O Grupo de Galois de $x^n - x^{n-1} - \dots - x - 1$.

Marcos Goulart Lima

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito: 2 de dezembro de
2008

Assinatura:

O Grupo de Galois de $x^n - x^{n-1} - \dots - x - 1$

Marcos Goulart Lima

Orientador: *Prof. Dr. Daniel Levcovitz*

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências - Matemática.

USP – São Carlos
Dezembro/2008

Agradecimentos

A Deus por me fazer lembrar a todo instante que o importante na minha vida é Ele.

Ao meu orientador Professor Doutor Daniel Levcovitz pela paciência e disposição nos seminários e principalmente na elaboração da dissertação.

Ao Professor Doutor Paulo Agozzini Martin por escrever o artigo que gerou essa dissertação e por responder meus e-mails.

Ao Professor Doutor Eduardo Tengan pela disposição de atenção e tempo. E por ter entrado no ICMC-USP em momento oportuno para mim.

Aos meus irmãos em Cristo da Igreja Batista Maranata por suas orações e pelos momentos que passamos juntos. Em especial ao Pastor Idalmar e à Dona Lu por me hospedar com tanto carinho nos finais de semana.

À toda minha família pelo sustento financeiro, sentimental e espiritual.

Aos meus pais Almir e Dalva; e meus irmãos Filipe e Ana Paula. Desculpem mas eu não encontrei palavras que expressam meu agradecimento.

À Helen pela amizade, companheirismo, paciência, fé e amor; pelas discussões, brigas e reconciliações; pelos incansáveis "eu te amo" e por fazer parte da minha vida.

Ao meu amigo Samid pelas horas jogando conversa fora e jogando video game.

Aos meus amigos e colegas da USP de São Carlos e da UNESP de Rio Claro. Em especial: Eduard, Fábio, Lucas, Paulo Liboni, Paulo Mendes e Thaís pelo tempo de estudo, RPG e conversa muito bem gasto.

Aos funcionários e docentes do ICMC pela competência e profissionalismo.

À CNPQ pelo apoio financeiro.

Resumo

Nessa dissertação provamos que se n é um inteiro par ou primo, então o Grupo de Galois de $x^n - x^{n-1} - \dots - x - 1$ é o grupo simétrico S_n . Essa família de polinômios surge naturalmente de uma generalização da sequência de Fibonacci.

Abstract

In this dissertation we prove that if n is even integer or a prime number, then the Galois Group of $x^n - x^{n-1} - \dots - x - 1$ is the symmetric group S_n . This polynomial family arises quite naturally from a kind of generalized Fibonacci sequence.

Introdução

Trabalhando com a teoria de Galois rapidamente se observa que descobrir o grupo de Galois de um polinômio em geral não é uma tarefa fácil. Não existe uma fórmula ou um método padrão para esse fim. Assim, uma alternativa é buscar famílias de polinômios e investigar seu grupo de Galois. Aqui apresentamos o resultado para o polinômio

$$f_n(x) = x^n - x^{n-1} - x^{n-2} - \dots - x - 1, \quad n \text{ par ou primo.}$$

Uma excelente ferramenta para caracterizar o grupo de Galois de uma extensão pode ser encontrada na Teoria Algébrica de Números. Para toda extensão de $\mathbb{Q}$, o grupo de Galois é gerado pelos subgrupos de inércia dos primos que se ramificam. Então, se obtermos informações suficientes sobre esses subgrupos de inércia podemos obter propriedades ou até mesmo caracterizar o grupo de Galois da extensão. E é justamente essa a técnica usada nesta dissertação.

Para leitura dessa dissertação assumimos um conhecimento básico de Teoria Algébrica de Números, como em [6], por exemplo. No entanto, não assumimos um conhecimentos de Corpos Locais e de fato, vamos demonstrar a maioria dos resultados sobre esses corpos utilizados nessa dissertação.

Partindo do pressuposto que o leitor tenha conhecimentos de Álgebra Comutativa, a primeira seção do capítulo 1 constrói as bases da Teoria Algébrica de Números que serão utilizadas como: elemento inteiro, definições e teoremas relativos ao índice de ramificação e o grau de inércia da decomposição de um ideal primo em uma extensão, e um critério para que um primo se ramifique em uma extensão.

