seja* $K = \mathbb{Q}(\alpha)$, *onde* $P_{\alpha/\mathbb{Q}} = x^3 + x^2 - 2x + 8$.
Assim $1, \alpha, 4\alpha^{-1}$ *formam uma base integral de* K,
temos que $disc(K) = disc_{K/\mathbb{Q}}(1, \alpha, 4\alpha^{-1}) = -503$.
Por outro lado, $disc_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -2012 = 4disc(K) \Rightarrow t_\alpha = 2$
e para qualquer $\gamma \in I_K, disc_{K/\mathbb{Q}}(1, \gamma, \gamma^2)$ *é um multiplo de* $disc_{K/\mathbb{Q}}(1, \alpha, \alpha^2)$,
isto é, $disc_{K/\mathbb{Q}}(1, \gamma, \gamma^2) = 4m \cdot disc(K)$, $m \in \mathbb{Z}$
e portanto, $d_{NED} = 2$.

Com este exemplo vimos que nem todo corpo de números algébricos K possui uma base integral da forma $1, \alpha, \ldots, \alpha^{n-1}$. Ou seja, às vezes não é simples o processo de determinar o elemento primitivo α.

1.5.1 Discriminante de Corpos quadráticos

Proposição 1.33 *Seja* $K = \mathbb{Q}(\sqrt{d})$, *onde* $d \in \mathcal{D}$, *um corpo quadrático. Temos que* $disc(K) = d$, *se* $d \equiv 1 (mod.4)$ *ou* $disc(K) = 4d$, *se* $d \equiv 2$ *ou* $3 (mod.4)$

Prova. Para $\alpha = r + s\sqrt{d}$, com $r, s \in \mathbb{Q}$, temos que $\alpha^2 = r^2 + s^2 d + 2rs\sqrt{d}$;

$$\text{logo } \mathrm{disc}_{K/\mathbb{Q}}(1, \alpha) = det \begin{pmatrix} \mathcal{T}(1) & \mathcal{T}(\alpha) \\ \mathcal{T}(\alpha) & \mathcal{T}(\alpha^2) \end{pmatrix}$$

Tomando $1, \sqrt{d}$ como base da extensão $K/\mathbb{Q}$, temos;

$$\begin{array}{l} 1 \cdot 1 = a_{11} \cdot 1 + a_{12}\sqrt{d} = 1 \cdot 1 + 0 \cdot \sqrt{d} \Rightarrow a_{11} = 1 \text{ e } a_{12} = 0 \\ 1 \cdot \sqrt{d} = a_{21} \cdot 1 + a_{22}\sqrt{d} = 0 \cdot 1 + 1 \cdot \sqrt{d} \Rightarrow a_{21} = 0 \text{ e } a_{22} = 1 \end{array} \Rightarrow c = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$F_{1,K|\mathbb{Q}} = \begin{vmatrix} x-1 & 0 \\ 0 & x-1 \end{vmatrix} = (x-1)^2 = x^2 - 2x + 1 \Rightarrow \mathrm{T}(\alpha) = 2r \quad \text{e} \quad \mathrm{N}(\alpha) = r^2 - s^2 d$$

$$\alpha \cdot 1 = (r + s\sqrt{d})1 = r + s\sqrt{d} = a_{11} \cdot 1 + a_{12}\sqrt{d} \Rightarrow a_{11} = r \text{ e } a_{12} = s$$

$$\alpha \cdot \sqrt{d} = (r + s\sqrt{d})\sqrt{d} = sd + r\sqrt{d} = a_{21} \cdot 1 + a_{22}\sqrt{d} \Rightarrow a_{21} = sd \text{ e } a_{22} = r$$

$$\Rightarrow c = \begin{pmatrix} r & s \\ sd & r \end{pmatrix}$$

$$F_{\alpha,K/\mathbb{Q}} = \begin{vmatrix} x - r & -s \\ -sd & x - r \end{vmatrix} = x^2 - 2rx + r^2 - s^2 d \Rightarrow \mathcal{T}(\alpha) = 2r \text{ e } \mathcal{N}(\alpha) = r^2 - s^2 d$$

$$\alpha^2 \cdot 1 = (r^2 + s^2 d + 2rs\sqrt{d}) \cdot 1 = r^2 + s^2 d + 2rs\sqrt{d} = a_{11} \cdot 1 + a_{12} \cdot \sqrt{d}$$

$$\Rightarrow a_{11} = r^2 + s^2 d \text{ e } a_{12} = 2rs$$

$$\alpha^2 \cdot \sqrt{d} = (r^2 + s^2 d + 2rs\sqrt{d}) \cdot \sqrt{d} = 2rsd + (r^2 + s^2 d)\sqrt{d} = a_{21} \cdot 1 + a_{22} \cdot \sqrt{d}$$

$$\Rightarrow a_{21} = 2rsd \text{ e } a_{22} = r^2 + s^2 d$$

$$\Rightarrow c = \begin{pmatrix} r^2 + s^2 d & 2rs \\ 2rsd & r^2 + s^2 d \end{pmatrix} \Rightarrow F_{\alpha^2,K/\mathbb{Q}} = \begin{vmatrix} x - r^2 - s^2 d & -2rs \\ -2rsd & x - r^2 - s^2 d \end{vmatrix}$$

$$= x^2 - (2r^2 + 2s^2 d)x + x^4 - 2r^2 s^2 d + s^4 d^2$$

$$\Rightarrow \mathcal{T}(\alpha^2) = 2(r^2 + s^2 d) \text{ e } \mathcal{N}(\alpha^2) = r^4 - 2r^2 s^2 d + s^4 d^2$$

daí

$$\text{disc}_{K/\mathbb{Q}}(1, \alpha) = \begin{vmatrix} 2 & 2r \\ 2r & 2(r^2 + s^2 d) \end{vmatrix} = 4s^2 d$$

Em particular, temos $\text{disc}_{K/\mathbb{Q}}(1, \sqrt{d}) = 4d$, pois $\sqrt{d} = 0 \cdot 1 + 1 \cdot \sqrt{d} = r + s\sqrt{d} \Rightarrow s = 1$ e $\text{disc}_{K/\mathbb{Q}}\left(1, \dfrac{1 + \sqrt{d}}{2}\right) = d$, pois $\dfrac{1 + \sqrt{d}}{2} = \dfrac{1}{2} + \dfrac{1}{2}\sqrt{d} = r + s\sqrt{d} \Rightarrow s = \dfrac{1}{2}$ daí $4s^2 d = 4 \cdot \left(\dfrac{1}{2}\right)^2 d = 4 \cdot \dfrac{1}{4} d = d$.

Como $1, \sqrt{d}$ formam uma base integral de K no caso $d \equiv 2$ ou $3(mod.4)$ ou $1, \dfrac{1 + \sqrt{d}}{2}$ formam uma base integral de K no caso $d \equiv 1(mod.4)$, concluímos que

$$\text{disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d, \text{ se } d \equiv 1(mod.4) \\ 4d, \text{ se } d \equiv 2 \text{ ou } 3(mod.4) \end{cases}$$

■

1.5.2 O Condutor dos CQ's em Função do Discriminante

Diremos que m é o condutor do corpo K, se m é o menor inteiro, tal que $K \subset \mathbb{Q}(\zeta_m)$. Com relação ao inteiro livre de quadrados d, se um primo p divide d, então $d = pd'$, com $(p, d') = 1$. O menor corpo ciclotômico contendo $\mathbb{Q}(\sqrt{d})$ é;

a) $\mathbb{Q}(\zeta_{d'})$, se $d \equiv 1(mod.4)$

b) $\mathbb{Q}(\zeta_{4d'})$, se $d \equiv 3(mod.4)$

c) $\mathbb{Q}(\zeta_{8d'})$, se $d \equiv 2(mod.4)$

Se o discriminante de $\mathbb{Q}(\sqrt{d})$ for denotado por Δ, então para todo d, o menor corpo ciclotômico contendo $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta})$ é $\mathbb{Q}(\zeta_{|\Delta|})$.

1.5.3 Discriminante de Corpos Ciclotômicos

Proposição 1.34 *Seja $L = \mathbb{Q}(\zeta_p)$, sendo ζ_p uma raíz primitiva p-ésima da unidade, onde p é um número primo ímpar.*

Temos que $disc(L) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

Prova. Recordemos que $P_{\zeta_p/\mathbb{Q}} = F_{\zeta_p, L/\mathbb{Q}} = \Phi_p$ e que $\Phi_p(\zeta_p^j) = 0$, para $j =$

$1, 2, \ldots, p-1$ e que $1, \zeta_p, \ldots, \zeta_p^{p-2}$ formam uma base integral de L.

Temos por 1.21 que $disc_{L/\mathbb{Q}}(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{p-1}{2}} \mathcal{N}_{L/\mathbb{Q}}(\Phi_p'(\zeta_p))$.

$$\begin{pmatrix} p-1 \\ 2 \end{pmatrix} = \frac{(p-1)!}{2!(p-3)!} = \frac{(p-1)(p-2)}{2!} = \frac{p-1}{2}(p-2)$$

Note que $\frac{p-1}{2}(p-2)$ e $\frac{p-1}{2}$ têm a mesma paridade,

então $(-1)^{\binom{p-1}{2}} = (-1)^{\frac{p-1}{2}}$

Basta provar que $\mathcal{N}_{L/\mathbb{Q}}(\Phi_p'(\zeta_p)) = p^{p-2}$

Sabemos que $\Phi_p = \frac{x^p-1}{x-1} \Rightarrow (x^p - 1)' = ((x-1)\Phi_p)'$

$\Rightarrow px^{p-1} - 0 = (x-1)'\Phi_p + (x-1)\Phi_p' = \Phi_p + (x-1)\Phi_p' \Rightarrow$

$px^{p-1} = (x-1)\Phi_p' + \Phi_p$ aplicado em $\zeta_p \Rightarrow p\zeta_p^{p-1} = (\zeta_p - 1)\Phi_p'(\zeta_p) + \Phi_p(\zeta_p)$

aplicando $\mathcal{N}_{P/\mathbb{Q}}$ na igualdade $p\zeta_p^{p-1} = (\zeta_p - 1)\Phi_p'(\zeta_p)$, temos

$\mathcal{N}(p\zeta_p^{p-1}) = \mathcal{N}((\zeta_p - 1)\Phi_p'(\zeta_p)) \Rightarrow \mathcal{N}(p)\mathcal{N}(\zeta_p^{p-1}) = \mathcal{N}(\zeta_p - 1)\mathcal{N}(\Phi_p'(\zeta_p))$

Pela proposição 1.7, $\mathcal{N}(p) = p^{p-1}$, $\mathcal{N}(\zeta_p^{p-1}) = 1$ *e* $\mathcal{N}(\zeta_p - 1) = p$, daí

$$p^{p-1} \cdot 1 = p\mathcal{N}(\Phi_p'(\zeta_p)) \Rightarrow \mathcal{N}(\Phi_p'(\zeta_p)) = p^{p-2}$$

Portanto, $disc(\mathbb{Q}(\zeta_p)) = (-1)^{\frac{p-1}{2}} p^{p-2}$, onde p é um primo ímpar. ■

Capítulo 2

Teoria dos Caracteres

"Um conjunto se diz infinito se pode ser colocado em correspondência biunívoca com uma parte própria de si mesmo".

Richard Dedekind, séc. XIX

Sendo G um grupo abeliano finito, estudaremos neste capítulo um conjunto importante de homomorfismos: O grupo de caracteres, $Hom(G, \mathbb{C}^*)$. Tal grupo, também conhecido como dual de G, tem a mesma ordem de G.

O conjunto $\{\chi_1, \chi_2, \ldots, \chi_n\}$ de caracteres do grupo G são independentes, no sentido de que não existem $a_1, a_2, \ldots, a_n \in \mathbb{C}$, nem todos nulos, tais que $\sum_{i=1}^{n} a_i \chi_i(x) = 0$, para todo $x \in G$, formando portanto uma base para o $\mathbb{C}$-espaço vetorial, definido pelas operações

$$\chi_1 + \chi_2 : \ x \ \rightsquigarrow \ \chi_1(x) + \chi_2(x) \quad \text{e} \quad \alpha\chi : x \rightsquigarrow \alpha\chi(x), \quad \alpha \ \in \ \mathbb{C}.$$

Em consequência disso, todo subconjunto de automorfismos distintos de $Aut(G, \mathbb{C}^*)$ é também independente.

Veremos também que a estrutura de um grupo abeliano finito é determinado pelo fato de que ele pode ser representado como o produto direto de subgrupos cíclicos, e esta representação em geral não é única, mas as ordens dos subgrupos cíclicos, que são potências de primos, são univocamentes determinadas por G.

Essas ordens são chamadas de invariante do grupo abeliano finito G, e assim o produto de todos os invariantes de G é igual à ordem de G.

2.1 Caracteres de Grupos abelianos finitos

Definição 2.1 *Seja G um grupo abeliano finito.Chamamos de caracter do grupo G a um homomorfismo de G no grupo multiplicativo do corpo dos complexos*

$$\chi : G \to \mathbb{C}^*,$$

em outras palavras , um caracter de G é uma função de G em $\mathbb{C}^*$,
com $\chi(ab) = \chi(a)\chi(b)$, para todo $a, b \ \in \ G$.

Se o elemento $a \in G$ tiver ordem n, então $\chi(a)$ é uma raiz n-ésima da unidade. De fato,

$$\big(\chi(a)\big)^n = \chi(a^n) = \chi(e) = 1.$$

Daí a imagem $\chi(G)$ é um subgrupo do grupo multiplicativo das raízes da unidade contidas em $\mathbb{C}^*$.

$$\chi : G \to \chi(G) \leq \{\zeta \in \mathbb{C}^* \ ; \zeta^n = 1 \ e \ n \geq 1\} \subseteq \mathbb{C}$$

Exemplo 2.2 *Se n é um inteiro positivo e $\zeta \in \mathbb{C}$ uma raiz n-ésima da unidade ($\zeta^n = 1$), então $\chi : \mathbb{Z}_n \to \mathbb{C}^*$, dada por $\chi(\bar{a}) = \zeta^a$, $\forall \bar{a} \in \mathbb{Z}_n$ está bem definida e é um caracter de $\mathbb{Z}_n$.*

$\bar{a} \in \mathbb{Z}_p^*$ é um quadrado em $\mathbb{Z}_p^*$, se existe um $\bar{b} \in \mathbb{Z}_p^*$, tal que $\bar{b}^2 = \bar{a}$.

Exemplo 2.3 *Outro caracter muito usado é o símbolo de Legendre para o primo p.*

Seja p primo e seja $G = (\mathbb{Z}_p^*, \cdot)$, então a aplicação $\chi : G \to \mathbb{C}^*$, definida por

$$\chi(a) = \begin{cases} 1, & \text{se } \bar{a} \text{ é um quadrado em } \mathbb{Z}_p^* \\ -1, & \text{se } \bar{a} \text{ não é um quadrado em } \mathbb{Z}_p^* \end{cases}$$

é um caracter em G.

De fato,
Seja o corpo finito $\mathbb{F} = \mathbb{Z}_q$, onde $q = p^r$, para um p primo.
Então o grupo multiplicativo é cíclico, $\mathbb{F}^* = \langle g \rangle$.
a e b são quadrados em $\mathbb{F}^*$, $a = (g^m)^2$ e $b = (g^n)^2$
c e d não são quadrados, $c = g^{2m+1}$ e $d = g^{2n+1}$ $m, n \in \mathbb{N}$, daí;
$\chi(ab) = \chi(g^{2m}g^{2n}) = \chi((g^{m+n})^2) = 1 = 1 \cdot 1 = \chi(a)\chi(b)$
$\chi(cd) = \chi(g^{2m+1}g^{2n+1}) = \chi((g^{m+n+1})^2) = 1 = (-1)(-1) = \chi(c)\chi(d)$
$\chi(ad) = \chi(g^{2m}g^{2n+1}) = \chi(g^{2(m+n)+1}) = -1 = 1 \cdot (-1) = \chi(a)\chi(d)$.

Exemplo 2.4 *Seja $G = (\mathbb{R}, +)$, então para $\theta \in G$, a aplicação $\chi : G \to \mathbb{C}^*$ dada por $\chi(\theta) = e^{i\theta}$ é um caracter do grupo aditivo dos reais.*

Os caracteres de um grupo abeliano G formam um grupo multiplicativo. É o chamado dual de G e denotado por $\widehat{G}$.
$\widehat{G} = \{\chi : G \to \mathbb{C}^* \ ; \chi \text{ é homomorfismo }\}$ ou $\widehat{G} = Hom(G, \mathbb{C}^*)$ o conjunto de caracteres de G.

Se $\chi, \chi' \in \widehat{G}$, definimos $\chi\chi' : G \to \mathbb{C}^*$ por $\chi\chi'(a) = \chi(a)\chi'(a)$, para todo $a \in G$.

Temos $\chi(a)\chi'(a) \in \mathbb{C}^*$, o que implica $\chi\chi'$ ser um caracter de G

$$\cdot : \widehat{G} \times \widehat{G} \longrightarrow \widehat{G}$$

$$(\chi, \chi') \rightsquigarrow \chi\chi'$$

Temos, assim definida uma operação em $\widehat{G}$(multiplicação de G) e esta operação satisfaz as propriedades de um grupo abeliano, onde;

$\chi_0 : G \to \mathbb{C}^*$, dado por $\chi_0(a) = 1, \forall a \in G$, é o elemento neutro de $\widehat{G}$, e

$\bar{\chi} : G \to \mathbb{C}^*$, dado por $\bar{\chi}(a) = \chi(a^{-1}), \forall a \in G$, é o caracter inverso de χ.

$$De\ fato,\ \chi\bar{\chi}(a) = \chi(a)\bar{\chi}(a) = \chi(a)\chi(a^{-1}) = \chi(a)(\chi(a))^{-1} = \chi(a)\frac{1}{\chi(a)} = 1 \Rightarrow \chi\bar{\chi} = \chi_0,$$

e portanto $(\widehat{G}, \cdot)$ é também um grupo multiplicativo.

Obviamente, se H é um subgrupo de G e χ é um caracter de G, então a restrição de χ a H é um caracter de H.

$$\begin{array}{ccc} \chi : G & \longrightarrow & \chi(G) \\ \Big| & & \\ H & \longrightarrow & \chi(H) \end{array}$$

$\chi \in \widehat{G}$ e $H \leq G \Longrightarrow \chi|_H \in \widehat{H}$

Esta restrição será usada mais adiante, quando veremos o conceito de condutor de caracteres de Dirichlet.

Ordenando as ordens do grupo G, teremos m a maior delas, que chamamos de expoente de G. Então a ordem de qualquer elemento de G divide m, daí $\chi(a)$ é uma raiz m-ésima da unidade, qualquer que seja $a \in G$

$$m = exp(G) \Leftrightarrow m = \max\{o(a)\ \ ; a \in G\} \Rightarrow o(a)|m, \forall a \in G,$$

e portanto $\chi(a) \in U_{(m)}$.

Podemos então, definir um caracter de um grupo abeliano finito G como um homomorfismo de G no grupo multiplicativo das raízes m-ésimas da unidade, onde m é o expoente de G

$$\chi : G \xrightarrow{hom} U_{(m)} \subseteq \mathbb{C}^*,$$

onde $m = exp(G)$.

Teorema 2.5 *O número de caracteres de um grupo abeliano finito G é igual à ordem de G isto é, $|G| = |\widehat{G}|$.*

Prova.

De fato, G pode ser representado como produto de grupos cíclicos

$$G = \prod_{i=1}^{r} G_i$$

sendo $G_1 =< g_1 >, G_2 =< g_2 >, \ldots, G_r =< g_r >$, daí, todo elemento $g \in G$ pode ser representado de modo único, a menos da ordem , na forma $g = g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_r^{\alpha_r}$. E se χ é um caracter de G, $\chi(g) = \chi(g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_r^{\alpha_r}) = \chi(g_1)^{\alpha_1}\chi(g_2)^{\alpha_2} \cdots \chi(g_r)^{\alpha_r}$, temos que χ é um caracter de G e completamente determinado pelos valores de $\chi(g_1), \chi(g_2), \ldots, \chi(g_r)$.

Agora, se $o(g_1) = m_1, \quad o(g_2) = m_2, \ldots, o(g_r) = m_r$, então G tem ordem $m_1 m_2 \cdots m_r$ e

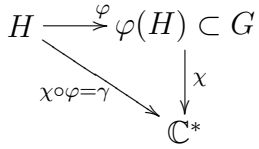
$$\begin{array}{ll} \chi(g_1), & \text{é uma raiz } m_1\text{-ésima da unidade;} \\ \chi(g_2), & \text{é uma raiz } m_2\text{-ésima da unidade;} \\ & \vdots \\ \chi(g_r), & \text{é uma raiz } m_r\text{-ésima da unidade,} \end{array}$$

então, temos

$$\begin{array}{lllll} m_1 \text{ possibilidades para } \chi_i(g_1) & \text{i.e} & m_1 \text{ caracteres} & \chi_i(g_1), & i = 1, 2, \ldots, m_1; \\ m_2 \text{ possibilidades para } \chi_i(g_2) & \text{i.e} & m_2 \text{ caracteres} & \chi_i(g_2), & i = 1, 2, \ldots, m_2; \\ & & \vdots & & \\ m_r \text{ possibilidades para } \chi_i(g_r) & \text{i.e} & m_r \text{ caracteres} & \chi_i(g_r), & i = 1, 2, \ldots, m_r, \end{array}$$

logo, temos $m_1 m_2 \cdots m_r$ caracteres em G e portanto $|G| = |\widehat{G}|$. ■

Dados dois grupos abelianos finitos e distintos, se $\varphi : H \longrightarrow G$ é um homomorfismo, então φ induz um homomorfismo $\gamma : \widehat{G} \to \widehat{H}$ dado pela sua composição com caracteres de G, conforme diagrama abaixo:



$\varphi : H \overset{hom}{\longrightarrow} G$ induz $\gamma : \widehat{G} \overset{hom}{\longrightarrow} \widehat{H}$, dado por $\gamma(\chi) = \chi \circ \varphi$.

O núcleo de γ consiste de todos os caracteres χ de $\widehat{G}$, tais que $\gamma(\chi) = \chi_0$.

Desta forma o núcleo de γ consiste de todos os caracteres de G cuja restrição à imagem de φ é o caracter trivial

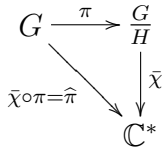
$$Ker\gamma = \{\chi \ \in \ \widehat{G};\ \chi|_{\varphi(H)} = \chi_0\}.$$

Em particular, se φ é a inclusão($\varphi = \iota \ \ e \ \ \gamma = \widehat{\iota}$), temos que H é um subgrupo de G, então $\widehat{\iota}(\chi)$ é a restrição de χ a H. Simbolicamente, temos

$$H \leq G \Rightarrow \widehat{\iota}(\chi) = \chi|_H.$$

Neste caso, o núcleo de $\widehat{\iota}$, será denotado por $H^{\perp}$.
Se $\pi : G \to \frac{G}{H}$ é um homomorfismo canônico, dado por $\pi(a) = aH, \forall a \in G$,
então o levantamento $\widehat{\pi} : \frac{\widehat{G}}{H} \to \widehat{G}$(homomorfismo induzido por π)
é tal que $\widehat{\pi}(\bar{\chi}) = \bar{\chi} \circ \pi = \chi$ e $\chi(a) = \bar{\chi} \circ \pi(a) = \bar{\chi}(\pi(a)) = \bar{\chi}(aH), \forall a \in G$,
então, $\chi(a) = 1, \forall a \in H$, o que significa que $\chi \in H^{\perp}$,

isso implica que a imagem de $\widehat{\pi}$ está contida no núcleo de $\widehat{\iota}$,
$\widehat{\pi}(\widehat{\frac{G}{H}}) \subseteq H^{\perp}$, conforme diagrama abaixo:



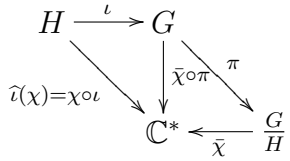
Observação 2.6 *Um resultado importante sobre caracteres é a propriedade que afirma existir caracteres que separam elementos de um grupo.*

Mais precisamente: Se $a, a' \in G$ e $a \neq a'$, então existe um caracter $\chi \in \widehat{G}$, tal que $\chi(a) \neq \chi(a')$.

Isso nos assegura que dado $\chi \in H^{\perp}$, temos $\chi \in \widehat{\pi}(\widehat{\frac{G}{H}})$, logo $H^{\perp} = \widehat{\pi}(\widehat{\frac{G}{H}})$

Concluimos que se $\{1\} \to H \xrightarrow{\iota} G \xrightarrow{\pi} \frac{G}{H} \to \{1\}$, é uma sequência exata de grupos abelianos finitos,

então a sequência $\{1\} \to \widehat{\frac{G}{H}} \xrightarrow{\widehat{\pi}} \widehat{G} \xrightarrow{\widehat{\iota}} \widehat{H} \to \{1\}$, também é exata.



Observação 2.7 *Olhando a parte do diagrama $H \xrightarrow{\iota} G \xrightarrow{\chi} \mathbb{C}^*$, podemos dizer que cada caracter $\chi \circ \iota$ de H pode ser estendido a $\frac{|G|}{|H|}$ caracteres χ de G, isto é, cada caracter χ de um subgrupo de G de ordem $\frac{|G|}{|H|}$ equivale a um caracter $\chi \circ \iota$ de H. Ou ainda, um caracter $\chi \circ \iota$ de H é a restrição de $\frac{|G|}{|H|}$ caracteres χ de G, isto é, cada caracter $\chi \circ \iota$ de H se indentifica com $\frac{|G|}{|H|}$ caracteres χ de G. Portanto a partir da extensão dos caracteres de um subgrupo podemos muitas vezes determinar parte dos caracteres do grupo.*

O seguinte teorema nos descreve, explicitamente, a obtenção dos caracteres de um grupo abeliano finito. Neste caso, em particular, consideraremos o grupo G cíclico.

Teorema 2.8 *Se G é um grupo cíclico de ordem n, então $G \cong \widehat{G}$.*

Prova.

Seja a um gerador de G e ζ uma raiz n-ésima primitiva da unidade,

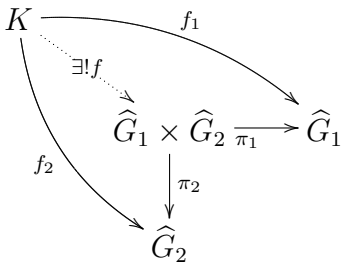
$$< a >= G \quad e \quad \zeta \in P_{(n)}$$

.

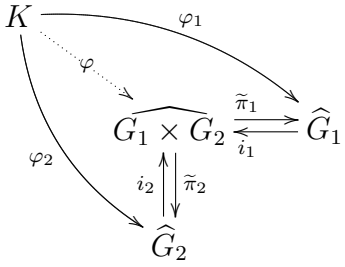
Seja $\chi : G \to \mathbb{C}^*$, dada por $\chi(a) = \zeta$.
Se $\chi^r(a^k) = \zeta^{rk}$, com $r, k \in \{1, 2, \ldots, n\}$, então os caracteres $\chi, \chi^2, \ldots, \chi^{n-1}, \chi^n = \chi_0$ são dois a dois distintos, e como $|\widehat{G}| = |G| = n$, temos $\widehat{G} = \{\chi_0, \chi, \chi^2, \ldots, \chi^{n-1}\}$ é cíclico de ordem n e gerado por χ. Logo, $G \cong \widehat{G}$ ■

Teorema 2.9 *Seja* $\theta : G \to \prod_{i=1}^{r} G_i$ *um isomorfismo de grupos, então* θ *induz um isomorfismo de grupos* $\widehat{\theta} : \widehat{G} \to \prod_{i=1}^{r} \widehat{G_i}$. *Ou seja,* $\widehat{\prod_{i=1}^{r} G_i} \cong \prod_{i=1}^{r} \widehat{G_i}$.

Prova. Considere as projeções π_1 e π_2, conforme diagrama.



A propriedede universal do produto direto nos assegura que para qualquer grupo K, existe um único homormorfismo f, que faz comutativo os diagramas componentes, isto é, $f_1 = \pi_1 \circ f$ e $f_2 = \pi_2 \circ f$.
Se demonstrarmos que existe um único homomorfismo φ de K em $\widehat{G_1 \times G_2}$ nas mesmas condições de f, então $\widehat{G_1 \times G_2}$ é isomorfo a $\widehat{G}_1 \times \widehat{G}_2$.
Considere as projeções $\widetilde{\pi}_1$,$\widetilde{\pi}_2$ e as inclusões i_1,i_2, conforme diagrama abaixo.



Sejam $\begin{array}{rccc} i_1: & \widehat{G}_1 & \longrightarrow & \widehat{G_1 \times G_2} \\ & \hat{g}_1 & \rightsquigarrow & (\hat{g}_1, e_2) \end{array}$, $\begin{array}{rccc} i_2: & \widehat{G}_2 & \longrightarrow & \widehat{G_1 \times G_2} \\ & \hat{g}_2 & \rightsquigarrow & (e_1, \hat{g}_2) \end{array}$
e $\varphi : K \longrightarrow \widehat{G_1 \times G_2}$,dada por $\varphi = (i_1 \circ \varphi_1)(i_2 \circ \varphi_2)$.

De $\widetilde{\pi}_1(\psi)(\hat{g}_1, \hat{g}_2) := \psi(\hat{g}_1, e_2)$,temos

$\widetilde{\pi}_1 \circ \varphi(k) = \widetilde{\pi}_1(\varphi(k)) = \widetilde{\pi}_1(i_1 \circ \varphi_1)(k)(i_2 \circ \varphi_2)(k) = \widetilde{\pi}_1(i_1(\varphi_1(k)))(i_2(\varphi_2(k))) = \varphi_1(k)e_1 = \varphi_1(k)$

e de $\widetilde{\pi}_2(\psi)(\hat{g}_1, \hat{g}_2) := \psi(e_1, \hat{g}_2)$, temos

$\widetilde{\pi}_2 \circ \varphi(k) = \widetilde{\pi}_2(\varphi(k)) = \widetilde{\pi}_2(i_1 \circ \varphi_1)(k)(i_2 \circ \varphi_2)(k) = \widetilde{\pi}_2(i_1(\varphi_1(k)))(i_2(\varphi_2(k))) = e_2\varphi_2(k) = \varphi_2(k)$,

logo

$$\widetilde{\pi}_1 \circ \varphi(k) = \varphi_1(k), \quad \forall \quad k \in K$$

e

$$\widetilde{\pi}_2 \circ \varphi(k) = \varphi_2(k), \quad \forall \quad k \in K.$$

Portanto $\widetilde{\pi_1} \circ \varphi = \varphi_1$ e $\widetilde{\pi_2} \circ \varphi = \varphi_2$, logo $\widehat{G}_1 \times \widehat{G}_2$ é isomorfo a $\widehat{G_1 \times G_2}$.

Por indução $\widehat{G}_1 \times \cdots \times \widehat{G}_n \cong \widehat{G_1 \times \cdots \times G_n}$ ■

Teorema 2.10 *Se G é um grupo abeliano finito, então $G \cong \widehat{G}$.*

Prova. Como todo grupo abeliano finito é isomorfo ao produto cartesiano de um número finito de grupos cíclicos (teo. fund. dos grupos abel. F.G.), temos que $G \cong G_1 \times G_2 \times \cdots \times G_r$, onde cada G_i é um grupo cíclico finito. Pelo teorema 2.8 $G_i \cong \widehat{G}_i$ e pelo teorema 2.9 $G \cong G_1 \times G_2$ induz um isomorfismo $\widehat{G} \cong \widehat{G_1} \times \widehat{G_2}$, daí $G \cong G_1 \times \cdots \times G_r \cong \widehat{G_1} \times \cdots \times \widehat{G_r} \cong \widehat{G}$ ■

Corolário 2.11 *Se G é um grupo abeliano finito, então $G \cong \widehat{\widehat{G}}$.*

2.2 Caracteres de Dirichlet, Condutores

Nesta seção veremos o tipo mais importante de caracter para o nosso estudo, os caracteres de Dirichlet das unidades do anel multiplicativo das classes de resto módulo n, que são conhecidos também como caracteres numéricos.

Conheceremos também o condutor, um número inteiro especial que é o menor divisor de n que satisfaz certas condições.

Definição 2.12 *Chamamos de Caracter de Dirichlet a um homomorfismo do grupo multiplicativo das unidades do anel $\frac{\mathbb{Z}}{n\mathbb{Z}}$ no grupo multiplicativo do corpo dos complexos.*

Se $\chi : (\frac{\mathbb{Z}}{m\mathbb{Z}})^* \to \mathbb{C}^*$ é um caracter de Dirichlet e m divide n, então χ induz um homomorfismo $(\frac{\mathbb{Z}}{n\mathbb{Z}})^* \to \mathbb{C}^*$ pela composição com a aplicação natural de $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ em $(\frac{\mathbb{Z}}{m\mathbb{Z}})^*$. Isto é,

$m \mid n \Rightarrow m\mathbb{Z} \supseteq n\mathbb{Z}$, logo temos $\pi : \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{\mathbb{Z}}{m\mathbb{Z}}$, dada por $[a]_n \rightsquigarrow [a]_m$

$[a]_n \in U(\mathbb{Z}_n) \Leftrightarrow (a,n) = 1 \Rightarrow (a,m) = 1 \Rightarrow [a]_m \in U(\mathbb{Z}_m)$, ou seja, $\pi([a]_n) \in U(\mathbb{Z}_m)$

portanto π induz ρ

$$\rho : (\frac{\mathbb{Z}}{n\mathbb{Z}})^* \to (\frac{\mathbb{Z}}{m\mathbb{Z}})^* \qquad e \qquad Ker\rho = \{\bar{a} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^* \,;(a,n) = 1 \;\; e \;\; a \equiv 1(mod.m)\}$$

Consideremos ψ um caracter de $\mathbb{Z}_n^*$ e escolhemos m dividindo n, tal que $Ker\rho \subseteq Ker\psi$

$\frac{\mathbb{Z}_n^*}{Ker\rho} \cong Im\rho \hookrightarrow \mathbb{Z}_m^*$ $\quad$ m é o menor inteiro tal que isso acontece.

Assim, podemos pensar χ como definido módulo m ou módulo n, já que ambos assumem os mesmos valores.

Quando um caracter está definido módulo m então ele também pode ser definido módulo qualquer múltiplo de m, logo quando um caracter está definido módulo n podemos perguntar se ele foi estendido de um módulo de definição menor, isto é, se n é um múltiplo de m e se este, por sua vez, é também um múltiplo de outro inteiro, e

assim por diante, até não poder mais ter diminuído o seu módulo de definição. Neste momento acabamos de encontrar o seu condutor.

É conveniente escolher m minimal, que no caso de satisfazer as condições do Lema 2.13, é chamado condutor de χ e denotado por f_χ.

2.2.1 Lema do Condutor

Lema 2.13 *Sejam m e n inteiros positivos e χ um caracter de Dirichlet definido módulo n. O condutor de χ é m se, e somente se m é o menor inteiro que divide n, satisfazendo a seguinte condição: Para todo inteiro $a \in m\mathbb{Z}+1$ e primo com n, tivermos a classe de a módulo n no núcleo de χ.*
Simbolicamente, seja $\chi : (\frac{\mathbb{Z}}{n\mathbb{Z}})^* \to \mathbb{C}^*$ um caracter de Dirichlet

$$f_\chi = m \Leftrightarrow \quad m = minD(n) \setminus \{1\}, \quad t.q. \ \ \forall a \in \mathbb{Z}, \ a \equiv 1(mod.m) \ \ e \ \ (a,n) = 1$$

tem-se $\chi(\bar{a}) = 1$

Prova. $[\Rightarrow$
Seja m um divisor de n ,i.é, $n = tm$, *com* $t \in \mathbb{Z}$. Vamos supor que $\forall\ a \in \mathbb{Z}$ tal que $(a,n) = 1$ e $a \equiv 1(mod.m)$, temos $\chi(\bar{a}) = 1$.
Seja $b \in \mathbb{Z}$ *t.q.* $(b,n) = 1$ *e* $a \equiv b(mod.m)$
$a \equiv b(mod.m) \Leftrightarrow \bar{a} = \bar{b} \Leftrightarrow \bar{a}(\bar{b})^{-1} = \bar{1}$, daí $\chi(\bar{a}(\bar{b})^{-1}) = \chi(\bar{1})$, isto é, $\chi(\bar{a})\chi(\bar{b})^{-1} = 1 \Rightarrow \chi(\bar{a}) = \chi(\bar{b})$, desta forma $\tilde{\chi} : (\frac{\mathbb{Z}}{m\mathbb{Z}})^* \to \mathbb{C}^*$, dada por $\tilde{\chi}(\bar{a}) = \chi(\bar{a})$, está bem definida, $\bar{a} = \bar{b}$ temos $\tilde{\chi}(\bar{a}) = \chi(\bar{a}) = \chi(\bar{b}) = \tilde{\chi}(\bar{b})$

e $\tilde{\chi}(\bar{a}\bar{b}) = \tilde{\chi}(\overline{ab}) = \chi(\overline{ab}) = \chi(\bar{a}\bar{b}) = \chi(\bar{a})\chi(\bar{b}) = \tilde{\chi}(\bar{a})\tilde{\chi}(\bar{b})$, sendo $\tilde{\chi}$ um homomorfismo. Portanto χ pode ser visto como um caracter módulo m.
$\Leftarrow]$
Por outro lado, se χ pode ser vista como um caracter módulo m, temos que para todo $a \in \mathbb{Z}$ tal que $(a,n) = 1$, e consequentemente $(a,m) = 1$, com $a \equiv 1(mod.m) \Rightarrow \bar{a} = \bar{1}$. Como χ está bem definida, $\chi(\bar{a}) = \chi(\bar{1}) = 1$. Assim o condutor de χ é m se, e somente se m é o menor inteiro dividindo n que satisfaz as condições enunciadas. ■

Um caracter definido módulo seu condutor é chamado caracter primitivo.

Na prática, um caracter de Dirichlet é uma aplicação de $\mathbb{Z}$ em $\mathbb{C}^*$, pois os elementos de uma classe de equivalência $\bar{a}$ são elementos de $\mathbb{Z}$.

$\chi : \mathbb{Z} \to \mathbb{C}$, fazendo $\chi(a) = 0$ se $(a, f_\chi) = d \neq 1$ e $\chi(a) \in \mathbb{C}^*$, sempre que $(a, f_\chi) = 1$.

Quando nos referimos a caracteres de $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ ou caracteres $mod.n$, estamos nos referindo a caracteres cujos condutores dividem n.

Observação 2.14 *Se $\chi(-1) = 1$, então χ é chamado de caracter par.*
· *Se $\chi(-1) = -1$, então χ é chamado de caracter ímpar.*

Observação 2.15 *χ, ψ são caracteres de condutores f_χ e f_ψ. Consideremos o homomorfismo*

$$\gamma : \big(\frac{\mathbb{Z}}{[f_\chi, f_\psi]\mathbb{Z}}\big)^* \to \mathbb{C}^*,$$

dado por $\gamma(a) = \chi(a)\psi(a)$, então $\chi\psi$ é o caracter primitivo associado a γ.

Exemplo 2.16 *Considere χ definido mod.12 por:*

$$\begin{gathered}\chi(\bar{1}) = 1\\ \chi(\bar{5}) = -1\\ \chi(\bar{7}) = 1\\ \chi(\overline{11}) = -1,\end{gathered}$$

e ψ definido mod.3 por

$$\begin{gathered}\psi(1) = 1\\ \psi(2) = -1\end{gathered}$$

então $\chi\psi$ em $\big(\frac{\mathbb{Z}}{12\mathbb{Z}}\big)^*$ tem condutor 4.

De fato, $\chi\psi$ tem imagem

$$\begin{gathered}\chi\psi(1) = \chi(1)\psi(1) = 1.1 = 1\\ \chi\psi(5) = \chi(5)\psi(5) = \chi(5)\psi(2) = (-1).(-1) = 1\\ \chi\psi(7) = \chi(7)\psi(7) = \chi(7)\psi(1) = (-1).(1) = -1\\ \chi\psi(11) = \chi(11)\psi(11) = \chi(11)\psi(2) = 1.(-1) = -1,\end{gathered}$$

$4 \mid 8$ e $\forall\ a \in \mathbb{Z}$, tal que $(a, 12) = 1$ e $a \equiv 4k + 1, com\ \ k \in \mathbb{Z}$, temos as seguintes imagens:

$$\left\|\begin{array}{c} k = 0 \quad a = 1, \quad (1,12) = 1 \quad e \quad \chi\psi(1) = 1,\\ k = 1 \quad a = 5, \quad (5,12) = 1 \quad e \quad \chi\psi(5) = 1,\\ k = 2 \quad a = 9, \quad (9,12) \neq 1 \quad e \quad 9 \notin \big(\frac{\mathbb{Z}}{12\mathbb{Z}}\big)^*\\ k = 3 \quad a = 13, \quad (13,12) = 1 \quad e \quad \chi\psi(13) = \chi\psi(1) = 1,\\ k = 4 \quad a = 17, \quad (17,12) = 1 \quad e \quad \chi\psi(17) = \chi\psi(5) = 1,\\ k = 5 \quad a = 21, \quad (21,12) \neq 1 \quad e \quad 21 \notin \big(\frac{\mathbb{Z}}{12\mathbb{Z}}\big)^*\\ k = 6 \quad a = 25, \quad (25,12) = 1 \quad e \quad \chi\psi(25) = \chi\psi(1) = 1,\\ k = 7 \quad a = 29, \quad (29,12) = 1 \quad e \quad \chi\psi(29) = \chi\psi(5) = 1,\\ k = 8 \quad a = 33, \quad (33,12) \neq 1 \quad e \quad 33 \notin \big(\frac{\mathbb{Z}}{12\mathbb{Z}}\big)^*, \end{array}\right.$$

daí, $a \in \{1, 5, 13, 17, \ldots, 12n - 11\ ou\ 12n - 7, \ldots \quad ; n \in \mathbb{Z}^*\} \subseteq Ker\chi\psi$.

Observação 2.17 *Se $(f_\chi, f_\psi) = 1$, então $f_{\chi\psi} = f_\chi f_\psi$.*

Note do exemplo anterior que $f_{\chi\psi} = 4$ e $4 = 2.2$ ou $4 = 4.1$, mas

$$f_\chi \neq 4 \mid 12, \quad \text{para} \quad a = 5, \quad \text{temos} \quad 5 \equiv 1(mod.4),\ (5,12) = 1, \quad \text{mas} \quad \chi(5) = -1$$

$$f_\chi \neq 2 \mid 12, \quad \text{para} \quad a = 5, \quad \text{temos} \quad 5 \equiv 1(mod.4),\ (5,12) = 1, \quad \text{mas} \quad \chi(5) = -1,$$

verificar se $f_\chi = 3, \ \ ou \ \ 6$

$f_\chi \neq 3 \mid 12, \quad$ para $\quad a = 7, \ \$ temos $\ 7 \equiv 1(mod.3), \ (7,12) = 1, \ \$ mas $\ \chi(7) = -1,$

logo $f_\chi \neq 3$.

Agora,

$f_\chi \neq 6 \mid 12, \ \$ para $\ a = 19, \ \$ temos $\ 19 \equiv 1(mod.12), \ (19,12) = 1, \ \$ mas $\ \chi(19) = \chi(7) = -1,$

logo $f_\chi \neq 6$, agora só nos resta dizer que $f_\chi = 12$.

e $f_\psi = 3$, pois ψ não é trivial, e portanto $(f_\chi, f_\psi) \neq 1$.

Seja $\prod_{i=1}^{r} m_i$ uma decomposição de m em produtos de inteiros m_i dois a dois relativamente primos, $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

Seja $\theta : \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \to \left(\frac{\mathbb{Z}}{m_1\mathbb{Z}}\right)^* \times \cdots \times \left(\frac{\mathbb{Z}}{m_r\mathbb{Z}}\right)^*$ um isomorfismo de grupos dado por $\theta([x]_m) = ([x]_{m_1}, [x]_{m_2}, \ldots, [x]_{m_r})$, onde $[x]_m$ é a classe do x módulo m.