A próxima seção é uma preparação para o estudos de Corpos Locais onde definimos o corpo $\mathbb{Q}_p$, que é um corpo completo, de duas maneiras distintas: usando limite projetivo e o completamento em relação a uma valorização de $\mathbb{Q}$. Enunciamos também o teorema de Hensel.

Na seção 1.3 está o estudo de Corpos Locais. A definição do índice de ramificação e grau de inércia para valorizações e a relação entre subgrupo de inércia e a extensão maximal

não ramificada de um Corpo Local também são apresentadas nessa seção. Terminamos o capítulo com a regra de sinal de Descartes que será usada na investigação das raízes do polinômio $f_n(x) = x^n - x^{n-1} - x^{n-2} - \dots - x - 1$.

O capítulo 2 trata das contas relativas ao polinômio e seu grupo de Galois. Na primeira seção damos uma justificativa para o interesse nesse polinômio. A seção 2.2 trata das características do polinômio: raízes, irreducibilidade e o discriminante.

Finalmente nas seções 2.3 e 2.4 está demonstrado que o Grupo de Galois do polinômio $f_n(x) = x^n - x^{n-1} - x^{n-2} - \dots - x - 1$ é S_n , para n par ou primo. No caso de n par isso é feito usando a teoria de Corpos Locais e no caso de n primo usando propriedades de grupo de permutações e teoria de Corpos Locais. Resta observar que para n ímpar não primo não se conhece ainda qual é o grupo de Galois do polinômio $f_n(x)$.

Sumário

Sumário	ix
1 Preliminares	3
1.1 Conceitos básicos	3
1.2 O corpo $\mathbb{Q}_p$	6
1.3 Corpos locais e suas extensões	9
1.4 Regra do sinal de Descartes	16
2 O polinômio $x^n - x^{n-1} - \dots - x - 1$	20
2.1 Origem do polinômio	20
2.2 Raízes, irreducibilidade e discriminante	21
2.3 O caso n par	24
2.4 O caso n primo	28
Referências Bibliográficas	33

CAPÍTULO 1

Preliminares

Neste capítulo apresentaremos definições e teoremas necessários para leitura desta dissertação. Tomamos como ponto de partida um curso inicial de teoria algébrica de números, como em [6], por exemplo. Primeiro serão enunciados alguns teoremas e definições básicas. Depois daremos duas definições para o corpo dos números p -ádicos $\mathbb{Q}_p$. Em seguida apresentamos alguns resultados sobre Corpos Locais. Por último, demonstraremos um teorema que não está diretamente relacionados à Teoria Algébrica de Números.

1.1 Conceitos básicos

Definição 1. *Sejam B uma anel e A um subanel de B . Um elemento $b \in B$ é inteiro sobre A se é raiz de um polinômio mônico em $A[x]$. Seja $p(x) \in A[x]$ um polinômio mônico tal que $p(b) = 0$. A relação $p(x) = 0$ é chamada de relação de dependência integral de b sobre A .*

Teorema 2. *Seja B um anel, A um subanel de B e $x \in B$. São equivalentes*

- 1. $x \in B$ é inteiro sobre A .*
- 2. O anel $A[x]$ é um A -módulo de finitamente gerado.*
- 3. Existe um subanel C de B tal que C contém A e x , e C é um A -módulo finitamente gerado.*

Demonstração: [6], pág. 28.

Definição 3. *Sejam B um anel e A um subanel de B . O conjunto A' dos elementos de B que são inteiros sobre A é um anel. O anel A' é chamado de fecho integral de A em B .*

Definição 4. *Sejam A um domínio de integridade e K seu corpo de frações. O fecho integral de A em K é chamado de fecho integral de A . O anel B é dito integral sobre A se todo elemento de B é inteiro sobre A . O anel A é dito integralmente fechado se todo elemento de K que é inteiro sobre A está em A .*

Definição 5. *Sejam $L \supset K$ uma extensão Galoisiana e $G = \text{Gal}(L/K)$. Seja $x \in L$. A norma de x relativa a L e K é dada por*

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x).$$

O traço de x relativo a K e L é dado por

$$\text{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x).$$

Teorema 6. *Sejam A um domínio de integridade e K seu corpo de frações. Seja L uma extensão finita de K e $x \in L$ inteiro sobre A . Assuma que K possui característica zero. Então os coeficientes do polinômio minimal de x em K são inteiros sobre A . Em particular, $N_{L/K}$ e $\text{Tr}_{L/K}$ são inteiros sobre A .*

Demonstração: [6], pág. 38.