Dado um caracter χ de $\prod_{i=1}^{r} \left(\frac{\mathbb{Z}}{m_i\mathbb{Z}}\right)^*$, isto é

$$\chi : \left(\frac{\mathbb{Z}}{m_1\mathbb{Z}}\right)^* \times \cdots \times \left(\frac{\mathbb{Z}}{m_r\mathbb{Z}}\right)^* \to \mathbb{C}^*,$$

definido por

$$\begin{aligned} \chi(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_r) &= \chi((x_1, 1, \ldots, 1)(1, x_2, \ldots, 1) \cdots (1, 1, \ldots, x_r)) \\ &= \chi(x_1, 1, \ldots, 1)\chi(1, x_2, \ldots, 1) \cdots \chi(1, 1, \ldots, x_r) \\ &= \chi_1(\bar{x}_1)\chi_2(\bar{x}_2) \cdots \chi_r(\bar{x}_r), \quad \forall \ \bar{x}_i \in \left(\frac{\mathbb{Z}}{m_i\mathbb{Z}}\right)^*, \end{aligned}$$

onde cada $\chi_i \in \widehat{\left(\frac{\mathbb{Z}}{m_i\mathbb{Z}}\right)^*}$ é dado por $\chi_i(\bar{x}_i) = \chi(1, 1, \ldots, x_i, \ldots, 1)$.

Assim temos

$$\widehat{\theta} : \left(\frac{\mathbb{Z}}{m_1\mathbb{Z}}\right)^* \widehat{\times \cdots \times} \left(\frac{\mathbb{Z}}{m_r\mathbb{Z}}\right)^* \longrightarrow \widehat{\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*},$$

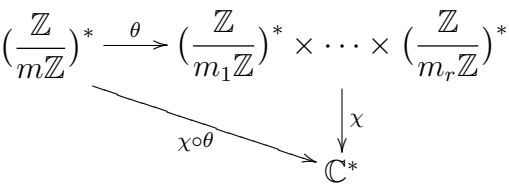
dada por $\widehat{\theta}(\chi) = \chi \circ \theta$.

Daí,

$$\chi \circ \theta(\bar{x}) = \chi(\theta(\bar{x})) = \chi(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_r) = \chi_1(\bar{x}_1)\chi_2(\bar{x}_2) \cdots \chi_r(\bar{x}_r)$$

$$\forall \ \bar{x} \in \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*, \ \ \forall \ \bar{x}_i \in \left(\frac{\mathbb{Z}}{m_i\mathbb{Z}}\right)^* \ \ e \ \ \forall \ \chi_i \in \widehat{\left(\frac{\mathbb{Z}}{m_i\mathbb{Z}}\right)^*},$$

conforme diagrama abaixo:



Daí, podemos identificar $\widehat{\theta}(\chi) = (\chi_1, \chi_2, \ldots, \chi_r)$ e $\widehat{\theta}$ é isomorfismo, logo todo caracter ψ de $(\frac{\mathbb{Z}}{m\mathbb{Z}})^*$ pode ser escrito na forma $\psi = \chi_1 \cdot \chi_2 \cdots \chi_r$, onde cada χ_i é um caracter módulo m_i.

Portanto, para escrevermos os caracteres de $(\frac{\mathbb{Z}}{m\mathbb{Z}})^*$ precisamos decompor m em fatores primos para conhecermos os caracteres módulo cada fator de m.

Um dos isomorfismos mais importantes para o nosso estudo é aquele que identifica cada caracter de Dirichlet do grupo multiplicativo das unidades do anel $\frac{\mathbb{Z}}{n\mathbb{Z}}$ com um automorfismo do grupo de Galois do corpo ciclotômico $\mathbb{Q}(\zeta_n)$.

Afirmação 2.18 $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ *é isomorfo a* $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Pois existe uma aplicação $\varphi : (\frac{\mathbb{Z}}{n\mathbb{Z}})^* \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, dada por $\varphi(\bar{a}) = \sigma_a$,
$\forall\ \bar{a} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ que é um isomorfismo,
onde $\sigma_a : U_{(n)} \hookleftarrow$ é um automorfismo definido por $\sigma_a(\zeta_n) = \zeta_n^a$.
Prova.

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b(mod.n) \Rightarrow a - b = qn \Rightarrow a = qn + b, \quad q \in \mathbb{Z},$$

$\varphi(\bar{a}) = \sigma_a$ e

$$\sigma_a(\zeta_n) = \zeta_n^a = \zeta_n^{qn+b} = (\zeta_n^n)^q.\zeta_n^b = \zeta_n^b = \sigma_b(\zeta_n) \Rightarrow \sigma_a = \sigma_b \Rightarrow \varphi(\bar{a}) = \varphi(\bar{b}),$$

então φ está bem definida.

Agora,

$$\varphi(\bar{a}\bar{b}) = \varphi(\overline{ab}) = \sigma_{ab} \overset{(*)}{=} \sigma_a \circ \sigma_b = \varphi(\bar{a}) \circ \varphi(\bar{b})$$

então φ é um homomorfismo.

$(*)$: $\quad \sigma_{ab}(\zeta_n) = \zeta_n^{ab} = (\zeta_n^b)^a = \sigma_a(\zeta_n^b) = \sigma_a(\sigma_b(\zeta_n)) = \sigma_a \circ \sigma_b(\zeta_n)$
e $\forall\ \sigma_a \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}),\ \exists!\ \bar{a} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$, tal que $\sigma_a = \varphi(\bar{a})$, então φ é bijetiva, isto é, todo automorfismo de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ é da forma σ_a univocamente determinado por $\bar{a}$ e portanto φ é isomorfismo. ■

Ao identificarmos $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ com $\big(\frac{\mathbb{Z}}{n\mathbb{Z}}\big)^*$, um caracter de Dirichlet *mod.n* pode ser chamado de um caracter de Galois. Um caracter $\chi \in \widehat{\big(\frac{\mathbb{Z}}{n\mathbb{Z}}\big)^*}$ pode ser identificado com um automorfismo $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Seja K o corpo fixo de H,ou seja, H é o subgrupo de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que fixa K,

$$Gal(\mathbb{Q}(\zeta_n)/K) = H \leq Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

H é um conjunto tanto de automorfismos quanto de caracteres e $|H| = [\mathbb{Q}(\zeta_n) : K]$

$K = \{\alpha \in \mathbb{Q}(\zeta_n) \ \ ; \sigma(\alpha) = \alpha \ , \ \forall \ \ \sigma \in H\}$ é o corpo fixo de H.

Seja X o dual de $\big(\frac{\mathbb{Z}}{n\mathbb{Z}}\big)^*$, ou seja, o grupo dos caracteres de Dirichlet *mod.n*, $X = \widehat{\big(\frac{\mathbb{Z}}{n\mathbb{Z}}\big)^*}$

Vamos conhecer agora um subgrupo importante de X, o grupo dos caracteres associados a K, que é denotado por X_K, e é constituído de caracteres numéricos cujos núcleos contêm o grupo que fixa K.

$$X_K = \{\chi \in X \ ; \chi(h) = 1, \ \forall h \in H\}$$

Note que para um caracter χ de X_K na aplicação $\chi(h) = 1$, o automorfismo $h \in H$ deve ser visto como uma classe de equivalência $\bar{a}$, já que H é isomorfo a um subgrupo de $\big(\frac{\mathbb{Z}}{n\mathbb{Z}}\big)^*$, e tal subgrupo está contido no núcleo de cada caracter de X_K. Logo,

$$H = \bigcap_{\chi \ \in \ X_K} Ker\chi.$$

Note também que, devido à correspondência de Galois, o número de caracteres associados a K divide o grau da extensão $\mathbb{Q}(\zeta_n)$ de $\mathbb{Q}$,

$$\begin{array}{l} \mathbb{Q}(\zeta_n) \\ | \ \big) |H| \\ K \\ | \ \big) |X_K| \\ \mathbb{Q} \end{array}$$

que é dado pela função de Euler $\varphi(n)$. Logo, $|X_K| = [K : \mathbb{Q}]$.

Nestas condições, quando n é uma potência de um primo ímpar, podemos fazer uma analogia entre a teoria dos caracteres e a teoria de Galois, pois cada caracter se identifica com um automorfismo(caracter de Galois) e a ordem de X_K vezes a ordem de H é igual ao grau da extensão $\mathbb{Q}(\zeta_n)$ de $\mathbb{Q}$.

Capítulo 3

Resultados Intermediários Aplicados

"Louis Lagrange é a grande pirâmide da Matemática".
Napoleão Bonaparte, séc. XIX

Neste capítulo apresentaremos três resultados que serão aplicados diretamente na demonstração do nosso resultado principal, o teorema 4.1. São dois lemas e um teorema que, além do lema 2.13, formam um preâmbulo para o cálculo do discriminante para o qual nos propusemos.

Considere o corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$, onde p é primo ímpar e $r \geq 1$. $\mathbb{Q}(\zeta_{p^r})$ é uma extensão galoisiana de $\mathbb{Q}$.

O grupo $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$ é cíclico de ordem $\varphi(p^r) = (p-1)p^{r-1}$. O isomorfismo entre $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ e $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$ é dado pela aplicação $\sigma_a \rightsquigarrow \bar{a}$, com $0 < a \leq p^r$ e $mdc(a, p^r) = 1$. Daí $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ também é cíclico de ordem $\varphi(p^r)$.

O teorema fundamental de Galois garante que existe uma correspondência entre os subcorpos de $\mathbb{Q}(\zeta_{p^r})$ e os subgrupos de $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$.

A correspondência de Galois associa a cada subcorpo K de $\mathbb{Q}(\zeta_{p^r})$ um subgrupo H de $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ formado pelos automorfismos de $\mathbb{Q}(\zeta_{p^r})$ que fixam K.

Dado um divisor d de $\varphi(p^r)$, existe um único subcorpo K de $\mathbb{Q}(\zeta_{p^r})$ de grau d e tal corpo é fixado pelo único subgrupo H de $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ de índice d, ou seja, $H = Gal(\mathbb{Q}(\zeta_{p^r})/K)$ e $(Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) : H) = d$. Logo, $[K : \mathbb{Q}] = d$.

3.1 Primeiro Lema

Lema 3.1 *Sejam p um número primo ímpar, r um inteiro positivo, g um inteiro, tal que $\bar{g} = [g]_{p^r}$ é um gerador do grupo $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$. Então para todo j, tal que $0 < j \leq r$, temos que*

$$g^k \equiv 1(mod.p^j) \quad se,e\ somente\ se \quad k \equiv 0(mod(p-1)p^{j-1}).$$

Prova. $[\Rightarrow$

$o(\bar{g}) = \varphi(p^r) = (p-1)p^{r-1} \Leftrightarrow g^{\varphi(p^r)} \equiv 1(modp^r).$

$g^k \equiv 1(modp^j) \Rightarrow g^{k^{p^{n-j}}} \equiv 1(mod\ p^r) \Rightarrow o(g) \mid kp^{r-j}$

Daí

$(p-1)p^{r-1} \mid kp^{r-j} \Rightarrow p-1 \mid k$ e $p^{(r-1)-(r-j)} \mid k \Rightarrow$

$p-1 \mid k$ e $p^{j-1} \mid k \Rightarrow (p-1)p^{j-1} \mid k$, ou seja, $k \equiv 0(mod(p-1)p^{j-1})$.
$\Leftarrow]$

$$k \equiv 0(mod.(p-1)p^{j-1}) \Rightarrow \varphi(p^j)|k \overset{(*)}{\Rightarrow} o(g)|k \Rightarrow g^k = 1 \Rightarrow \bar{g}^k = \bar{1} \Rightarrow g^k \equiv 1(mod.p^j).$$

$(*)$ $\left(\frac{\mathbb{Z}}{p^j\mathbb{Z}}\right)^*$ tem ordem $\varphi(p^j)$ desde que g e p sejam primos entre si $(g,p) = 1$, $o(\bar{g}) = (p-1)p^{j-1}$ e portanto

$$g^k \equiv 1(mod.p^j) \Leftrightarrow k \text{ é um múltiplo de } \varphi(p^j)$$

■

Em resumo

Se $\bar{g}$ gera $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$, então $p^j | g^{t\varphi(p^j)} - 1$, *onde* $j = 1, 2, \ldots, r$ e $t \in \mathbb{N}$.

Seja o inteiro g, tal que $\bar{g}$ é um gerador do grupo $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$, χ um caracter de Dirichlet definido módulo p^r.

Como o número de caracteres de um grupo abeliano finito é igual à ordem do próprio grupo, existem $(p-1)p^{r-1}$ caracteres de Dirichlet definidos módulo p^r, isto é, $\widehat{\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*} = \{\chi_0, \ldots, \chi_{\varphi(p^r)-1}\}$ e pela correspondência $\bar{g} \rightsquigarrow \widehat{g}$, cada caracter χ é completamente determinado pala imagem de $\chi(\bar{g})$.

Considerando o número de caracteres e todas as possibilidades para o inteiro i, podemos concluir, de acordo com o que foi determinado no teorema 2.8, que todos os caracteres definidos $mod.p^r$ são da forma

$$\chi_i(\bar{g}) = \zeta^i_{(p-1)p^{r-1}} \quad , \quad i = 0, 1, 2, \ldots, (p-1)p^{r-1} - 1.$$

Com essas notações veremos o seguinte lema.

3.2 Segundo Lema

Lema 3.2 *Sejam i um inteiro, tal que $0 \leq i < (p-1)p^{r-1}$, g um inteiro, tal que $\bar{g} = [g]_{p^r}$ é um gerador de $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$ e χ_i um caracter de Dirichlet definido módulo p^r, por $\chi_i(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$. Então*

$$p^j = (i, p^r) \text{ se, e somente se o condutor de } \chi_i \text{ é } p^{r-j}.$$

Prova. Para $i = 0$ é imediato,

[$\Rightarrow$

$$(0, p^r) = p^j \Leftrightarrow j = r \Rightarrow p^{r-j} = f_{\chi_i} = p^0 = 1 \Rightarrow f_{\chi_0} = 1$$

$\Leftarrow$]

$$f_{\chi_0} = 1 = p^{r-j} \Rightarrow (i, p^r) = p^j = p^r \Rightarrow \quad \text{com} \;\; i = 0 \;,\; (0, p^r) = p^r.$$

Agora, para $i \neq 0$

[$\Rightarrow$ Se $(i, p^r) = p^j$, então $i = tp^j$, para algum $t \in \mathbb{Z}$. Pelo lema 2.13, χ_i pode ser definido módulo p^{r-j} sss p^{r-j} é o menor inteiro que divide p^r satisfazendo: $\forall \;\; h \in \mathbb{Z}$, tal que $(h, p^r) = 1$ e $h \equiv 1(mod.p^{r-j})$, temos a imagem $\chi_i(\bar{h}) = 1$.

Seja $H = \{\bar{g}^k \in \big(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\big)^* \,; g^k \equiv 1(mod.p^{r-j})\}$ um subgrupo de $\big(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\big)^*$. Pelo lema 3.1, $g^k \equiv 1(mod.p^{r-j}) \Leftrightarrow k = r\varphi(p^{r-j})$, para algum $r \in \mathbb{N}$, ou seja $H = \langle \bar{g}^{(p-1)p^{r-j-1}} \rangle$.

Pela definição do caracter $\chi_i(\bar{g}) = \zeta^i_{\varphi(p^r)}$, temos $\chi_i(\bar{g}^k) = \zeta^{ik}_{\varphi(p^r)}$. No entanto $\bar{g}^{\varphi(p^{r-j})} = \bar{h} \in H$, logo

$$\chi_i(\bar{h}) = \chi_i(\bar{g}^{(p-1)p^{r-j-1}}) = \zeta^{i(p-1)p^{r-1-j}}_{(p-1)p^{r-1}} = \zeta^{tp^j(p-1)p^{r-1}\cdot\frac{1}{p^j}}_{(p-1)p^{r-1}} = \zeta^{t(p-1)p^{r-1}}_{(p-1)p^{r-1}} = 1 \Rightarrow f_{\chi_i} = p^{r-j}.$$

$\Leftarrow$]
Supor que χ_i possa ser definido módulo p^{r-j}, então $\chi_i(\bar{h}) = 1, \quad \forall \quad h \in H$, em particular $\chi_i(\bar{g}^{(p-1)p^{r-j-1}}) = \zeta^{i(p-1)p^{r-j-1}}_{(p-1)p^{r-1}} = 1$ desde que exista um inteiro t tal que $i(p-1)p^{r-j-1} = t(p-1)p^{r-1}$ implicando que $i = tp^j$, para algum inteiro t ■

Em resumo, $i = tp^j$ sss χ_i pode ser definido módulo p^{r-j}, o que equivale dizer que o condutor de χ_i é p^{r-j} se p^j é a maior potência de p que divide i, ou seja, se $p^j = (i, p^r)$ e portanto $(i, p^r) = p^j \Leftrightarrow f_{\chi_i} = p^{r-j}$, onde $i = 0, 1, 2, \ldots, \varphi(p^r) - 1$ e $\chi_i(\bar{g}) = \zeta^i_{\varphi(p^r)}$, para $< \bar{g} >= \big(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\big)^*$.

3.3 O Teorema de Hasse

Também conhecido como a fórmula do condutor-discriminante, o teorema de Hasse, afirma que se um corpo de números abelianos K é fixado por um subgrupo H de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, o discriminante de K pode ser obtido de H, calculando o produto dos condutores de todos os caracteres de Dirichlet definidos módulo n, que estão associados a K. Tal teorema assegura que o discriminante de K é, a menos de sinal, o produto desses condutores.

Teorema 3.3 *Sejam n um inteiro positivo, L o corpo ciclotômico $\mathbb{Q}(\zeta_n)$, H um subgrupo do grupo dos automorfismos de L, e K o subcorpo de L fixado por H. Então o*

discriminante do corpo K é, a menos de sinal, o produto dos condutores dos caracteres numéricos definidos módulo n que são associados a K.

$$\big|Disc(K)\big| = \prod_{\chi \in X_K} f_\chi$$

Observação 3.4 *A expressão , a menos de sinal, diz respeito ao fato de o discriminante ser um número positivo ou negativo, e está relacionado à paridade do número de imersões complexas de K.*

Assim, $Disc(K) = (-1)^{r_2} \prod_{\chi \in X_K} f_\chi$, onde r_2 é $\frac{1}{2}$ do número de imersões complexas

Veremos agora quem são os números r_1 *e* r_2.

Seja $L = \mathbb{Q}(\alpha)$ uma extensão normal de corpos e finita de $\mathbb{Q}$ e $\Omega = A_{\mathbb{C}}(L)$ o fecho algébrico de L em $\mathbb{C}$

$$\begin{array}{l} \mathbb{C} \\ | \\ \Omega \\ | \\ L = \mathbb{Q}(\alpha) \\ | \ \big) n = \partial P_{\alpha|\mathbb{Q}} \\ \mathbb{Q} \end{array}$$

Existem n $\mathbb{Q}$-isomorfismos de L em Ω e m $\mathbb{Q}$-isomorfismos de L em $\mathbb{R}$.

Isto é, existem m raízes reais distintas de $P_{\alpha/\mathbb{Q}}$ e $(n-m)$ raízes complexas puras distintas de $P_{\alpha/\mathbb{Q}}$.
Daí, o conjunto das raízes de $P_{\alpha/\mathbb{Q}}$ é $\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_{m+1}, \overline{\beta_{m+1}}, \ldots, \beta_{\frac{n-m}{2}}, \overline{\beta_{\frac{n-m}{2}}}\}$.
Então o número de raízes reais $r_1 = m$ e $r_2 = \frac{n-m}{2}$, e temos $n = r_1 + 2r_2$

Exemplo 3.5 *Seja $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ o subcorpo real maximal de $\mathbb{Q}(\zeta_p)$, usando o teorema 3.3 vamos calcular o disc(K).*

$$\varphi(p) \left(\begin{array}{l} L = \mathbb{Q}(\zeta_p) \\ | \ \big) 2 \\ K = \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \\ | \ \big) \frac{\varphi(p)}{2} = \frac{p-1}{2} \\ \mathbb{Q} \end{array} \right.$$

Sabemos que $P_{\zeta_p/K} = x^2 + (\zeta_p + \zeta_p^{-1})x + 1$, logo ζ_p, ζ_p^{-1} são raízes de $P_{\zeta_p/K}$ e $\partial P_{\zeta_p/K} = 2$, donde $[K : \mathbb{Q}] = \frac{p-1}{2}$ e que $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, pela proposição 1.9, é o maior subcorpo de L que está contido em $\mathbb{R}$, logo $r_2 = 0$.

K é o corpo fixo do subgrupo H de $Aut(L/\mathbb{Q})$ gerado por σ, onde $\sigma(\zeta_p) = \zeta_p^{-1}$,

$$< \sigma >= H = Aut(L/K) = \{Id, \sigma\}$$

e $[K:\mathbb{Q}] = |Aut(K/\mathbb{Q})| = \frac{p-1}{2} \Rightarrow Aut(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{\frac{p-1}{2}}\}$.

Daí, temos $\frac{p-1}{2}$ automorfismos que vistos como caracteres tornam-se

$$X_K = \{\chi_o, \chi_1, \chi_2, \ldots, \chi_{\frac{p-3}{2}}\}.$$

Note que cada χ_i é caracter de Dirichlet $\chi : (\frac{\mathbb{Z}}{p\mathbb{Z}})^* \to \mathbb{C}^*$, definido módulo p. Logo com exceção de χ_o todos têm condutor p. E pelo teorema 3.3,

$$Disc(K) = (-1)^0 p^{\frac{p-3}{2}} = p^{\frac{p-3}{2}}.$$

Temos agora as ferramentas necessárias e suficientes para o cálculo do discriminante absoluto de um corpo K nas condições descritas no título da dissertação.

Capítulo 4

Cálculo do Discriminante

"Eu vi um professor de Matemática ser enterrado como um Rei; daqueles que tivera feito um grande bem a seus súditos".

François Voltaire, sec. XVIII, se pronunciando após ter assistido aos funerais de Isaac Newton.

Considere o corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$, onde p é primo impar e r é um inteiro positivo. Seja K um subcorpo próprio da extensão $\mathbb{Q}(\zeta_{p^r})$ de $\mathbb{Q}$. Então temos que o grau de K sobre $\mathbb{Q}$ é um divisor próprio de $\varphi(p^r) = (p-1)p^{r-1}$.

Assim, podemos escrever $[K:\mathbb{Q}] = up^j$, onde $j = 0, 1, \ldots, r-1$ e u divide $p-1$.

O discriminante de K é, de acordo como o teorema de Hasse, a menos de sinal, o produtos dos condutores de todos os caracteres que estão associados a K, isto é, os caracteres de Dirichlet definidos módulo p^r cujos núcleos contêm o subgrupo de $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ que fixa K.

Devido aos teoremas 1.6 e 2.10 , faremos uso dos isomorfismos entre os grupos $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$, $\big(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\big)^*$ e $\widehat{\big(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\big)^*}$, no sentido de que ora um automorfismo funcionará como um caracter, ora este, por sua vez, pode ser identificado com uma unidade de $\frac{\mathbb{Z}}{p^r\mathbb{Z}}$.

O seguinte teorema que nos fornece o discriminante absoluto do corpo K, nas condições acima citadas, é o nosso resultado principal.

4.1 A Fórmula do Discriminante

Teorema 4.1 *[Tra]Sejam p um primo impar, r um inteiro positivo e K um subcorpo de $\mathbb{Q}(\zeta_{p^r})$, com $[K:\mathbb{Q}] = up^j$, onde $u \mid p-1$. Então*

$$|Disc(K)| = p^{u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}]-1}.$$

Prova.

Se $[K:\mathbb{Q}] = up^j$, então o subgrupo H de $Gal(\mathbb{Q}(\zeta_{p^r})|\mathbb{Q})$ que fixa K também é cíclico de ordem

$$\frac{[\mathbb{Q}(\zeta_{p^r}):\mathbb{Q}]}{[K:\mathbb{Q}]} = \frac{\varphi(p^r)}{up^j},$$

isto é,

$$|H| = \frac{(p-1)p^{r-1}}{up^j} = \frac{p-1}{u} \cdot \frac{p^{r-1}}{p^j} = \frac{p-1}{u} \cdot p^{r-j-1},$$

$$\varphi(p^r) \begin{cases} \mathbb{Q}(\zeta_{p^r}) \\ | \\ \frac{p-1}{u}p^{r-j-1} = |H| \\ | \\ K \\ | \\ up^j \\ | \\ \mathbb{Q} \end{cases}$$

A nossa meta agora é a descrição detalhada do conjunto

$$X_K = \{\chi \in \widehat{(\frac{\mathbb{Z}}{p^r\mathbb{Z}})^*} \, ; \chi(H) = 1\}$$

grupo dos caracteres associados a K. Sua constituição é essencial para que possamos explicitar os condutores de seus elementos.

Se σ_a é um gerador de H, pela afirmação 2.18, $\langle \bar{a} \rangle = H$ e χ um caracter de Dirichlet definido módulo p^r, podemos concluir que χ é associado a K se, e somente se $\chi(\sigma_a) = 1$.

Agora, seja $g \in \mathbb{Z}$, tal que $\bar{g} = [g]_{p^r}$ é um gerador de $(\frac{\mathbb{Z}}{p^r\mathbb{Z}})^*$.
A ordem de $\bar{a} = [a]_q$, com $\varphi(q)$ dividindo $\varphi(p^r)$, é igual a ordem de H, isto é,

$o(\bar{a}) = \varphi(q) = \frac{p-1}{u}p^{r-j-1}$.

Podemos supor, sem perda de generalidade, que $a \equiv g^d (mod.p^r)$, onde $d = up^j$, pois $\bar{a} = \bar{g}^d$.

Consequentemente, dado um caracter χ_i definido módulo p^r temos que $\chi_i(\bar{a}) = 1$ se, e somente se a ordem de $\bar{g}$ for um divisor do fator id.

De fato, pela definição $\chi_i(\bar{g}) = \zeta^i_{\varphi(p^r)}$, com $i = 0, 1, \ldots, \varphi(p^r) - 1$.

Daí $\chi_i(\bar{a}) = \chi_i(\bar{g}^d) = \zeta^{id}_{\varphi(p^r)} = 1$ se, e somente se $id = t\varphi(p^r)$.

Ou seja, $i = \frac{t}{d}\varphi(p^r)$, com $t = 0, 1, \ldots, d-1$, pois $t < d$ e $i < \varphi(p^r)$.

Ou equivalentemente, sendo $d = up^j$, o caracter χ_i é associado a K se, e somente se i for um múltiplo da ordem de H.

Isto é, $\chi_i(\bar{a}) = 1 \Leftrightarrow i = t\frac{p-1}{u}p^{r-j-1}$, onde $t = 0, 1, \ldots, up^j - 1$. Como K é corpo fixo, a ordem de H é invariante, logo para $\chi_i \in X_K$ o índice i é uma função de t, $i = t|H|$.

- Se $t = 0 \Rightarrow i = 0$ e $\chi_{i=0}(\bar{a}) = 1$ e $f_{\chi_0} = 1$, logo para $t = 0$ o condutor de χ_i é 1 e portanto ele é neutro para o cálculo do discriminante de K.

- Para $t \neq 0$, ou seja, para $t \in \{1, 2, \ldots, up^j - 1\}$ que importa para o nosso cálculo. Note que o discriminante de K é, em tese, uma potência de p cujo expoente está em função de u, p e j, logo procederemos para tornar t em função deles.

  Seja $t = p^l t_k$, onde $l = 0, 1, \ldots, j$ e $(t_k, p) = 1$.

  Para $l = 0$, temos a pergunta: Quantos elementos $t = t_k$ primos com p existem entre 1 e $up^j - 1$?
  Entre 1 e $up^j - 1$ os múltiplos de p são: $p, 2p, \ldots, (up^{j-1} - 1)p$, ou seja, teremos $(up^{j-1} - 1)$ números que não são primos com p, logo os números primos com p são todos menos esses, i.é.,
  $(up^j - 1) - (up^{j-1} - 1) = up^j - up^{j-1} = u(p-1)p^{j-1} = u\varphi(p^j)$

  Para $l = 1$, quantos elementos $t = pt_k$ primos com p existem entre 1 e $up^{j-1} - 1$? os múltiplos de p são: $p, 2p, \ldots, (up^{j-2} - 1)p$. Analogamente,
  $(up^{j-1} - 1) - (up^{j-2} - 1) = up^{j-1} - up^{j-2} = u(p^{j-1} - p^{j-2}) = u(p-1)p^{j-1}p^{-1} = \frac{u}{p}\varphi(p^j)$

  Para $l = 2$, chegaremos pelo mesmo raciocínio em $\frac{u}{p^2}\varphi(p^j) \ldots$

  Desta forma, teremos $\frac{u}{p^l}\varphi(p^j)$ elementos $t_{k'}s$ primos com p, e $0 \leq l \leq j$.

  Para $l = 0$, teremos $u(p-1)p^{j-1}$ elementos $t_{k'}s$ nestas condições, isto é, $u(p-1)p^{j-1}$ caracters χ_i(pois o índice i está em função de t_k)em X_K cujos condutores, pelo lema 3.2, são todos iguais a p^{j+1}.

  $l = 0, \quad p^l = p^0 = 1$, então $(i, p^r) = p^l \Leftrightarrow f_{\chi_i} = p^{r-l} = p^r = p^{j+1}$.

  Para $l = 1$, $t = pt_k$, com $(t_k, p) = 1$. Daí temos $\frac{u}{p^l}\varphi(p^j)$ elementos $t'_k s$ nestas condições, isto é, $u(p-1)p^{j-2}$ caracteres χ_i em X_K cujos condutores, pelo lema 3.2, são todos iguais a p^j.

  $l = 1, \quad p^l = p^1 = p$, então $(i, p^r) = p^l \Leftrightarrow f_{\chi_i} = p^{r-l} = p^{r-1} = p^{j+1-1} = p^j$. Analogamente...

  Para $l = j - 1$, $t = p^{j-1}t_k$, com $(t_k, p) = 1$. Daí temos $\frac{u}{p^l}\varphi(p^j)$ elementos $t_{k's}$ nestas condições, isto é, $u(p-1)p^{j-1-j+1} = u(p-1)$ caracteres χ_i cujos condutores, pelo lema 3.2, são todos iguais a p^2.

  $l = j - 1, \quad p^l = p^{j-1}$, então $(i, p^r) = p^{j-1} \Leftrightarrow f_{\chi_i} = p^{r-l} = p^{j+1-j+1} = p^2$.

  E finalmente para $l = j$, temos $t = p^j t_k$. Daí, existem $(u-1)$ elemetos $t'_k s$ primos com p, $(t_k, p) = 1$, pois t é no máximo $up^j - 1$, isto é, $u - 1$ caracteres χ_i cujos condutores, pelo lema 3.2, são todos iguais a p.

  $$l = j \Rightarrow p^l = p^j \Rightarrow (i, p^r) = p^j \Leftrightarrow f_{\chi_i} = p^{r-j} = p^{j+1-j} = p.$$

Obtemos então a seguinte tabela

l	n^o de χ_i associado a K	condutor
0	$up^{j-1}(p-1)$	p^{j+1}
1	$up^{j-2}(p-1)$	p^j
2	$up^{j-3}(p-1)$	p^{j-1}
$\vdots$	$\vdots$	$\vdots$
s	$up^{j-(s+1)}(p-1)$	$p^{j-(s-1)}$
$\vdots$	$\vdots$	$\vdots$
j-1	$up^0(p-1)$	p^2
j	$u-1$	p

Na 1^a coluna temos os possíveis valores de l.

Na 2^a coluna temos o número de caracteres não triviais χ_i para os quais $i = t_k\frac{p-1}{u}p^{r-j-1+l}$ e $(t_k, p) = 1$.

Exceto para o caracter trivial, todos os caracteres associados a K estão registrados nesta tabela.

Note que o somatório da 2^a coluna é igual a $up^j - 1$

$$u(p-1)(1+p+p^2+\cdots+p^{j-1})+u-1;$$
$$u(p-1)(\frac{1.p^{j-1}p-1}{p-1})+u-1;$$
$$u(p-1)(\frac{p^j-1}{p-1})+u-1;$$
$$u(p^j-1)+u-1 = up^j-u+u-1 = up^j-1.$$

Confirmando que, $|X_K| = [K:\mathbb{Q}]$.

Na 3^a coluna temos os condutores correspondentes desses caracteres.

Continuando. Pelo teorema 3.3, o discriminante de K é, a menos do sinal, igual ao produto dos condutores dos caracteres χ_i que são associados a K.

$$|Disc(K)| = \prod_{\chi_i \in X_K} f_{\chi_i}$$

$$l=0, \quad \text{temos} \quad \underbrace{p^{j+1}p^{j+1}\cdots p^{j+1}}_{up^{j-1}(p-1) \quad fatores} = (p^{j+1})^{up^{j-1}(p-1)} = p^{up^{j-1}(p-1)(j+1)}$$

$$l=1, \quad \text{temos} \quad \underbrace{p^{j}p^{j}\cdots p^{j}}_{up^{j-2}(p-1) \quad fatores} = (p^{j})^{up^{j-2}(p-1)} = p^{up^{j-2}(p-1)j}$$

$$l=2, \quad \text{temos} \quad \underbrace{p^{j-1}p^{j-1}\cdots p^{j-1}}_{up^{j-3}(p-1) \quad fatores} = (p^{j-1})^{up^{j-3}(p-1)} = p^{up^{j-3}(p-1)(j-1)}$$

$$\vdots$$

$$l=j-1, \quad \text{temos} \quad \underbrace{p^{2}p^{2}\cdots p^{2}}_{up^{0}(p-1) \quad fatores} = (p^{2})^{up^{0}(p-1)} = p^{up^{0}(p-1)2}$$

$$l=j, \quad \text{temos} \quad \underbrace{pp\cdots p}_{u-1 \quad fatores} = (p^{1})^{u-1} = p^{(u-1)1}$$

$$\prod_{\chi_i \in X_K} f_{\chi_i} = p^{up^{j-1}(p-1)(j+1)}p^{up^{j-2}(p-1)j}p^{up^{j-3}(p-1)(j-1)}\cdots p^{up^{0}(p-1)2}p^{u-1} =$$

$$p^{u(p-1)[(j+1)p^{j-1}+jp^{j-2}+(j-1)p^{j-3}+\cdots+2p^{0}]+(u-1)} = p^{u(p-1)\frac{\sum_{i=0}^{j}(i+1)p^{i}-1}{p}+(u-1)}.$$

Ou seja, $Disc(K)$ é uma potência de p cujo expoente é computado como sendo o somatório de cada elemento da 2ª coluna multiplicado pelo $\log_p$ dos elementos correspondentes da 3ª coluna.

Agora,

$$u(p-1)\frac{\sum_{i=0}^{j}(i+1)p^{i}-1}{p}+(u-1) = \frac{u(p-1)}{p}\big(\sum_{i=0}^{j}(i+1)p^{i}-1\big)+u-1 =$$

$$\frac{u(p-1)}{p}\sum_{i=0}^{j}(i+1)p^{i}-\frac{u(p-1)}{p}+u-1 = \frac{u(p-1)}{p}\sum_{i=0}^{j}(i+1)p^{i}+\frac{u}{p}-1,$$

e note que

$$\sum_{i=0}^{j}(i+1)p^{i} = 1+2p+3p^{2}+\cdots+(j+1)p^{j} = \frac{(j+2)p^{j+1}(p-1)-(p^{j+2}-1)}{(p-1)^{2}}.$$

Pois,

$$1+p+p^{2}+\cdots+p^{j+1} = \frac{p^{j+1}p-1}{p-1} = \frac{p^{j+2}-1}{p-1},$$

E que p é raiz do polinômio $1 + x + x^2 + \cdots + x^{j+1} - \frac{x^{j+2}-1}{x-1}$, que como equação polinomial tem seu conjunto solução, neste caso, contido no conjunto dos números primos.

$$De \quad \frac{d}{dx}(1 + x + x^2 + \cdots + x^{j+1})\Big|_{x=p} - \frac{d}{dx}\left(\frac{x^{j+2}-1}{x-1}\right)\Big|_{x=p}$$

Temos

$$1 + 2p + 3p^2 + \cdots + (j+1)p^j - \frac{(j+2)p^{j+1}(p-1) - (p^{j+2}-1)}{(p-1)^2} = 0$$

Daí,

$$\frac{u(p-1)}{p}\left(\frac{(j+2)p^{j+1}(p-1) - (p^{j+2}-1)}{(p-1)^2}\right) + \frac{u}{p} - 1 =$$

$$\frac{u(p-1)(j+2)p^{j+1}(p-1)}{p(p-1)^2} - \frac{u(p-1)(p^{j+2}-1)}{p(p-1)^2} + \frac{u}{p} - 1$$

$$= \; u(j+2)p^j - \frac{u(p^{j+2}-1)}{p(p-1)} + \frac{u}{p} - 1 =$$

$$u\left((j+2)p^j - \frac{(p^{j+2}-1)}{p(p-1)} + \frac{1}{p}\right) - 1.$$

Portanto o expoente encontrado é $u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}] - 1$ ■

Corolário 4.2 *Dados inteiros positivos p e r, com p primo ímpar, o discriminante do corpo ciclotônico $\mathbb{Q}(\zeta_{p^r})$ é dado por*

$$Disc(\mathbb{Q}(\zeta_{p^r})) = (-1)^{\frac{p-1}{2}} p^{(p-1)[(r+1)p^{r-1} - \frac{p^{r-1}-1}{p-1}]-1}$$

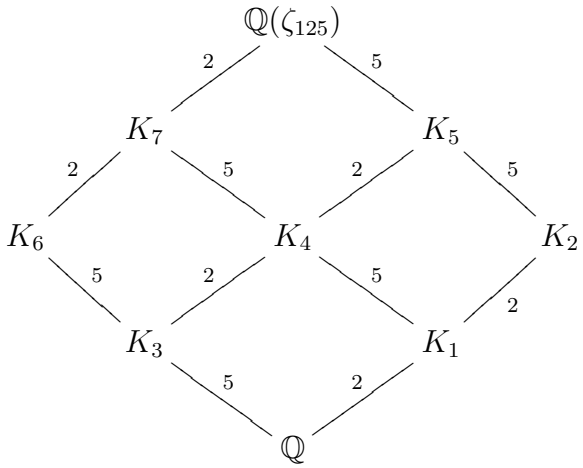
Corolário 4.3 *Se p é um primo ímpar, e $K \subseteq \mathbb{Q}(\zeta_p)$, então*

$$|Disc(K)| = p^{[K:\mathbb{Q}]-1}$$

Exemplo 4.4 *Para $p = 5$ e $r = 3$, temos exatamente sete subcorpos próprios da extensão $\mathbb{Q}(\zeta_{125})$ de $\mathbb{Q}$ correspondendo a sete subgrupos de $Gal(\mathbb{Q}(\zeta_{125})|\mathbb{Q})$.*

Se $[K_i : \mathbb{Q}] = d$, então $|H_i| = |Gal(\mathbb{Q}(\zeta_{125})|K_i)| = \frac{100}{d}$.

Esquematicamente, temos



Dos sete subcorpos próprios de $\mathbb{Q}(\zeta_{5^3})$ *podemos identificar, por 1.5.2; o corpo quadrático* $K_1 = \mathbb{Q}(\sqrt{5})$*, os ciclotômicos* $K_2 = \mathbb{Q}(\zeta_5)$*,* $K_5 = \mathbb{Q}(\zeta_{5^2})$ *e, por 1.9, o subcorpo real maximal* $K_7 = \mathbb{Q}(\zeta_{5^3} + \zeta_{5^3}^{-1})$*. Para identificar os não ciclotômicos* K_3*,* K_4 *e* K_6 *será necessário encontrar os subgrupos, que os fixam, de um grupo de automorfismos de ordem* 100*, o que não é o objetivo do nosso trabalho, mas expressar os discriminantes como uma potência de* $p = 5$*, como segue:*

$$disc(\mathbb{Q}(\zeta_{125})) = 5^{275}$$

$$[K_7 : \mathbb{Q}] = 50 \Rightarrow |H_7| = 2 \qquad disc(K_7) = 5^{137}$$

$$[K_6 : \mathbb{Q}] = 25 \Rightarrow |H_6| = 4 \qquad disc(K_6) = 5^{68}$$

$$[K_5 : \mathbb{Q}] = 20 \Rightarrow |H_5| = 5 \qquad disc(K_5) = 5^{35}$$

$$[K_4 : \mathbb{Q}] = 10 \Rightarrow |H_4| = 10 \qquad disc(K_4) = 5^{17}$$

$$[K_3 : \mathbb{Q}] = 5 \Rightarrow \ |H_3| = 20 \qquad disc(K_3) = 5^{8}$$

$$[K_2 : \mathbb{Q}] = 4 \Rightarrow \ |H_2| = 25 \qquad disc(K_2) = 5^{3}$$

$$[K_1 : \mathbb{Q}] = 2 \Rightarrow \ |H_1| = 50 \qquad disc(K_1) = 5$$

Vejamos agora na literatura onde o leitor poderá estender o nosso resultado e encontrar o caso $p = 2$ e o discriminante absoluto de um corpo ciclotômico qualquer.

Observação 4.5 *A diferença no cálculo do discriminante de subcorpos de* $\mathbb{Q}(\zeta_{2^r})$ *consiste no fato de que o grupo de Galois de* $\mathbb{Q}(\zeta_{2^r})$ *sobre* $\mathbb{Q}$ *não é cíclico, daí não existir a unicidade do caso primo ímpar, podendo haver dois ou mais subcorpos de mesmo grau com diferentes discriminantes.*

Neste caso, dado um divisor d do grau de $\mathbb{Q}(\zeta_{2^r})$,basta analisar se o subcorpo K de $\mathbb{Q}(\zeta_{2^r})$ de grau d é ciclotômico ou não.

Veja o resultado do artigo "discriminants of subfields $\mathbb{Q}(\zeta_{2^r})$" publicado no "Journal of algebra and applications "[Lop].

Seja K o corpo ciclotômico $\mathbb{Q}(\zeta_{2^m})$ subcorpo de $\mathbb{Q}(\zeta_{2^r})$, de grau 2^{m-1} e corpo fixo de $H =< \bar{5}^{2^{m-2}} >$, onde $|H| = 2^{r-m}$. Então $|disc(K)| = 2^{(m-1)2^{m-1}}$.

Noutro caso, $|disc(K)| = 2^{m2^{m-1}-1}$, onde o corpo intermediário K, corpo fixo do subgrupo $H =< -\bar{1}, \bar{5}^{2^{m-1}} >$, não é ciclotômico.

Observação 4.6 *Mencionamos sem demonstração a fórmula do discriminante que se generaliza ao m-ésimo corpo ciclotômico, para qualquer $m > 1$*

$$|disc(\mathbb{Q}(\zeta_m))| = \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\frac{\varphi(m)}{p-1}}}, \qquad veja \ \ [Was].\ prop\ 2.7$$

Nesta Dissertação apresentamos um método para o cálculo do discriminante de corpos com condutor potência de um primo ímpar, isto é, de subcorpos de $\mathbb{Q}(\zeta_{p^r})$, neste caso um corpo abeliano, o qual pode se aplicar a fórmula do condutor-discriminante.

Isso foi possível devido ao fato de o grupo de Galois de $\mathbb{Q}(\zeta_{p^r})$ sobre os racionais ser cíclico.

Então para cada divisor $d = up^j$ do grau de $\mathbb{Q}(\zeta_{p^r})$ com $j = 0, 1, \ldots, r-1$, existe um único subcorpo K de $\mathbb{Q}(\zeta_{p^r})$ de grau d, fixado por um subgrupo H de $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ de ordem $(p-1)p^{r-1}d^{-1}$, e reciprocamente.

E é justamente por essa correspondência biunívoca que o discriminante absoluto de K pôde ser obtido como uma função de seu grau.

Apêndice A

Apêndice

"A Matemática é uma linguagem. A linguagem que Deus descrevera o universo".
Galileu Galilei, séc. XVII, externando sua opinião a respeito da rainha das ciências.

Este apêndice, escrito com o objetivo introdutório, é constituído dos resultados básicos aplicados ao cálculo do discriminante, vizando atender aos leitores sem formação em Teoria Algébrica dos Números, porém interessados num melhor entendimento das técnicas aqui abordadas, tal como a definição de inteiro algébrico, anel integralmente fechado, norma e traço relativos e polinômio característico.

Veremos a construção do polinômio característico e sua relação com o polinômio minimal de um elemento algébrico sobre $\mathbb{Q}$, o discriminante de um polinômio f com coeficientes sobre um corpo, corpos conjugados e elementos conjugados e uma apresentação superficial da Teoria de Galois com ênfase em seu teorema fundamental.

Os K-espaços vetoriais serão expressos em sua versão generalizada, os A-módulos, e quando existir um sistema finito de geradores, estaremos nos referindo a um A-módulo F.G. (finitamente gerado), que é uma ferramenta importante na determinação do posto e de bases integrais.

Iniciamos com uma apresentação das estruturas algébricas, campos aplicativos onde se caracterizam as operações, com destaque para o grupo de Galois, grupo multiplicativo das unidades do anel dos inteiros módulo n e extensão galoisiana dos racionais, bem como o objeto sobre o qual discorre quase todo nosso estudo, o anel dos inteiros algébricos.

Admitiremos já conhecidos os conceitos de estruturas como Anéis, Domínios e Corpos, como também os resultados básicos da Teoria dos Grupos e de Anéis, subanéis unitários e ideais primos e maximais. O leitor poderá relembrar alguns desses conceitos consultando a literatura em [Gon,Gar].

A.1 Estruturas Algébricas

Sejam E um conjunto não-vazio, e $* : E \times E \longrightarrow E$ uma operação binária.

Denotamos $*(x, y)$ por $x * y$, para quaisquer que sejam $x, y \in E$.

Chamamos de estrutura algébrica um conjunto não-vazio E, munido de pelo menos uma operação binária.

Assim, se a operação $*$ for associativa temos que a estrutura E é nomeada semi-grupo;

Além disso, se existir um único elemento neutro $e \in E$, tal que $x * e = e * x = x$, para qualquer $x \in E$, E é chamado de monóide;

Se ainda, além dessas duas propriedades operativas, todo elemento de E for simetrizável, isto é, para cada $x \in E$ existir um $x^{-1} \in E$, tal que $x * x^{-1} = x^{-1} * x = e$, diremos que E tem estrutura de grupo.

A.2 A-módulos

Definição A.1 *Um A-módulo é um par (M, φ), onde M é um grupo abeliano e $\varphi : A \times M \longrightarrow M$ é tal que para todo $a, b \in A$ e $m, n \in M$, temos;*

$i)$ $\varphi(ab, m) = \varphi(a, bm)$

$ii)$ $\varphi(a + b, m) = \varphi(a, m) + \varphi(b, m)$

$iii)$ $\varphi(a, m + n) = \varphi(a, m) + \varphi(a, n)$

$iv)$ $\varphi(1, m) = m$

Temos que $a \cdot m$ denota a imagem do par (a, m) pela aplicação φ.
Os elementos do anel A são denominados escalares.

Consideremos o conjunto $\mathcal{L}(M, A)$ das formas A-lineares de M, isto é, o conjunto dos homomorfismos de A-módulos.

$$\mathcal{L}(M, A) = \mathcal{L} = \{u : M \longrightarrow A;\ \text{u é A-linear}\}$$

Para $u, v \in \mathcal{L}$ e $a \in A$ definimos a adição e multiplicação externa por;

$$u + v : M \longrightarrow A, \qquad (u + v)\ \ (m) = u(m) + v(m)$$

$$a \cdot u : M \longrightarrow A, \qquad (a \cdot u)\ \ (m) = a \cdot u(m)$$

obviamente $\mathcal{L}(M, A)$ é um A-módulo, pois $\mathcal{L}$ é um grupo abeliano $u + v = v + u$ e a aplicação $\psi : A \times \mathcal{L} \longrightarrow \mathcal{L}$, dada por $\psi(a, u) = a \cdot u$ é tal que, $\forall\ a, b \in A$ e $u, v \in \mathcal{L}$, temos;

$i)$ $(ab) \cdot u = a(b \cdot u)$

$ii)$ $(a + b) \cdot u = a \cdot u + b \cdot u$

$iii)$ $a \cdot (u + v) = a \cdot u + a \cdot v$

$iv)$ $1 \cdot u = u$

Portanto o par $(\mathcal{L}, \psi)$ é também um A-módulo.

O produto cartesiano de A-módulos é um A-módulo, sendo as operações definidas componente a componente.

No caso em que A é um corpo, o A-módulo M é um A-espaço vetorial. Assim a definição de A-módulo para um anel A qualquer, obtém-se como generalização natural da noção de K-espaço vetorial.

Um submódulo de um A-módulo M é um subconjunto não-vazio N de M tal que;

i) N é um subgrupo de M

ii) Para todo $a \in A$ e $n \in N$, temos $an \in N$

Sejam B um subconjunto de um A-módulo M e

$$\mathcal{N} = \{N \ ; N \text{ é submódulo de } M \text{ e } \ N \supseteq B\}$$

então $\langle B \rangle = \bigcap_{N \in \mathcal{N}} N$ é o menor A-módulo de M contendo B, chamado de A-submódulo gerado por B.

Seja M um A-módulo. Se $m \in M$ pode ser escrito como

$$m = \sum_{i=1}^{n} a_i m_i; \quad a_i \in A \text{ e } m_i \in M$$

diremos que m é uma combinação linear dos elementos $m_1, \ldots, m_n$ sobre A.

Evidentemente, o conjunto de todas as combinações lineares de $m_1, \ldots, m_n$ é o A-submódulo $\langle m_1, \ldots, m_n \rangle = \left\{ \sum_{i=1}^{n} a_i m_i; \ a_i \in A \right\}$ gerado por $m_1, \ldots, m_n$.

Se existir um subconjunto finito B de um A-módulo M, tal que $M = \langle B \rangle$, diremos que M é um A-módulo F.G. (finitamente gerado).

Se $B = \{m\}$, isto é, B é contituído de um único elemento, então o A-módulo $\langle m \rangle = \{am; a \in A\}$ será chamado de A-módulo cíclico gerado por m.

Uma seqüência finita $m_1, \ldots, m_n$ de elementos de um A-módulo M será chamado linearmente independente se a soma $\sum_{i=1}^{n} a_i m_i = 0$ implicar $a_1 = a_2 = \ldots = a_n = 0$. Caso contrário, diremos que a seqüência é linearmente dependente.

Um subconjunto B de um A-módulo M será chamado linearmente independente se qualquer seqüência finita de elementos distintos de B é linearmente independente. Caso contrário, B é dito linearmente dependente.

Um subconjunto B de um A-módulo M será uma A-base se as seguintes condições são satisfeitas;

i) $M = \langle B \rangle$

ii) B é linearmente independente

Um A-módulo M será dito um A-módulo livre se possuir uma A-base.

Quando todas as bases de A forem finitas e tiverem a mesma cardinalidade, chamaremos este número de o posto de A.

Teorema A.2 *Sejam A um Domínio de Ideais Principais e M um A-módulo livre de posto p, então todo A-submódulo N de M é livre com posto $q \leq p$.*

A.2.1 A-álgebras

Cosideremos $f : A \longrightarrow B$ um homomorfismo de anéis, com $a, a' \in A$ e $b, b' \in B$.

Definimos sobre B a seguinte multiplicação $a \cdot b := f(a)b$,

a adição $+ : B \times B \longrightarrow B$, por $+(b, b') = b + b'$

e multiplicação externa $\cdot : A \times B \longrightarrow B$, por $\cdot(a, b) = a \cdot b = f(a) \cdot b$.

Temos que B é um A-módulo, pois

i) $(B, +)$ é um grupo abeliano

ii) $a(a'b) = f(a)(f(a')b) = f(a)f(a')b = f(aa')b = (aa')b$

iii) $(a + a')b = f(a + a')b = (f(a) + f(a'))b = f(a)b + f(a')b = ab + a'b$

iv) $a(b + b') = f(a)(b + b') = f(a)b + f(a)b' = ab + ab'$

v) $1 \cdot b = f(1)b = 1_B b = b$

Nestas condições, dizemos que o A-módulo B é uma A-álgebra.

Vejamos o caso em que $f : A \longrightarrow B$ é a inclusão.

$f : K \longrightarrow B$ é um homomorfismo injetivo, onde K é corpo, então B é uma K-álgebra, isto é, B é um anel que contém uma cópia do corpo K.

Definição A.3 *Uma A-álgebra B é finitamente gerada se existirem $b_1, \ldots, b_n \in B$, tais que $B = A[b_1, \ldots, b_n]$.*

Definição A.4 *Diremos que B é uma A-álgebra finita se B é um A-módulo finitamente gerado.*

Proposição A.5 *Se B é uma A-álgebra finita, então B é uma A-álgebra finitamente gerada.*

Agora, sendo $K \subseteq L$ corpos, temos o seguinte teorema:

Teorema A.6 *Se L é uma K-álgebra finitamente gerada, então L é uma K-álgebra finita.*

A-álgebras são generalizações de A-módulos.

A.3 Extensões de Corpos

Definição A.7 *Dados dois corpos L e K, diremos que L é uma extensão de K ou que L/K é uma extensão de corpos, sempre que K for um subcorpo de L.*

Neste caso, consideramos L como K-espaço vetorial, em relação à operação externa $K \times L \longrightarrow L$, definida como restrição da multiplicação em L. Em outras palavras, $a\alpha$ representa o produto de $a \in K$ por $\alpha \in L$.

A.3.1 Extensões Finitas

A dimensão do K-espaço L é denotada por $[L : K]$ e é chamado de grau de L/K. Obviamente $[L : K] \geq 1$.

Diremos que L/K é uma extensão finita quando $[L : K] < \infty$

Proposição A.8 $[L : K] = 1 \Leftrightarrow L = K$

Prova. $[\Rightarrow$ $[L : K] = 1 \Rightarrow \{1\}$ é um sistema gerador linearmente independente maximal, e portanto, uma base de L/K resulta que todo $\alpha \in L$ é da forma $\alpha = a \cdot 1$, com $a \in K$. Logo $\alpha \in K \Rightarrow L \subset K$, e como $K \subset L \Rightarrow K = L$.

$\Leftarrow]$ $L = K \Rightarrow \forall\ \alpha \in L, \alpha \in K$ e portanto $\{1\}$ é uma base de $L/K \Rightarrow [L : K] = 1$ ■

Dadas duas extensões sucessivas L/K e M/L, obtém-se uma base M/K multiplicando-se os elementos de uma base de L/K pelos de uma base de M/L. De fato

Proposição A.9 *Suponhamos que $\beta_1, \ldots, \beta_n$, respectivamente $\gamma_1, \ldots, \gamma_m$, formam uma base de L/K e, respectivamente de M/L. Então*

$$\beta_1\gamma_1, \ldots, \beta_n\gamma_1, \beta_1\gamma_2, \ldots, \beta_n\gamma_2, \ldots, \beta_1\gamma_m, \ldots, \beta_n\gamma_m$$

formam uma base de M/K.

$$\begin{array}{l} M \\ | \quad = \{\gamma_1, \ldots, \gamma_m\} \\ L \\ | \quad = \{\beta_1, \ldots, \beta_n\} \\ K \end{array} \Rightarrow \begin{array}{l} \{\beta_1, \ldots, \beta_n\} \cdot \{\gamma_1, \ldots, \gamma_m\} = \{\beta_i\gamma_j;\ \ \beta_i \in \text{ base de } L/K \\ \text{e } \gamma_j \in \text{ base de } M/L\} \text{ é uma base de } M/K \end{array}$$

A.3.2 Extensões Algébricas

Definição A.10 *Diremos que a extensão L de K é algébrica se todo elemento $\alpha \in L$ for raiz de algum polinômio não-nulo f em $K[x]$.*

Simbolicamente, L/K é alg. $\Leftrightarrow \forall\ \alpha \in L, \exists\ f \in K[x] \setminus \{0\}; f(\alpha) = 0$.

Caso contrário, se a extensão L de K não for algébrica será chamada de transcedente. Ou seja, se existir um elemento $\alpha \in L$ que não seja raiz de qualquer polinômio

não-nulo f em $K[x]$.

Simbolicamente, L/K é transc. $\Leftrightarrow \exists\ \alpha \in L;\ \forall\ f \in K[x] \setminus \{0\},\ f(\alpha) \neq 0$.

Definição A.11 *Diremos que um polinômio não-nulo $f \in K[x]$ é separável se for possível fatorá-lo em polinômios lineares distintos em algum corpo que contenha K.*

Por exemplo, $f = x^3 - 2 \in \mathbb{Q}[x]$ e $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta)(x - \sqrt[3]{2}\zeta^2)$, onde ζ é uma raiz cúbica da unidade. Assim o corpo de decomposição de f, $\mathbb{Q}(\sqrt[3]{2}, \zeta)$, é uma extensão cúbica de $\mathbb{Q}$.

Diremos que um elemento α é separável quando for raiz de algum polinômio separável.

A.3.3 Extensões Separáveis

Definição A.12 *Diremos que uma extensão L de K é separável quando todos seus elementos $\alpha \in L$ forem separáveis.*

Teorema A.13 *Seja K um corpo finito ou de característica zero, L uma extensão finita de K de grau n e Ω um corpo algebricamente fechado contendo K. Então existem n K-isomorfismos distintos de L em Ω.*

Corolário A.14 *[Teorema do elemento primitivo] Sejam K um corpo finito ou de característica zero, L uma extensão finita de K de grau n. Então existe um elemento $\alpha \in L$, tal que $L = K(\alpha)$. Nestas condições α é chamado de Elemento Primitivo.*

A.3.4 Extensões Normais

Definição A.15 *Diremos que uma extensão N/K é normal se, para todo $\alpha \in N$, $P_{\alpha/K}$(polinômio minimal do elemento α) se fatorar completamente em polinômios lineares em $N[x]$.*

Ou seja, N é um corpo de decomposição dos polinômios minimais. O que equivale a dizer que se uma raiz de $P_{\alpha/K}$ está em N, então todas as raízes de $P_{\alpha/K}$ estão em N.

A.3.5 Extensões Galoisianas

Definição A.16 *Diremos que uma extensão L/K é de Galois se L for um corpo de raízes de um polinômio separável.*

Ou seja, L/K é uma extensão galoisiana se L é simultaneamente uma extensão normal e separável de K.

A.3.6 Extensões Ciclotômicas

Definição A.17 *Diremos que a extensão L/K é ciclotômica, se $L = K(\zeta)$, onde ζ é uma raiz primitiva n-ésima da unidade.*

Uma exposição mais detalhada de corpos ciclotômicos encontra-se no capítulo 1.

A.4 Elemento algébrico sobre um corpo

Seja L um corpo e K um subcorpo de L. Por um elemento algébrico entendemos qualquer $\alpha \in L$ que é algébrico sobre K, isto é, existem $a_0, a_1, \ldots, a_n \in K$, tais que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, ou seja α é raíz de um polinômio em $K[x]$.

O fecho algébrico de K em L, $A_L(K) = \Omega$, é o conjunto constituído de elementos de L que são algébricos sobre K, pois L pode conter elementos não algébricos sobre K.

Diremos que um corpo K é algebricamente fechado em L quando o conjunto de todos os elementos de L que são raízes de algum polinômio com coeficientes em K é o próprio K.

$A_L(\Omega) = \Omega$ um fecho algébrico é algebricamente fechado, e também é maximal, no sentido de que não existe nenhuma extensão algébrica de K que o contenha.

Assim uma extensão L/K é algébrica se, e somente se $A_L(K) = L$ e um subcorpo K é algebricamente fechado em L se todo polinômio não constante $p(x) \in K[x]$ se decompõe em fatores do primeiro grau em $K[x]$, ou equivalentemente, se $\Omega = K$.

Para qualquer extensão algébrica L de $\mathbb{C}$, temos $A_L(\mathbb{C}) = \mathbb{C} = L$, isto é, o corpo dos complexos é algebricamente fechado (teo. fund. da Álgebra, 1798, C. Gauss), mas nem para todo subcorpo K de $\mathbb{C}$ vale a igualdade $A_{\mathbb{C}}(K) = \mathbb{C}$, isto é, $\mathbb{C}$ não é um fecho algébrico, pois $\mathbb{C}$ é uma extensão transcedente de $\mathbb{Q}$.

Lema A.18 *Se K é corpo, então todo ideal do anel $K[x]$ é principal, isto é, $K[x]$ é um domínio de ideais principais.*

Teorema A.19 *Seja $\alpha \in L \supseteq K$. As seguintes condições são equivalentes;*

i) α é algébrico sobre K

ii) $K[\alpha]$ é um corpo

iii) $K(\alpha)/K$ é uma extensão finita

Este teorema afirma que se $\alpha \in L$ e existe um polinômio de grau n, $f(x) \in K[x]$, tal que $f(\alpha) = 0$, então o conjunto

$$K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \ \ ; a_1, \ldots, a_n \text{ percorrem todo } K\}$$

é um corpo. E isto implica que o corpo de frações $K(\alpha) = \left\{ \dfrac{f(\alpha)}{g(\alpha)} \ \ ; f, g \neq 0 \in K[\alpha] \right\}$ é uma extensão finita de K e isso, por sua vez, é condição necessária para $\alpha \in L$ ser um

elemento algébrico sobre K. Neste caso, $P_{\alpha|K}$ que é irredutível sobre K gera $\langle P_{\alpha|K}\rangle$, um ideal maximal de $K[x]$, $K[\alpha] = K(\alpha)$, e os elementos $1, \alpha, \ldots, \alpha^{n-1}$ formam uma base da extensão $K(\alpha)$ de K, sendo $n = \partial P_{\alpha|K} = [K(\alpha) : K]$.

Prova. i) $\Rightarrow$ ii)
Seja o homomorfismo $\varphi_\alpha : K[x] \longrightarrow K[\alpha]$, dado por $\varphi_\alpha(f) = f(\alpha)$.

Então $\ker \varphi_\alpha = \{f \in K[x] \ \ ; f(\alpha) = 0\} = \langle P_{\alpha|K}\rangle = \mathfrak{I}_{\alpha,K}$, pois $K[x]$, por A.18, é um DIP e se $\alpha \in L$ é algébrico sobre K, então existe, conforme lema A.22, um polinômio mônico irredutível em $K[x]$ que se anula em α.
Como o polinômio gerador de $\mathfrak{I}_{\alpha,K}$ é irredutível sobre K, então $\mathfrak{I}_{\alpha,K}$ é um Ideal primo, e todo ideal primo num domínio de ideais principais é maximal.

Logo, $\dfrac{K[x]}{\mathfrak{I}_{\alpha,K}} \simeq Im\ \varphi_\alpha = K[\alpha]$. E portanto $K[\alpha]$ é corpo.

ii) $\Rightarrow$ iii)
$K[\alpha] \subseteq K(\alpha)$ e $K(\alpha)$ é o menor corpo que contém K e α que é algébrico sobre K, então $K(\alpha) \subset K[\alpha]$, daí $K(\alpha) = K[\alpha]$.
Seja $n = \partial P_{\alpha/K}$. Os elementos $1, \alpha, \ldots, \alpha^{n-1}$ são linearmente independentes sobre K, pois não existe nenhum $g \in \mathfrak{I}_{\alpha,K} \setminus \{0\}$, com $\partial g < n$.
Seja $\gamma \in K[\alpha]$, digamos $\gamma = h(\alpha)$, com $h \in K[x]$.
Pelo algoritmo da divisão, existem únicos $q, r \in K[x]$,tais que $h = qP_{\alpha/K} + r$, com $r = 0$ ou $\partial r < n$, então $h(\alpha) = q(\alpha)P_{\alpha/K}(\alpha) + r(\alpha)$.
temos $h(\alpha) = r(\alpha) \in K + K\alpha + \ldots + K\alpha^{n-1}$, ou seja $\gamma \in \sum_{i=0}^{n-1} K\alpha^i$ e portanto $1, \alpha, \ldots, \alpha^{n-1}$ formam um sistema de geradores K-lineares, logo uma base de $K(\alpha)/K$, em particular $[K(\alpha) : K] = n$.

iii) $\Rightarrow$ i)
$K(\alpha)/K$ é finito $\Rightarrow$ α é algébrico sobre K.
Suponha α transcedente sobre K, isto é, $f(\alpha) \neq 0$ para qualquer que seja o polinômio não-nulo $f \in K[x]$.
Considere o conjunto $\{1, \alpha, \ldots, \alpha^n, \ldots\}$ das potências de α e tome um subconjunto finito qualquer, digamos $\{\alpha^{m_1}, \alpha^{m_2}, \ldots, \alpha^{m_r}\}$.
Com $a_1, a_2, \ldots, a_r \in K$, a equação $a_1\alpha^{m_1} + a_2\alpha^{m_2} + \cdots + a_r\alpha^{m_r} = 0$ se, e somente se $a_1 = a_2 = \cdots = a_r = 0$, pois α é transcedente sobre K.
Isso implica em dizer que o subconjunto tomado é linearmente independente, e como é parte qualquer, significa dizer que o conjunto inicial é também L.I., isto é, $\{\alpha^i \ \ ; i \in \mathbb{N}\}$ é um sistema linearmente independente e infinito e portanto $[K(\alpha) : K] = \infty$ ■

A.5 Elemento inteiro sobre um anel

Sejam A um anel e R um subanel de A.

Diremos que um elemento $\alpha \in A$ é inteiro sobre R, se existirem $a_0, a_1, \ldots, a_{n-1}$ pertencentes a R, tais que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, isto é, α é raíz de um polinômio mônico em $R[x]$.

Obviamente todo elemento de R é inteiro sobre R.

No caso em que $A = \mathbb{C}$ e $R = \mathbb{Z}$, os elementos inteiros sobre $\mathbb{Z}$ serão chamados de inteiros algébricos.

Por exemplo; $i = \sqrt{-1}$, $\sqrt[7]{12}$, $e^{\frac{2\pi}{n}i}$, $\dfrac{1+\sqrt{5}}{2}$ são inteiros algébricos, pois são raízes dos seguintes polinômios; x^2+1, x^7-12, x^n-1, e $x^2-x+1 \in \mathbb{Z}[x]$,respectivamente.

O fecho inteiro de R em A, $I_A(R)$, é o conjunto constituído de elementos de A que são inteiros sobre R, pois A pode conter elementos não-inteiros sobre R.

Diremos que um anel R é inteiramente (ou integralmente) fechado em A quando o conjunto de todos os elementos de A que são raízes de algum polinômio mônico com coeficientes em R é o próprio R.

$I_A(I_A(R)) = I_A(R)$ um fecho inteiro é integralmente fechado, e também é maximal, no sentido de que não existe nenhuma extensão inteira de R que o contenha.

Assim uma extensão A/R é inteira se, e somente se $I_A(R) = A$ e um subanel R é integralmente fechado em A se todo polinômio mônico não constante $p(x) \in R[x]$ se decompõe em fatores do primeiro grau em $R[x]$, ou equivalentemente, se $I_A(R) = R$.

O seguinte resultado relaciona a propriedade de um elemento ser inteiro sobre R com a propriedade de um certo R-módulo, um submódulo do R-módulo A, ser finitamente gerado.

Teorema A.20 *Para qualquer $\alpha \in A$ as seguintes condições são equivalentes;*

i) α é inteiro sobre R

ii) $R[\alpha]$ é um R-módulo F.G.

Prova. i) $\Rightarrow$ ii)
α é raíz de um polinômio $f = a_0 + a_1 + \cdots + a_{n-1}x^{n-1} + x^n \in R[x]$ isto é

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \qquad (*)$$

Seja o R-módulo F.G.

$$M = R + R\alpha + \cdots + R\alpha^{n-1}$$

isto é $\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle = M$ obviamente

$$M \subseteq R[\alpha] \qquad (1).$$

$\forall m \in \mathbb{N}$, temos que $\alpha^m \in R[\alpha]$, sabemos que $\alpha, \alpha^2, \ldots, \alpha^{n-1} \in M$ por $(*)$

$$\begin{aligned}
&\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \in M\\
&\alpha^{n+1} = \alpha^n\alpha = -(a_{n-1}\alpha^{n-1}\alpha + \cdots + a_1\alpha\alpha + a_0\alpha) \in M\\
&\alpha^{n+2} = \alpha^n\alpha^2 = -(a_{n-1}\alpha^{n-1}\alpha^2 + \cdots + a_1\alpha\alpha^2 + a_0\alpha^2) \in M\\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots\\
&\alpha^{n+(n-1)} = \alpha^n\alpha^{n-1} = -(a_{n-1}\alpha^{n-1}\alpha^{n-1} + \cdots + a_1\alpha\alpha^{n-1} + a_0\alpha^{n-1}) \in M\\
&\alpha^{n+n} = \alpha^n\alpha^n = -(a_{n-1}\alpha^{n-1}\alpha^n + \cdots + a_1\alpha\alpha^n + a_0\alpha^n) \in M\\
&\alpha^{n+k} = \alpha^n\alpha^k, \text{ onde } k > n
\end{aligned}$$

Pelo algoritmo da divisão $k, n \in \mathbb{N}$, com $n < k$ então $\exists\exists!$ q, r tais que $k = nq + r$, com $0 \leq r < n$. Então

$$\alpha^n \alpha^k = \alpha^n \alpha^{nq+r} = \alpha^n \alpha^{nq} \alpha^r$$

Sabemos que $\alpha^r \in M$ e $\alpha^{nq} = (\alpha^n)^q \in M$, pois $\alpha^n \in M$, ou seja, $\alpha^{n+k} \in M$, para qualquer $k > 0$, isto é, $\forall m \in \mathbb{N}$, $\alpha^m \in M$. Logo

$$R[\alpha] \subseteq M \qquad (2)$$

e de (1) e (2) temos a igualdade $R[\alpha] = M$.

ii) $\Rightarrow$ i)
$R[\alpha]$ é um R-módulo F.G., sejam $\alpha_1, \ldots, \alpha_n \in R[\alpha] \subseteq A$, tais que $R[\alpha] = R\alpha_1 + \cdots + R\alpha_n$
Como $\alpha \in R[\alpha]$, temos que $\alpha\alpha_i \in R[\alpha]$, $i = 1, \ldots, n$

$$\begin{cases} \alpha\alpha_1 = a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n & \text{com } a_{ij} \in R,\ j = 1, \ldots, n \\ \alpha\alpha_2 = a_{21}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n \\ \vdots \qquad\qquad\qquad \vdots \\ \alpha\alpha_n = a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + a_{nn}\alpha_n \end{cases}$$

Logo, $\exists a_{ij} \in R$, com $\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, $\forall i = 1, \ldots, n$

$$\begin{aligned} (a_{11} - \alpha)\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n &= 0 \\ a_{21}\alpha_1 + (a_{22} - \alpha)\alpha_2 + \cdots + a_{2n}\alpha_n &= 0 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + (a_{nn} - \alpha)\alpha_n &= 0 \end{aligned}$$

$$\sum_{j=1}^{n} a_{ij}\alpha_j - \alpha\alpha_i = 0 \Rightarrow \sum_{j=1}^{n} (a_{ij} - \delta_{ij}\alpha)\alpha_j = 0, \qquad \delta_{ij} = \begin{cases} 0, \text{ se } i \neq j \\ 1, \text{ se } i = j \end{cases}$$

Assim a matriz $M = (a_{ij} - \delta_{ij}\alpha) \in M_n(R[\alpha])$, desta forma o sistema $Mx = 0$ tem solução não-nula $(\alpha_1, \ldots, \alpha_n) \in R[\alpha]$, logo $\det M = 0$.
Note que na matriz M o elemento α está em sua diagonal principal assim o det de M e um polinômio mônico em α de grau n, pois os termos fora da diagonal principal são constantes $a_{ij}\alpha_j \in R[\alpha]$.
Veja a contrução do polinômio característico na próxima seção. Este é o chamado truque determinantal de Nakayama.

$$\det M = \prod_{i=1}^{n} (a_{ii} - \alpha)\alpha_i + \text{ termos de menor grau em } \alpha = f(\alpha) \in R[\alpha],$$

com $f \in R[x]$ mônico de grau n.
Daí $f(\alpha) = 0$, isto é, α é inteiro sobre R. ■

Corolário A.21 *Se $\alpha_1, \ldots, \alpha_m \in A$ forem inteiros sobre R, então $R[\alpha_1, \ldots, \alpha_m]$ será um R-módulo finitamente gerado.*

Prova. $R_0 = R$ tem posto 1, como R-módulo, logo é F.G.
$R_1 = R[\alpha]$ é F.G.
Supor $R_k = R[\alpha_1, \alpha_2, \ldots, \alpha_k]$ considerado como R-módulo possua um sistema finito $\beta_1, \ldots, \beta_r$ de geradores.
Como α é inteiro sobre R, α_2 é inteiro sobre $R_1, \ldots$, α_{k+1} é inteiro sobre R_k. O anel $R_{k+1} = R[\alpha_1, \ldots, \alpha_{k+1}] = R_k[\alpha_{k+1}]$ considerado como R_K-módulo possui um sistema finito de geradores $\gamma_1, \ldots, \gamma_s$; logo, considerado como R-módulo, é gerado pelos produtos $\beta_i\gamma_j$ $(i = 1, \ldots, r$ e $j = 1, \ldots, s)$ e portanto por indução concluimos que $R_m = R[\alpha_1, \ldots, \alpha_m]$ é um R-módulo F.G. qualquer que seja $m \in \mathbb{N}$ ■

No caso em que $R = \mathbb{Z}$, temos que se α é inteiro sobre $\mathbb{Z}$ o $\mathbb{Z}$-módulo $\mathbb{Z}[\alpha]$ é finitamente gerado e que se $\alpha_1, \ldots, \alpha_m \in A$ forem inteiros algébricos, então o anel $\mathbb{Z}[\alpha_1, \ldots, \alpha_m]$ é F.G. como $\mathbb{Z}$-módulo.

Lema A.22 *Se $\alpha \in L \supseteq K$ é algébrico sobre K, então α é inteiro sobre $K[\alpha]$, isto é, existe um polinômio mônico irredutível $p(x) \in K[x]$ tendo α como raíz, $p(\alpha) = 0$.*

Proposição A.23 *[Ste] Um número algébrico α é um inteiro algébrico se, e somente se seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.*

Proposição A.24 *[Ste] Um inteiro algébrico é um número racional se, e somente se é um inteiro. Equivalentemente $I_A \cap \mathbb{Q} = \mathbb{Z}$.*

A.6 Polinômio Característico, Norma e Traço

Seja K uma extensão finita de $\mathbb{Q}$, $[K : \mathbb{Q}] = n$. A seguir associamos a cada elemento $\alpha \in K$ o seu polinômio característico e este será contruído usando-se uma base qualquer.

Seja $\{\beta_1, \beta_2, \ldots, \beta_n\}$ uma base de K/$\mathbb{Q}$, para cada $\alpha \in K$ existem $a_{ij} \in \mathbb{Q}$ tais que $\alpha\beta_i = \sum_{j=1}^{n} a_{ij}\beta_j$

Colocando esse sistema de igualdade em forma matricial temos:

$$\alpha \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$$

O polinômio característico do elemento α em relação à extensão K/$\mathbb{Q}$ é o determinante da matriz $(xI - (a_{ij}))$, com $i, j \in \{1, 2, ..., n\}$.

$$F_{\alpha, K/\mathbb{Q}} = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} \in \mathbb{Q}[x]$$

Obs$_1$: O polinômio mônico $F_{\alpha,\ K/\mathbb{Q}}$ independe da escolha da base $\{\beta_1, \beta_2, \ldots, \beta_n\}$, e tem α como raiz, i.é. $F_{\alpha,\ K/\mathbb{Q}}(\alpha)$=0

Da matriz $C = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ podemos extrair;

o traço e a norma do elemento α em relacão à extensão $K/\mathbb{Q}$, que são definidos como sendo

$$\mathcal{T}_{K/\mathbb{Q}}(\alpha) \ = \Sigma a_{ii}, \quad e \ \ \mathcal{N}_{K/\mathbb{Q}}(\alpha) = det(C)$$

O traço e a norma de um elemento $\alpha \in K$ são, a menos de sinal, o segundo e o último coeficientes, respectivamente, do seu polinômio característico.

Seja $F_{\alpha,\ K/\mathbb{Q}} = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$a_{n-1} = -\mathcal{T}_{K/\mathbb{Q}}(\alpha)$ $\qquad$ $a_0 = (-1)^n \mathcal{N}_{K/\mathbb{Q}}(\alpha)$

Particularmente, para $n = 2$, temos $F_{\alpha,\ K/\mathbb{Q}} = x^2 - \mathcal{T}_{K/\mathbb{Q}}(\alpha)x + \mathcal{N}_{K/\mathbb{Q}}(\alpha)$

Se K é uma extensão separável de $\mathbb{Q}$ e $\sigma_1, \sigma_2, \ldots, \sigma_n$ são os $\mathbb{Q}-$isomorfismos de K em Ω(corpo algebricamente fechado que contém K), onde $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ são as n raízes distintas do polinômio característico, então;

a) O polinômio característico é expresso na forma

$$F_{\alpha,\ K/\mathbb{Q}} = x^n + \sum_{j=0}^{n} (-1)^j S_j(\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)) x^{n-j} \in \mathbb{Z}[x]$$

onde S_j é o j-ésimo polinômio símétrico elementar em n indeterminadas.

b) O traço do elemento α em relação à extensão $K/\mathbb{Q}$ é a soma das raízes do polinômio característico $F_{\alpha,\ K/\mathbb{Q}}$.

$$\mathcal{T}_{K/\mathbb{Q}}(\alpha) \ = \sum_{i=1}^{n} \sigma_i(\alpha)$$

.

c) A norma do elemento α em relação à extensão $K/\mathbb{Q}$ é o produto das raízes do polinômio característico $F_{\alpha,\ K/\mathbb{Q}}$.

$$\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=n}^{n} \sigma_i(\alpha)$$

O polinômio minimal,denotado por $P_{\alpha/\mathbb{Q}}$, está relacionado com o polinômio característico da seguinte maneira.

$F_{\alpha,\mathbb{Q}(\alpha)/\mathbb{Q}}$=$P_{\alpha/\mathbb{Q}}$ $\Rightarrow \partial P_{\alpha/\mathbb{Q}}$=$[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Seja a torre de corpos $\begin{array}{c} L \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$ com $[L : \mathbb{Q}] < \infty$, para todo $\alpha \in K$, $F_{\alpha,L/\mathbb{Q}} = F_{\alpha,\ K/\mathbb{Q}}^{[L:K]}$

Sendo $K = \mathbb{Q}(\alpha)$, $F_{\alpha,L/\mathbb{Q}} = P_{\alpha/\mathbb{Q}}{}^{[L:\ \mathbb{Q}(\alpha)]}$.

Escrevendo $\mathcal{T}$ e $\mathcal{N}$ no lugar de $\mathcal{T}_{K/\mathbb{Q}}$ e $\mathcal{N}_{K/\mathbb{Q}}$, temos para todo $\alpha, \beta \in K$ e $a \in \mathbb{Q}$ as seguintes propriedades;

i) $\mathcal{T}(\alpha + \beta) = \mathcal{T}(\alpha) + \mathcal{T}(\beta)$

ii) $\mathcal{T}(a\alpha) = a\mathcal{T}(\alpha)$

iii) $\mathcal{N}(\alpha.\beta) = \mathcal{N}(\alpha).\mathcal{N}(\beta)$

iv) $\mathcal{T}(a) = na$ e $\mathcal{N}(a) = a^n$, onde n é o grau do polinômio $F_{\alpha,\ K/\mathbb{Q}}$.

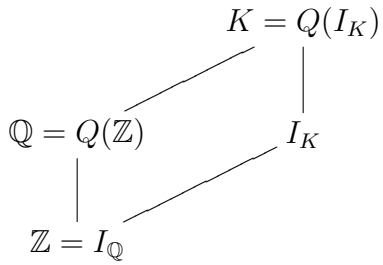
De i e ii temos que $\mathcal{T}$ é uma aplicação linear.

A.7 Anel dos inteiros Algébricos

Considera-se além do corpo $K = \mathbb{Q}(\alpha)$ um certo subanel distinguido I_K de K, denominado anel dos inteiros algébricos de K, com corpo de frações igual a K, que entretanto nem sempre é da forma $\mathbb{Z}[\alpha]$.

O estudo desse anel, cujo papel relativo a K é análogo ao de $\mathbb{Z}$ em relação a $\mathbb{Q}$, pode ser considerado, segundo o prof. Otto Endler, o objetivo principal da Teoria dos Números Algébricos.

.



Sendo A um anel e R um subanel de A pretendemos mostrar que o conjunto dos elementos de A que são inteiros sobre R formam um subanel $I_A(R)$ de A. Para provar que a diferença e respectivamente o produto de dois elementos $\alpha, \beta \in A$ inteiros sobre R são também inteiros sobre R, basta construir, a partir de polinômios mônicos $f, g \in \mathbb{Z}[x]$, tais que $f(\alpha) = g(\beta) = 0$, dois polinômios mônicos $d, p \in \mathbb{Z}[x]$, tais que $d(\alpha - \beta) = 0$ e $p(\alpha\beta) = 0$. Tal construção é viável somente em casos bem simples, vejamos então o caso geral.

Teorema A.25 *$I_A(R)$ é um subanel de A que contém R.*

Prova. De fato, $R \subseteq I_A(R) \subseteq A$ e sejam $\alpha, \beta \in I_A(R)$. Então $\alpha - \beta$, $\alpha\beta \in R[\alpha, \beta]$ e pelo corolário A.21 $R[\alpha, \beta]$ é um R-módulo F.G. Logo, pelo Teorema A.20, $\alpha - \beta$, $\alpha\beta \in I_A(R)$ ■

Temos também a maximalidade de $I_A(R)$, no sentido de que qualquer subanel de A, que é um R-módulo finitamente gerado, estará nele contido, isto é;

Corolário A.26 *Todo subanel S de K, que é um $\mathbb{Z}$-módulo F.G., está contido em I_K.*

A propriedade de ser inteiro é transitiva no seguinte sentido

Proposição A.27 *Seja A um anel, R um subanel de A e S um subanel de R, são equivalentes;*

i) A é inteiro sobre R e R é inteiro sobre S

ii) A é inteiros sobre S.

O nome fecho inteiro se justifica pelo fato de $I_A(\ )$ ser uma operação de fecho no seguinte sentido

Seja $\mathcal{R}$ o conjunto dos subanéis de A. Por $R \rightsquigarrow I_A(R)$ é definida uma operação de $\mathcal{R}$ em $\mathcal{R}$, tal que para todo $R, S \in \mathcal{R}$;

a) $R \subseteq I_A(R) \subseteq A$

b) $I_A(I_A(R)) = I_A(R)$

c) $S \subseteq R \Rightarrow I_A(S) \subseteq I_A(R)$.

No caso $A = \mathbb{Q}$, o anel $I_A(\mathbb{Z}) = I_{\mathbb{Q}}(\mathbb{Z}) = I_{\mathbb{Q}}$ coincide com o anel $\mathbb{Z}$ dos números inteiros racionais. Isto é uma consequência imediata do seguinte teorema

Teorema A.28 *Todo domínio fatorial é integralmente fechado no seu corpo de frações.*

Prova. Todo $0 \neq \alpha \in K = Q(R)$ pode ser escrito na forma $\alpha = ab^{-1}$

$$a, b \in R \quad \text{e} \quad mdc(a,b) = 1$$

se $\alpha \in I_K(R)$, então existem $c_1, \ldots, c_m \in R$, tais que

$$\begin{aligned}
&\alpha^m + c_1\alpha^{m-1} + \cdots + c_{m-1}\alpha + c_m = 0 \\
&\alpha^m b^m + c_1 b^m \alpha^{m-1} + \cdots + c_{m-1} b^m \alpha + b^m c_m = 0 \\
&a^m + c_1 b a^{m-1} + \cdots + c_{m-1} b^{m-1} a + c_m b^m = 0 \\
&a^m = b(-c_1 a^{m-1} - \cdots - c_{m-1} b^{m-2} a = c_m b^{m-1}) \Rightarrow b | a^m
\end{aligned}$$

Mas $mdc(a,b) = 1 \Rightarrow b \in U(R) \Rightarrow \alpha = ab^{-1} \in R \ \therefore \ I_K(R) = R$ ■

Supondo $A = L$ um corpo e R um subanel de A, estudaremos o corpo das frações do anel $I_L(R)$.

Teorema A.29 *Seja R um subanel do corpo L. Então o fecho inteiro do corpo de frações de R em L é o corpo de frações do fecho inteiro de R em L, simbolicamente*

$$Q(I_L(R)) = I_L(Q(R))$$

Em particular, $Q(I_L(R)) = L$ se, e somente se L for algébrico sobre $Q(R)$.

Prova. Seja $\gamma \in Q(I_L(R))$, digamos $\gamma = \alpha\beta^{-1}$, onde $\alpha, \beta \in I_L(R)$. Como $I_L(Q(R))$ é um subcorpo de L contendo $I_L(R)$, $I_L(R) \subseteq I_L(Q(R)) \subseteq L$ temos que

$$\gamma \in I_L(Q(R)) \Rightarrow Q(I_L(R)) \subseteq I_L(Q(R)) \qquad (1)$$

Para qualquer $\gamma \in I_L(Q(R))$ existem $\frac{b_1}{c_1}, \frac{b_2}{c_2}, \ldots, \frac{b_m}{c_m}$, tais que

$$\gamma^m + \frac{b_1}{c_1}\gamma^{m-1} + \cdots + \frac{b_{m-1}}{c_{m-1}}\gamma + \frac{b_m}{c_m} = 0 \qquad (*)$$

Seja $d = c_1 c_2 \cdots c_m \neq 0$. Multiplicando a equação (*) por dd^{-1}, temos

$$\gamma^m + \underbrace{b_1 c_2 c_3 \cdots c_m}_{a_1} d^{-1}\gamma^{m-1} + \cdots + \underbrace{b_{m-1} c_1 \cdots c_{m-2} c_m}_{a_{m-1}} d^{-1}\gamma + \underbrace{b_m c_1 c_2 \cdots c_{m-1}}_{a_m} d^{-1} = 0$$

$$\Rightarrow \gamma^m + a_1 d^{-1}\gamma^{m-1} + \cdots + a_{m-1} d^{-1}\gamma + a_m d^{-1} = 0 \quad \text{com } a_1, \ldots, a_m \in R \quad (**)$$

Multiplicando (**) por d^m, temos

$$(d\gamma)^m + a_1(d\gamma)^{m-1} + a_2 d(d\gamma)^{m-2} + \cdots + a_{m-2} d^{m-3}(d\gamma)^2 + a_{m-1} d^{m-2}(d\gamma) + a_m d^{m-1} = 0$$

$$\Rightarrow d\gamma \in I_L(R) \Rightarrow \gamma \in \frac{I_L(R)}{d} \Rightarrow \gamma \in (I_L(R))_{R\setminus\{0\}} \Rightarrow \gamma \in Q(I_L(R))$$
$$\Rightarrow I_L(Q(R)) \subseteq Q(I_L(R)) \qquad (2)$$

e de (1) e (2) temos a igualdade $Q(I_L(R)) = I_L(Q(R))$ ■

Agora se L é algébrica sobre $Q(R) \Leftrightarrow I_L(Q(R)) = L$.

Daí $Q(I_L(R)) = L$ se, e somente se L é algébrica sobre $Q(R)$.

Aplicando A.29 ao caso em que L é um corpo de números algébricos obtemos o seguinte

Corolário A.30 *Um corpo de números se identifica com o corpo de frações do seu anel dos inteiros. Isto é*

$$Q(I_L) = L, \quad \textit{qualquer que seja o corpo de números algébricos } L.$$

Dados um corpo L qualquer e um subanel R de L, consideramos, para todo elemento $\gamma \in I_L(R)$, o seu polinômio minimal $P_{\gamma/K}$ sobre $K = Q(R)$. Apesar de γ ser raíz de algum polinômio mônico $f \in R[x]$, não podemos afirmar, em geral, que $P_{\gamma/K} \in R[x]$. A este respeito podemos mostrar apenas o seguinte

Teorema A.31 *Seja R um subanel de L e seja $K = Q(R)$.*

a) *Se f, g forem polinômios mônicos em $K[x]$ e $fg \in R[x]$, então $f, g \in I_K(R)[x]$*

b) *Para qualquer $\gamma \in I_L(R)$ temos que $P_{\gamma/K} \in I_K(R)[x]$.*

Prova. a) Existem $\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n \in \Omega$ (fecho algébrico de L, $A_{\mathbb{C}}(L)$) tais que

$$f = \prod_{i=1}^{m}(x - \alpha_i) \quad \text{e} \quad g = \prod_{j=m+1}^{n}(x - \alpha_j)$$

Então fg também é mônico.

$$De \quad fg = (x - \alpha_1)\cdots(x - \alpha_m)(x - \alpha_{m+1})\cdots(x - \alpha_n) \in R[x]$$

temos que $fg(\alpha_i) = 0$ para $i = 1, 2, \ldots, n$, logo

$$\alpha_i \in I_\Omega(R) \qquad (1)$$

Então existem $a_1, a_2, \ldots, a_n \in R$ tais que

$$\alpha_i^n + a_1\alpha_i^{n-1} + \cdots + a_{n-1}\alpha_i + a_n = 0$$

$$a_{n-1}\alpha_i = -\alpha_i^n - a_1\alpha_i^{n-1} - \cdots - a_{n-2}\alpha_i^2 - a_n$$

$$\alpha_i = -\frac{1}{a_{n-1}}\alpha_i^n - \frac{a_1}{a_{n-1}}\alpha_i^{n-1} - \cdots - \frac{a_{n-2}}{a_{n-1}}\alpha_i^2 - \frac{a_n}{a_{n-1}}$$

Logo $\alpha_i \in K \qquad (2)$

Note que fg é um polinômio mônico e como tal

$$fg = x^n - \left(\sum_{i=1}^{n} \alpha_i\right) x^{n-1} + \left(\sum_{\substack{i=1\\j=2\\i\neq j}}^{\substack{n\\n-1}} \alpha_i\alpha_j\right) x^{n-2} - \left(\sum_{\substack{i=1\\j=2\\k=3\\i\neq j\neq k}}^{\substack{n\\n-1\\n-2}} \alpha_i\alpha_j\alpha_k\right) x^{n-3} + \cdots + (-1)^n \left(\prod_{i=1}^{n} \alpha_i\right)$$

Seus coeficientes são combinações de suas raízes.
Portanto de (1) e (2) os coeficientes de f e g estão em $I_\Omega(R) \cap K$ ou seja $f, g \in I_K(R)[x]$.

b) $\gamma \in L$ é raíz de um polinômio mônico $h \in R[x]$, $h(\gamma) = 0$.
Logo existe um polinômio mônico $q \in K[x]$, tal que $h = qP_{\gamma/K}$.
Pelo item a) $q, P_{\gamma/K} \in K[x]$ e $qP_{\gamma/K} \in R[x]$. Então $q, P_{\gamma/K} \in I_K(R)[x]$. ■

Diremos que um domínio R é integralmente fechado se for integralmente fechado no seu corpo de frações isto é, $I_K(R) = R$, com $K = Q(R)$.

Neste caso podemos simplificar o Teorema A.31 substituindo $I_K(R)[x]$ por $R[x]$.

Corolário A.32 *Seja R um domínio integralmente fechado, L uma extensão finita de $K = Q(R)$, S um subanel de $I_L(R)$ que contém R. Para qualquer $\gamma \in S$ temos que;*

a) $F_{\gamma,L/K}$, $P_{\gamma/K} \in R[x]$ *e* $\mathcal{T}_{L/K}(\gamma), \mathcal{N}_{L/K}(\gamma) \in R$

b) $\mathcal{N}_{L/K}(\gamma)$ *é um múltiplo de* γ *no anel* S

c) $\gamma \in U(S)$ *se, e somente se* $\mathcal{N}_{L/K}(\gamma) \in U(R)$

d) *Se* $\mathcal{N}_{L/K}(\gamma)$ *for irredutível em* R*, então será irredutível em* S*.*

Prova. a) Sem perda de generalidade podemos supor que $\gamma \neq 0$ e do item b) do Teorema A.31 temos $P_{\gamma/K} \in R[x]$ e da igualdade

$$F_{\gamma,L/K} = P_{\gamma/K}^m, \quad \text{onde} \quad m = [L : K(\gamma)]$$

b) Como

$$F_{\gamma,L/K} = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$$

e que $a_{n-1} = -\mathcal{T}_{L/K}(\gamma)$ e $a_0 = (-1)^n \mathcal{N}_{L/K}(\gamma)$, mas

$$a_0 = -\gamma^n - a_{n-1}\gamma^{n-1} - \cdots - a_1\gamma = \gamma(-\gamma^{n-1} - a_{n-1}\gamma^{n-2} - \cdots - a_1)$$

$$\therefore \quad \mathcal{N}_{L/K}(\gamma) = \gamma(-1)^{n-1}(\gamma^{n-1} + a_{n-1}\gamma^{n-2} + \cdots + a_1)$$

c) Se $\gamma\delta = 1$, com $\delta \in S$, então $\mathcal{N}_{L/K}(\gamma)\mathcal{N}_{L/K}(\delta) = 1$, onde $\mathcal{N}_{L/K}(\delta) \in R$, por b) $\exists \beta \in S$ tal que $\mathcal{N}_{L/K}(\gamma) = \gamma\beta$.
Se $\mathcal{N}_{L/K}(\gamma) \in U(R)$, então $\beta\mathcal{N}_{L/K}^{-1}(\gamma) = \gamma^{-1}$ é o inverso de γ em S.

d) Resulta de c) e da multiplicatividade da norma ■

Reformulamos A.32 no caso especial em que $R = \mathbb{Z}$, observando que $\mathbb{Z}$ é integralmente fechado e está contido em qualquer subanel de I_L e que $U(\mathbb{Z}) = \{-1, 1\}$.

Corolário A.33 *Sejam L um corpo de números algébricos e S um subanel de I_L. Para qualquer $\gamma \in S$ temos que:*

a) $F_{\gamma,L/\mathbb{Q}}, P_{\gamma/\mathbb{Q}} \in \mathbb{Z}[x]$ *e* $\mathcal{T}_{L/\mathbb{Q}}(\gamma), \mathcal{N}_{L/\mathbb{Q}}(\gamma) \in \mathbb{Z}$

b) $\mathcal{N}_{L/\mathbb{Q}}(\gamma)$ *é um múltiplo de* γ *no anel* S.

c) $\gamma \in U(S)$ *se, e somente se* $\left|\mathcal{N}_{L/\mathbb{Q}}(\gamma)\right| = 1$

d) *Se* $\left|\mathcal{N}_{L/\mathbb{Q}}(\gamma)\right|$ *for um número primo, então* γ *será irredutível em* S

Este corolário mostra, em particular, que para decidir se um número algébrico é inteiro ou não, basta considerar o seu polinômio minimal sobre $\mathbb{Q}$. Por exemplo seja $\gamma = r\sqrt[p]{q}$, $r \in \mathbb{Q} \setminus \{0\}$ e p, q números primos. Então $P_{\gamma/\mathbb{Q}} = x^q - pr^q$, portanto γ será um inteiro algébrico se, e somente se $r \in \mathbb{Z}$ e certamente γ não é invertível em $I_{\mathbb{Q}(\gamma)}$.

Observação A.34 *ζ é invertível em $I_{\mathbb{Q}(\zeta)}$, onde ζ é uma raíz primitiva n-ésima da unidade, pois o termo independente de Φ_n (n-ésimo polinômio ciclotônico) é sempre 1.*

É natural perguntar se é possível decidir se um elemento $\alpha \in L$ é um inteiro algébrico ou não, através de uma base apropriada de $L/\mathbb{Q}$.

Mais precisamente, perguntamos se existe uma base $\{\beta_1, \ldots, \beta_n\}$ de $L/\mathbb{Q}$, tal que $\alpha = a_1\beta_1 + \cdots + a_n\beta_n$ se, e somente se $a_1, \ldots, a_n \in \mathbb{Z}$. Precisamos agora nos referir a um assunto do capítulo 1, bases integrais, para entender que sim, pois para qualquer extensão L de $\mathbb{Q}$, de grau n, o anel I_L é um $\mathbb{Z}$-módulo livre de posto n.

A seguir, consideraremos domínios quaisquer R e A, R contido em A, e estudaremos as relações entre estes domínios no caso em que A é inteiro sobre R, isto é, $I_A(R) = A$.

Teorema A.35 *Seja A um domínio inteiro sobre R. Então;*

a) *Para qualquer ideal $\mathfrak{a}$ não-nulo de A, $\mathfrak{a} \cap R$ é um ideal não-nulo de R*

b) *Os elementos inversíveis em A que estão em R são inversíveis em R*

c) *A será um corpo se, e somente se R for um corpo*

d) *Um ideal primo $\mathfrak{p}$ de A será um ideal maximal de A se, e somente se $\mathfrak{p} \cap R$ for um ideal maximal de R.*

Prova. a) Seja $\alpha \in \mathfrak{a} \neq 0$, como A é inteiro sobre S

$$seja \quad x^n + a_1x^{n-1} + \cdots + a_n$$

um polinômio mônico em $R[x]$ de menor grau que tenha α como raiz

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$$

daí

$$a_n = -\alpha^n - a_1\alpha^{n-1} - \cdots - a_{n-1}\alpha \neq 0$$

isto é

$$a_n = -\alpha(\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1}) \neq 0 \quad \text{e} \quad a_n \in R$$

então

$$a_n \in (\alpha A \cap R) \subseteq (\mathfrak{a} \cap R) \Rightarrow a_n \in (\mathfrak{a} \cap R) \text{ e } a_n \neq 0$$

b) Sabemos que

$$U(R) \subseteq (U(A) \cap R) \quad (1)$$

Seja $u \in (U(A) \cap R)$, então $u^{-1} \in A$ e é inteiro sobre R. Logo existem $c_1, \ldots, c_m \in R$ tais que

$$u^{-m} + c_1 u^{-m+1} + \cdots + c_{m-1} u^{-1} + c_m = 0$$

Multiplicando por (u^{m-1}) temos

$$u^{-1} + c_1 + c_2 u + c_3 u^2 + \cdots + c_{m-1} u^{m-2} + c_m u^{m-1} = 0$$

$$\Rightarrow u^{-1} = -(c_m u^{m-1} + c_{m-1} u^{m-2} + \cdots + c_2 u + c_1) \in R[u] \subseteq R,$$

pois $u \in R$ também, logo $u^{-1} \in R$, isto é, $u \in U(R)$, ou seja

$$(U(A) \cap R) \subseteq U(R) \quad (2)$$

De (1) e (2) temos, portanto a igualdade $(U(A) \cap R) = U(R)$

c) [$\Rightarrow$ Seja A um corpo, então $U(A) = A \setminus \{0\}$ por b)

$$U(R) = (U(A) \cap R) = (A \setminus \{0\} \cap R) = R \setminus \{0\} \Rightarrow R \text{ é corpo}$$

$\Leftarrow$] A não é corpo, então possuirá um ideal não nulo $\mathfrak{a}$, com $1 \notin \mathfrak{a}$. Pelo item a) o ideal $\mathfrak{a} \cap R$ de R é não-nulo. Logo R não é corpo.

d) Seja $\pi : A \longrightarrow \dfrac{A}{\mathfrak{p}}$ um homomorfismo canônico, logo $\pi(A) = \dfrac{A}{\mathfrak{p}}$ é inteiro sobre o subanel $\pi(R)$, o qual é isomorfo a $\dfrac{R}{\mathfrak{p} \cap R}$.
O ideal $\mathfrak{p}$ de A será maximal se, e somente se $\dfrac{A}{\mathfrak{p}}$ for um corpo, este fato, pelo item c, ocorrerá se, e somente se $\dfrac{R}{\mathfrak{p} \cap R}$ for um corpo e, por sua vez se, e somente se $\mathfrak{p} \cap R$ for um ideal maximal de R. ■

Corolário A.36 *Seja o domínio A inteiro sobre R.*
Se todo ideal primo não-nulo de R for maximal, então todo ideal primo não-nulo de A será maximal.

Prova. Seja $\mathfrak{p}$ um ideal primo não-nulo de A, então pelo teorema A.35 item a, $\mathfrak{p} \cap R$ é um ideal primo não-nulo de R, logo maximal por hipótese do corolário. Então pelo item d do Teorema A.35, $\mathfrak{p}$ é um ideal maximal de A. ■

É bem conhecido que $\mathbb{Z}$, e mais geralmente qualquer domínio principal, tem a propriedade acima indicada, ou seja, todo ideal primo não-nulo de um domínio inteiro sobre $\mathbb{Z}$ será maximal. Disso resulta em particular

Corolário A.37 *Seja K um corpo de números algébricos. Então todo ideal primo não-nulo de I_K é um ideal maximal.*

A.8 Discriminante do polinômio f

Seja K um corpo de caracerística 0 ou prima. $f(x) \in K[x]$ um polinômio separável de grau n, tendo como corpo de decomposição L/K.

Se $f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\ \ c \in K$, consideremos $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$.

Embora o número Δ não dependa da indexação e disposição das raízes, o sinal do número Δ depende. Por isso definimos o seguinte; o discriminante de um polinômio $f(x) \in K[x]$ como sendo Δ^2, e denotamos por $disc(f) = \Delta^2$ desta forma, o discriminante depende apenas do conjunto de raízes.

É interessante notar que embora as raízes $\alpha_i's$ pertençam a L, o discriminante do polinômio f, resultante de operações com essas raízes, pertence a K.

Isto é, seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$, com $a_0, \ldots, a_n \in K$. O discriminante de f é da forma $p(a_0, a_1, \ldots, a_n)$ para algum polinômio $p \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$. Isso pode ser concluído do fato de $disc(f)$ ser uma função simétrica nas raízes de f.

Daí $disc(f) \in K$, para qualquer grau de f. Em particular, temos

$$disc(x^2 + bx + c) = b^2 - 4c$$

$$disc(x^3 + bx^2 + cx + d) = b^2c^2 - 4c^3 - 3b^3d - 27d^2 + 18bcd$$

A.9 Corpos Conjugados e Elementos Conjugados

Definição A.38 *Dados dois corpos K e Ω contendo o corpo $\mathbb{Q}$, chamamos de $\mathbb{Q}$-isomorfismo de K sobre Ω a todo isomorfismo $\varphi : K \longrightarrow \Omega$, tal que $\varphi(a) = a$, para todo $a \in \mathbb{Q}$.*

Nestas condições dizemos que K e Ω são $\mathbb{Q}$-isomorfos.

Agora se K e Ω são extensões algébricas de $\mathbb{Q}$, diremos que K e Ω são corpos $\mathbb{Q}$-conjugados.

Definição A.39 *Dadas duas extensões K e Ω de $\mathbb{Q}$, dizemos que dois elementos $\alpha \in K$ e $\beta \in \Omega$ são $\mathbb{Q}$-conjugados se existir um $\mathbb{Q}$-isomorfismo*

$$\varphi : \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\beta)\ ,\ tal\ que\ \varphi(\alpha) = \beta$$

O isomorfismo φ que leva elemento primitivo em elemento primitivo é único, e o fato de dois elementos α, β serem conjugados sobre $\mathbb{Q}$ significa que ou α, β são trancedentes sobre $\mathbb{Q}$ ou α e β são algébricos sobre $\mathbb{Q}$ e, neste caso, têm o mesmo polinômio minimal, isto é, $P_{\alpha/\mathbb{Q}}$=$P_{\beta/\mathbb{Q}}$.

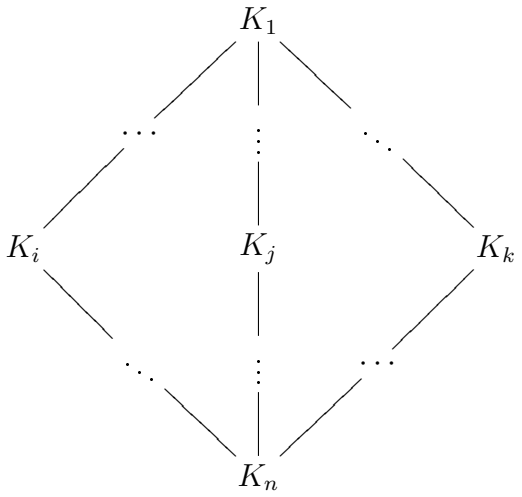
Por exemplo, se $f(x)$ é um polinômio irredutível sobre $\mathbb{Q}$ e $\alpha_1, \alpha_2, \ldots, \alpha_n$ são suas raízes distintas em uma extensão K de $\mathbb{Q}$, então α_i e α_j com $i \neq j$ são elementos dois a dois $\mathbb{Q}$-conjugados e $\mathbb{Q}(\alpha_i)$, $\mathbb{Q}(\alpha_j)$ são corpos dois a dois conjugados sobre $\mathbb{Q}$.

A.10 Teoria de Galois

Dada uma extensão de corpos normal e separável L de $\mathbb{Q}$, associamos a cada corpo intermediário K_{indice} de L um subgrupo Δ_{indice} de Γ e vice-versa.

Assim $L = K_1 \sim \Delta_1 = \{Id_L\}$, $K_i \sim \Delta_i$, $K_j \sim \Delta_j$, $K_k \sim \Delta_k$ e $\mathbb{Q} = K_n \sim \Delta_n = \Gamma$

com $i, j, k \in \{1, 2, \ldots, n\}$



onde $\Gamma = Aut(L/\mathbb{Q}) := \{\sigma : L \hookleftarrow \ ; \sigma(\alpha) = \alpha, \ \forall \alpha \in \mathbb{Q}\}$ é o conjunto de todos os automorfismos entre $\mathbb{Q}$ e L que fixam $\mathbb{Q}$.

Considere o conjunto de grupos $\mathcal{G} = \{\Delta \ ; \Delta \leq \Gamma\}$ e o conjunto de corpos $\mathcal{F} = \{K \ ; \mathbb{Q} \subseteq K \subseteq L\}$. Existe uma aplicação

$$\begin{array}{rccc} f: & \mathcal{F} & \to & \mathcal{G} \\ & K & \rightsquigarrow & \Delta \end{array}$$

cuja imagem é um grupo,

$$f(K) = \{\sigma \in \Gamma \ ; \sigma(\alpha) = \alpha, \ \forall \alpha \in K\} = \ Aut(L/K),$$

e outra aplicação

$$\begin{array}{rccc} g: & \mathcal{G} & \to & \mathcal{F} \\ & \Delta & \rightsquigarrow & K \end{array}$$

cuja imagem é um corpo,

$$g(\Delta) = \{\alpha \in L; \sigma(\alpha) = \alpha, \ \forall \sigma \in \Delta\} = corpo \ fixo \ de \ \Delta$$

.

Denotamos por $\mathcal{G}^*$ a imagem $f(\mathcal{F})$ e por $\mathcal{F}^*$ a imagem $g(\mathcal{G})$

$$f : \mathcal{F} \longrightarrow \mathcal{G} \Rightarrow f(\mathcal{F}) \subseteq \mathcal{G}, \text{ sendo } \mathcal{G}^* = f(\mathcal{F}) \Rightarrow \mathcal{G}^* \subseteq \mathcal{G}$$

$$g : \mathcal{G} \longrightarrow \mathcal{F} \Rightarrow g(\mathcal{G}) \subseteq \mathcal{F}, \text{ sendo } \mathcal{F}^* = g(\mathcal{G}) \Rightarrow \mathcal{F}^* \subseteq \mathcal{F}$$

Proposição A.40 *As aplicações $f : \mathcal{F} \longrightarrow \mathcal{G}$ e $g : \mathcal{G} \longrightarrow \mathcal{F}$;*

i) Invertem a inclusão

ii) Induzem bijeções entre $\mathcal{F}^*$ e $\mathcal{G}^*$ inversas entre si.

Prova. de i)

$$K' \subseteq K'' \Rightarrow \begin{array}{ccc} & L & \\ f(K'') = Aut(L/K'') & | & \\ & K'' & f(K') = Aut(L/K') \\ & | & \\ & K' & \\ & | & \\ & \mathbb{Q} & \end{array} \Rightarrow f(K') \supseteq f(K'')$$

$$\Delta'' \subseteq \Delta' \Rightarrow \begin{array}{ccc} & L & \\ \Delta'' & | & \\ \Delta' & K'' = g(\Delta'') & \\ & | & \\ & K' = g(\Delta') & \\ & | & \\ & \mathbb{Q} & \end{array} \Rightarrow g(\Delta'') \supseteq g(\Delta')$$

■

Para provar ii) vamos ver alguns resultados preliminares

Lema A.41 *As aplicações $f : \mathcal{F} \longrightarrow \mathcal{G}$ e $g : \mathcal{G} \longrightarrow \mathcal{F}$ satisfazem;*

$$K \subseteq g \circ f \ \ (K), \ \forall K \in \mathcal{F} \qquad e \qquad \Delta \subseteq f \circ g \ \ (\Delta), \ \forall \Delta \in \mathcal{G}$$

Prova. Se $\alpha \in K$, então $\exists \sigma \in \Gamma$, tal que $\sigma(\alpha) = \alpha$, $\forall \sigma \in Aut(L/K) = f(K)$. Isto é, para $\alpha \in K$, então $\sigma(\alpha) = \alpha$, $\forall \sigma \in f(K)$, logo $\alpha \in g(f(K)) \Rightarrow K \subseteq g \circ f(K)$ e se $\sigma \in \Delta$, então $\exists \alpha \in L$, tal que $\sigma(\alpha) = \alpha$, $\forall \alpha \in g(\Delta) =$ corpo fixo de Δ, isto é, para $\sigma \in \Delta$, então $\sigma(\alpha) = \alpha$, $\forall \alpha \in g(\Delta)$, logo $\sigma \in f(g(\Delta)) \Rightarrow \Delta \subseteq f \circ g(\Delta)$ ■

Concluimos do lema A.41 que;

Lema A.42 a) $K \in \mathcal{F}^* \Leftrightarrow K = g \circ f \ \ (K)$, *qualquer que seja* $K \in \mathcal{F}$

b) $\Delta \in \mathcal{G}^* \Leftrightarrow \Delta = f \circ g \ \ (\Delta)$, *qualquer que seja* $\Delta \in \mathcal{G}$.

Prova. a) [$\Rightarrow$ Consideremos $K \in \mathcal{F}^*$, isto é $K \in g(\mathcal{G})$, como

$$\begin{array}{rccc} g: & \mathcal{G} = \{\Delta \ ; \Delta \leq \Gamma\} & \longrightarrow & \mathcal{F} = \{K \ ; \mathbb{Q} \subseteq K \subseteq L\} \\ & \Delta & \rightsquigarrow & K \end{array}$$

digamos $g(\Delta) = K$, pelo lema A.41 $\Delta \subseteq f \circ g(\Delta)$, $\forall \Delta \in \mathcal{G}$, e como g inverte a inclusão

$g(\Delta) \supseteq g(f \circ g(\Delta))$, isto é, $K = g(\Delta) \supseteq g \circ f \circ g(\Delta) = g \circ f(K) \Rightarrow g \circ f(K) \subseteq K$ e

por A.41 $K \subseteq g \circ f(K)$, $\forall K \in \mathcal{F}$, temos a igualdade.

$\Leftarrow$] Seja $K = g \circ f(K)$, qualquer que seja $K \in \mathcal{F}$. Como

$$\begin{array}{rccc} f: & \mathcal{F} = \{K \ ; \mathbb{Q} \subseteq K \subseteq L\} & \longrightarrow & \mathcal{G} = \{\Delta \ ; \Delta \leq \Gamma\} \\ & K & \rightsquigarrow & \Delta \end{array}$$

digamos $f(K) = \Delta$

$$\Rightarrow K = g(f(K)) = g(\Delta) \Rightarrow K \in Im\ g \Leftrightarrow K \in g(\mathcal{G}) \Rightarrow K \in \mathcal{F}^*$$

b) [$\Rightarrow \Delta \in \mathcal{G}^*$, isto é, $\Delta \in f(\mathcal{F})$, como $f(K) = \Delta$,

pelo lema A.41 $K \subseteq g \circ f(K)$, $\forall K \in \mathcal{F}$

e como f inverte a inclusão $f(K) \supseteq f(g \circ f(K))$,

isto é $\Delta = f(K) \supseteq f \circ g \circ f(K) = f \circ g(\Delta) \Rightarrow f \circ g(\Delta) \subseteq \Delta$

e pelo lema A.41 $\Delta \subseteq f \circ g(\Delta)$, $\forall \Delta \in G$, temos a igualdade.

$\Leftarrow$] Seja $\Delta = f \circ g(\Delta)$, qualquer que seja $\Delta \in \mathcal{G}$.
Como

$$\begin{array}{rccc} g: & \mathcal{G} = \{\Delta \ ; \Delta \leq \Gamma\} & \longrightarrow & \mathcal{F} = \{K \ ; \mathbb{Q} \subseteq K \subseteq L\} \\ & \Delta & \rightsquigarrow & K \end{array}$$

digamos $g(\Delta) = K$

$\Rightarrow \Delta = f(g(\Delta)) = f(K) \Rightarrow \Delta \in Im\ f \Leftrightarrow \Delta \in f(\mathcal{F}) \Rightarrow \Delta \in \mathcal{G}^*$ ■

Prova da Proposição A.40, item ii). Se $K \in \mathcal{F}^* \Rightarrow K = g \circ f(K)$, $\forall K \in \mathcal{F} \Rightarrow f(K) = f(g \circ f(K))$, digamos $f(K) = \Delta$.

$$f(K) = f(g(\Delta)) \Rightarrow f(K) \in Im\ f \Rightarrow f(K) \Rightarrow f(K) \in \mathcal{G}^*$$

isto é, $K \in \mathcal{F}^* \Rightarrow f(K) \in \mathcal{G}^*$ (1).

Se $\Delta \in \mathcal{G}^* \Rightarrow \Delta = f \circ g(\Delta)$, $\forall \Delta \in \mathcal{G} \Rightarrow g(\Delta) = g(f \circ g(\Delta))$, digamos $g(\Delta) = K$

$$g(\Delta) = g(f(K)) \Rightarrow g(\Delta) \in Im\ g \Rightarrow g(\Delta) \in g(\mathcal{G}) \Rightarrow g(\Delta) \in \mathcal{F}^*$$

isto é, $\Delta \in \mathcal{G}^* \Rightarrow g(\Delta) \in \mathcal{F}^*$ (2).

(1) e (2) implicam em

$$\begin{array}{rccc} f: & \mathcal{F}^* \subseteq \mathcal{F} & \longrightarrow & f(\mathcal{F}) = \mathcal{G}^* \subseteq \mathcal{G}, \quad \forall K \in \mathcal{F}^*,\ \exists! \Delta \in \mathcal{G}^* \text{ ,tal que } \Delta = f(K) \\ & K & \rightsquigarrow & \Delta \end{array}$$

ou seja, $f : \mathcal{F}^* \longrightarrow \mathcal{G}^*$ é bijetora e

$$g : \mathcal{G}^* \subseteq \mathcal{G} \longrightarrow g(\mathcal{G}) = \mathcal{F}^* \subseteq \mathcal{F},\ \forall \Delta \in \mathcal{G}^*,\ \exists! K \in \mathcal{F}^* \text{ ,tal que } K = g(\Delta)$$

ou seja, $g : \mathcal{G}^* \longrightarrow \mathcal{F}^*$ é bijetora e

$$f \circ g(\sigma) = f(g(\sigma)) = f(\alpha) = \sigma \Rightarrow f \circ g = Id_{\mathcal{G}^*} \text{ e}$$

$$g \circ f(\alpha) = g(f(\alpha)) = g(\sigma) = \alpha \Rightarrow g \circ f = Id_{\mathcal{F}^*}$$
$$\Rightarrow f^{-1} = g \text{ e } g^{-1} = f$$

e portanto f e g são bijeções inversas entre si. ■

O par de aplicações $\mathcal{F} \leftrightarrows \mathcal{G}$ é chamada de conexão de Galois e, se forem bijetivas, esse par é dito uma correspondência de Galois entre os conjuntos $\mathcal{F}$ e $\mathcal{G}$ ordenados pela inclusão e denotado por $\mathcal{F}^* \longleftrightarrow \mathcal{G}^*$.

É natural perguntar quais são os corpos $K \in \mathcal{F}^*$ e os grupos $\Delta \in \mathcal{G}^*$ que satisfazem tal correspondência.

Para isto determinamos certos conjuntos

$\mathcal{F}' = \{K, \mathbb{Q} \subseteq K \subseteq L \ \ ; L/K \text{ é galoisiana e finita}\}$ de $\mathcal{F}^*$

e $\mathcal{G}' = \{\Delta, \Delta \leq \Gamma \ \ ; L/g(\Delta) \text{ é galoisiana e finita}\}$ de $\mathcal{G}^*$,

tais que $\mathcal{F} \leftrightarrows \mathcal{G}$ induza uma correspondência de Galois $\mathcal{F}' \longleftrightarrow \mathcal{G}'$.

A.10.1 2ª Parte do Teorema fundamental de Galois (Teorema de Artin)

Teorema A.43 *Seja Δ um subgrupo finito de $\Gamma = Aut(L/\mathbb{Q})$. Então $L/g(\Delta)$ é uma extensão normal e separável de grau $o(\Delta)$ e $\Delta = Aut(L/g(\Delta))$*

Corolário A.44 *Seja K um corpo tal que $\mathbb{Q} \subseteq K \subseteq L$ e $[L : K] < \infty$, então L/K é galoisiana $\Leftrightarrow g \circ f(K) = K$.*

Neste caso, $[L : K] = o(\Delta)$, onde $\Delta = f(K)$

Corolário A.45 *A conexão de Galois $\mathcal{F} \leftrightarrows \mathcal{G}$ induz uma correspondência de Galois $\mathcal{F}' \longleftrightarrow \mathcal{G}'$*

Corolário A.46 *Se $L/\mathbb{Q}$ é galoisiana finita, então a conexão de Galois $F \rightleftarrows G$ é uma correspondência de Galois.*

Definição A.47 $\Delta^\sigma = \{\sigma^{-1}\delta\sigma \ \ ; \sigma \in \Gamma \text{ e } \delta \in \Delta\}$ *é o subgrupo de Γ conjugado a Δ,*

$\Delta^\sigma \leq \Gamma$ *e $\Delta^\sigma \trianglelefteq \Gamma$, quando $\Delta^\sigma = \Delta,\ \forall \sigma \in \Gamma$.*

Mostraremos que, na conexão de Galois $F \rightleftarrows G$, subgrupos conjugados de Γ correspondem a subcorpos $\mathbb{Q}$-conjugados de L. No seguinte sentido:

Lema A.48 **a)** $\forall K \in \mathcal{F}$ *e* $\forall \sigma \in \Gamma$, *temos que* $\sigma^{-1} f(K)\sigma = f(\sigma(K))$

b) $\forall \Delta \in \mathcal{G}$ *e* $\forall \sigma \in \Gamma$, *temos que* $g(\sigma\Delta\sigma^{-1}) = \sigma(g(\Delta))$

Prova. a)$\forall \sigma \in \Gamma$, temos $\delta \in \sigma^{-1} f(K)\sigma \Leftrightarrow \sigma^{-1}\delta\sigma \in f(K) = Aut(L/K) \Rightarrow \sigma^{-1}\delta\sigma(\alpha) = \alpha,\ \forall \alpha \in K$.

$\delta\sigma(\alpha) = \sigma\alpha, \forall \alpha \in K \Rightarrow \delta\sigma(K) = \sigma(K) \Rightarrow \delta$ fixa $\sigma(K)$, ou seja, $\delta \in Aut(L/\sigma(K))$, logo $\delta \in f(\sigma(K))$, daí $\sigma^{-1} f(K)\sigma \subseteq f(\sigma(K))$ (1).

Seja $\delta \in f(\sigma(K)) \Rightarrow \delta \in Aut(L/\sigma(K) \Rightarrow \delta$ fixa $\sigma(K) \Rightarrow \delta(\sigma(K)) = \sigma(K) \Rightarrow \delta(\sigma(\alpha)) = \sigma(\alpha)$, $\forall \alpha \in K$

$\sigma^{-1}\delta\sigma(\alpha) = \alpha$, $\forall \alpha \in K \Rightarrow \sigma^{-1}\delta\sigma$ fixa $K \Rightarrow \sigma^{-1}\delta\sigma \in Aut(L/K) \Rightarrow \sigma^{-1}\delta\sigma \in f(K) \Leftrightarrow \delta \in \sigma^{-1} f(K)\sigma$

Daí $f(\sigma(K)) \subseteq \sigma^{-1} f(K)\sigma$ (2)

e de (1) e (2) temos a igualdade.

b) $\forall \alpha \in L$, temos $\alpha \in g(\sigma\Delta\sigma^{-1}) \Leftrightarrow \sigma\Delta\sigma^{-1}(\alpha) = \alpha$

$\Delta\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha) \Leftrightarrow \Delta$ fixa $\sigma^{-1}(\alpha) \Leftrightarrow \Delta \subseteq Aut(L/\sigma^{-1}(\alpha)) \Rightarrow \Delta \subseteq f(\sigma^{-1}(\alpha)) \Rightarrow g(\Delta) \supseteq g(f(\sigma^{-1}(\alpha))) \Rightarrow \sigma^{-1}(\alpha) \in g(\Delta)$ *aplica* σ

$\alpha \in \sigma(g(\Delta)) \Rightarrow g(\sigma\Delta\sigma^{-1}) \subseteq \sigma(g(\Delta))$ (1)

$\alpha \in \sigma(g(\Delta))$ $(\sigma^{-1}) \Rightarrow \sigma^{-1}(\alpha) \in g(\Delta) \Rightarrow f(\sigma^{-1}(\alpha)) \supseteq f(g(\Delta)) \Rightarrow \Delta \subseteq$

$f(\sigma^{-1}(\alpha)) \Rightarrow \Delta \subseteq f(\sigma^{-1}(\alpha)) \Rightarrow \Delta \subseteq Aut(L/\sigma^{-1}(\alpha)) \Rightarrow \Delta\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha)$ *aplica* σ

$\Rightarrow \sigma\Delta\sigma^{-1}(\alpha) = \alpha \Rightarrow \alpha \in g(\sigma\Delta\sigma^{-1})$ daí $\sigma(g(\Delta)) \subseteq g(\sigma\Delta\sigma^{-1})$ (2)

e de (1)e (2) temos a igualdade. ■

Do lema A.48 resulta que $\mathcal{F}^*$ e $\mathcal{G}^*$ são estáveis sob conjugação com elementos de Γ.

Lema A.49 **a)** *Seja* $K \in \mathcal{F}^*$, *então* $\sigma(K) \in \mathcal{F}^*$, *para todo* $\sigma \in \Gamma$

b) *Seja* $\Delta \in \mathcal{G}^*$, *então* $\sigma^{-1}\Delta\sigma \in \mathcal{G}^*$, *para todo* $\sigma \in \Gamma$

A.10.2 3ª Parte do Teorema Fundamental de Galois

Quanto a normalidade vale o seguinte:

Lema A.50 **a)** *Se* $K \in \mathcal{F}$ *e* $K/\mathbb{Q}$ *é uma extensão normal, então o grupo* $f(K)$ *será normal em* Γ

b) *Seja $L/\mathbb{Q}$ uma extensão normal. Se $\Delta \in \mathcal{G}$ for um subgrupo normal de Γ, então a extensão $g(\Delta)/\mathbb{Q}$ será normal.*

Prova. a)

$$\begin{array}{l} L \\ | \;\big) Aut(L/K) = f(K) \trianglelefteq \Gamma \\ K \\ | \;\big) \text{norm.} \\ \mathbb{Q} \end{array}$$

De fato, $\forall \sigma \in \Gamma$, temos $\sigma(K) = K$, pois $K/\mathbb{Q}$ é norm., logo pelo lema A.48

$$\sigma^{-1} f(K) \sigma = f(\sigma(K)) = f(K) \Leftrightarrow f(K)^{\sigma} = f(K) \Rightarrow f(K) \trianglelefteq \Gamma$$

b)

$$\text{norm.} \left(\begin{array}{ll} L & \\ | & \big) \Delta \trianglelefteq \Gamma \\ K & \Downarrow \\ | & \big) \text{norm.} \\ \mathbb{Q} & \end{array} \right.$$

De fato, $\forall \sigma \in \Gamma$, temos $\sigma^{-1} \Delta \sigma = \Delta$, pois $\Delta \trianglelefteq \Gamma$, logo pelo lema A.48

$$\sigma(g(\Delta)) = f(\sigma^{-1} \Delta \sigma) = g(\Delta)$$

Como $L/\mathbb{Q}$ é normal $\Rightarrow \sigma(L) \subseteq L$, $\forall \sigma \in \Gamma$ resulta que $g(\Delta)/\mathbb{Q}$ é normal. ■

Proposição A.51 *Seja $L/\mathbb{Q}$ uma extensão galoisiana finita, para quaisquer $K \in \mathcal{F}$ e $\Delta \in \mathcal{G}$ temos;*

a) *$\sigma(K)$ corresponde a Δ^{σ}, $\forall \sigma \in \Gamma$*

b) *$K/\mathbb{Q}$ será normal se, e somente se Δ é um subgrupo normal de Γ.*

$$\Gamma \trianglerighteq \Delta \left(\begin{array}{l} L \\ | \\ K \\ | \;\big) norm. \\ \mathbb{Q} \end{array} \right.$$

$\Delta^{\sigma} = \{\sigma^{-1} \delta \sigma \;\; ; \delta \in \Delta \text{ e } \sigma \in \Gamma\}$.

Neste caso, a restrição $\sigma \to \sigma_{|_K}$, $\sigma \in \Gamma$ é um homomorfismo de $\Gamma = Aut(L/\mathbb{Q})$ sobre $Aut(K/\mathbb{Q})$ com núcleo Δ.

$$\begin{array}{ccc} Aut(L/\mathbb{Q}) & \longrightarrow & Aut(K/\mathbb{Q}) \\ \sigma & \rightsquigarrow & \sigma_{|_K} \end{array}$$

Logo $\ker(\sigma_{|_K}) = \Delta$, portanto induz um isomorfismo $\dfrac{\Gamma}{\Delta} \simeq Aut(K/\mathbb{Q})$,

ou seja, $[K : \mathbb{Q}] = \dfrac{o(\Gamma)}{o(\Delta)} = (\Gamma : \Delta)$.

A.10.3 Teorema Fundamental de Galois

Teorema A.52 *Sejam L uma extensão galoisiana e finita de $\mathbb{Q}$ e Γ seu grupo de Galois , $\Gamma = Gal(L/\mathbb{Q})$. Para cada subgrupo Δ de Γ, seja $g(\Delta)$ o corpo fixo de Δ. Para cada subcorpo K de L que contém $\mathbb{Q}$, seja $f(K)$ o grupo dos K-automorfismos de L. Então;*

i) As aplicações f e g são bijeções inversas uma da outra e invertem a inclusão;

ii) L é uma extensão galoisiana de seu corpo intermediário K de grau $o(\Delta)$;

iii) Para que um corpo intermediário K seja uma extensão Galoisiana de $\mathbb{Q}$ é necessário e suficiente que $f(K) = \Delta$ seja um subgrupo normal de Γ.

Provamos o item *i* pela prova da proposição A.40 e lema A.41.
Para a prova dos itens *ii* e *iii*, veja a prova do teorema A.43 e lema A.48, bem como a do lema A.50 e proposição A.51 na literatura consultada, ref. [End2] §6 e [Rot].

Ensaio: Morre Intelectual, Nasce a Álgebra Moderna

"Só a ciência pura é digna de um espírito superior".
Arquimedes, séc. III a.C.

Aos dezenove anos um jovem cientista francês entregou ao Diretor geral do departamento de Matemática e Ciências da Escola Politécnica de Paris um artigo de sua autoria entitulado "Une mémoire sur les conditions le resolution de equations par des radicaux". O veterano professor rejeitou o manuscrito classificando-o de incompreensível. Quarenta anos depois, graças a J. Liouville, as idéias dessa obra começaram a ser compreendidas. Seu autor atendia pelo nome de Évariste Galois (1811-1832) e suas idéias sedimentaram as base do que hoje chamamos de Álgebra Moderna.

Galois caracterizou, em termos de teoria das permutações, as condições de resolubilidade por radicais das equações algébricas. Para tanto, criou o conceito de "grupo" e o próprio termo pelo qual é conhecido em matemática, e também, implicitamente, a noção de "corpo" que mais tarde Dedekind definiria de forma explícita.

Vamos tentar mostrar como Galois construiu sua teoria, desenhando o que só pode ocorrer na natureza e no raciocínio do gênio.

Galois estabeleceu uma analogia entre uma figura P (um polígono qualquer) no plano com entes algébricos.

Polígono P	Polinômio $p \in K[x]$
O plano que o contém	Corpo de decomposição L de $p(x)$
O gênero (n° de lados) de P	Grau de $p(x)$
Os vértices $v_1, \ldots, v_n$ de P	as raízes $\alpha_1, \ldots, \alpha_n$ de $p(x)$
Polígono regular	Polinômio irredutível

E chamou de $\sum(P)$ o conjunto de todas as permutações do polígono, deu-lhe uma estrutura de grupo com a operação composição, visto como a família de todas as transformações ortogonais $\sigma : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, tal que $\sigma(P) = P$.

Como uma transformação linear o elemento $\sigma \in \sum(P)$ seria um operador ortogonal simétrico, aquele que preserva módulo e sua matriz associada é invariante por transposição.

Se P é um polígono no plano de gênero n, $vert(P) = \{v_1, \ldots, v_n\}$ é o conjunto de seus vértices, temos que cada transformação ortogonal $\sigma \in \sum(P)$ permuta $Vert(P)$ e que $\sum(P)$ é isomorfo a um subgrupo de S_n.

Por exemplo, se P é um triângulo equilátero, então $\sum(P) \simeq S_3$.

Se P é um triângulo isósceles, então $\sum(P) \simeq \mathbb{Z}_2$.

Se P é um triângulo escaleno, então $\sum(P) = \{Id\}$ tem ordem um.

Ou seja, um polígono qualquer pode ser dividido em polígonos regulares, assim como um polinômio qualquer pode ser fatorado em polinômios irredutíveis.

Uma segunda analogia auxiliará na formação do que procuramos ver.

Transformação linear	Automorfismos de L
Transformação linear ortogonal invariante em P	Automorfismo de L fixando K

A grande sacada de Galois foi associar cada polígono (polinômio) a um grupo de permutação (automorfismos) chamado Grupo de Galois.

$$\sum(P) \qquad Gal(P(x)) = Gal(L/K)$$

A teoria de Galois associa a cada equação algébrica um conveniente grupo de permutação de suas raízes. Tal grupo é definido na teoria como grupo dos automorfismos que fixam um certo subcorpo do corpo de decomposição do polinômio (equação polinomial) em questão.

Galois iniciou suas pesquisas com um trabalho de Lagrange sobre permutações de raízes, o que lhe deu condições necessárias e suficientes para concluir que equações polinomiais são resolúveis por radicais e, baseado nas provas de Abel, descobriu que as equações algébricas irredutíveis são resolúveis por radicais se, e somente se o grupo de permutações sobre suas raízes é solúvel, isto é, possui uma série de composição cujos grupos quocientes são cíclicos de ordem prima. Sobre isso forneceu um algoritmo para achar essas raízes, assim como outros postulados, sempre votados mais para a estrutura algébrica do que para casos específicos. Dando um tratamento generalizante e aritmético à Álgebra.

A noite que antecedera seu duelo passou em claro escrevendo as últimas conclusões de sua teoria, pois sabia que a morte, que certamente viria no dia seguinte, era um detalhe fugaz, sem importância.

Atribulações pessoais, bem como o pouco tempo que viveu, não impediram que Galois produzisse uma obra que, embora pequena, seria das mais inovadoras da Matemática em todos os tempos.

Bibliografia

[End1] Endler, O., *Teoria dos Números Algébricos*. IMPA, Rio de Janeiro, 1985.

[End2] Endler, O., *Teoria dos Corpos*, Monografias de Matemática N°44, IMPA, Rio de Janeiro, 1973.

[Was] Washington, L.C., *Introduction to Cyclotomic Fields*, 2nd. ed., Springuer-Verlag, New York, 1997.

[Rot] Rotman, J.J., *Galois Theory*. Springer, New York, 1998.

[Bha] Bhattacharya, P.B. and Jain, S.K. and Nagpaul, S.R., *Basic Abstract Algebra*. Cambridge University Press, New York, 1994.

[Gar] Garcia, A.L. e Lequain, Y., *Álgebra*: *Um Curso de Introdução*. IMPA, Rio de Janeiro, 1988.

[Gon] Gonçalves, A., *Introdução à Álgebra*. IMPA, Rio de Janeiro, 1979.

[Lan] Lang, S., *Algebraic Number Theory*. Springer-Verlag, 1986.

[Sam] Samuel, P., *Algebraic Theory of Numbers*. Hermann, Paris 1970.

[Tra] Neto, T.P. e Interlando, J.C. e Lopes, J.O.D.,*"On computing discriminants of subfields of* $\mathbb{Q}(\zeta_{p^r})$*"*,*Journal of Number Theory* 96, 319-325 2002.

[Lop] Lopes, J.O.D., *"Discriminants of subfield of* $\mathbb{Q}(\zeta_{2^r})$,*Journal of Algebra and Its Applications* 4, 463-469 2003.

[Bor] Borevich, Z.I. and Shafarevich, I.R., *Number Theory*, Springer-Verlag, New York, 2001.

[Ste] Stewart, I.N. and Tall, D.O., *Algebraic Number Theory*. Chapman and Hall, London, 1987.

[Rib] Ribenboin, P.,*Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.

[Wei] Weiss, E., *Algebraic Number Theory*, Dover, 1998.