Definição 7. *Sejam B um anel e A um subanel de B tal que B é um A -módulo livre de posto finito n . Para $(x_1, \dots, x_n) \in B^n$ o discriminante do conjunto $(x_1, \dots, x_n)$ é o elemento de A dado por*

$$D(x_1, \dots, x_n) = \det(\text{Tr}_{B/A}(x_i x_j)).$$

Definição 8. *Um domínio de integridade A é chamado um domínio de Dedekind se é Noetheriano, integralmente fechado e todo ideal primo não nulo é maximal.*

Teorema 9. *Sejam A um domínio de Dedekind e K seu corpo de frações. Sejam $L \supset K$ uma extensão finita de K e B o fecho integral de A em L . Assuma que K é de característica zero. Então A' é um domínio de Dedekind e um A -módulo finitamente gerado.*

Demonstração: [6], pág. 49.

Definição 10. *Sejam A um domínio de integridade e K seu corpo de frações. Todo A -submódulo I de K para o qual existe $d \in A \setminus \{0\}$ tal que $d.I \subset A$ é chamado ideal fracionário de A (ou de K com respeito a A).*

Teorema 11. *Sejam A um domínio de Dedekind e P o conjunto de ideais primos não nulos de A . Então:*

1. Todo ideal fracionário não nulo I de A pode ser unicamente expresso da forma

$$I = \prod_{p \in P} p^{n_p(I)},$$

onde $p \in P$, $n_p(I) \in \mathbb{Z}$ e $n_p(I) = 0$ para quase todo $p \in P$.

2. O monóide dos ideais fracionários não nulos é um grupo.

Demonstração: [6], pág. 51.

O teorema acima mostra que em um domínio de Dedekind todo ideal pode ser fatorado como produto de ideais primos.

Definição 12. Sejam A um domínio de Dedekind de característica zero e K seu corpo de frações. Sejam $L \supset K$ uma extensão finita de grau n e B o fecho integral de A em L . Sejam p um ideal primo de A e Bp o ideal em B gerado por p . Pelo teorema 11 podemos escrever Bp da forma

$$Bp = \prod_{i=1}^q P_i^{e_i},$$

onde os P_i 's são ideais primos distintos de B e e_i 's são inteiros positivos.

-O expoente e_i é chamado índice de ramificação de P_i sobre A .

-Como B é um A -módulo finitamente gerado então B/P_i é um espaço vetorial de dimensão finita sobre A/p . A dimensão f_i de B/P_i como espaço vetorial de dimensão finita sobre A/p é chamado de grau de inércia de P_i sobre A , isto é, $f_i = [B/P_i : A/p]$.

Definição 13. Os ideais primos P_i 's que aparecem na fatoração de Bp em B são ditos acima de p (ou sobre p).

Teorema 14. Com as notações da definição 12:

$$\sum_{i=1}^q e_i f_i = [B/Bp : A/p] = n.$$

Demonstração: [6], pág. 71.

Definição 15. Com as notações da definição 12 dizemos que um primo p de A se ramifica em B se qualquer um dos índices de ramificação é maior que 1.

Definição 16. Sejam K um corpo e $L \supset K$ uma extensão. Sejam A e B os anéis de inteiros de K e L respectivamente. O discriminante de B sobre A (ou de L sobre K) é o ideal de A gerado pelo discriminante das bases de L sobre K que estão contidas em B .
Notação $D_{B/A}$.

Teorema 17. Um ideal primo p de A se ramifica em B se, e somente se, p contém o discriminante $D_{B/A}$. Existe somente um número finito de primos de A que se ramificam em B .

Demonstração: [6], pág. 74.

Teorema 18. (*Hermite-Minkowski*) *Seja K uma extensão finita de $\mathbb{Q}$ o corpo dos números racionais, $K \neq \mathbb{Q}$. Então o discriminante $D_{K/\mathbb{Q}} \neq \pm 1$.*

Demonstração: [6], pág. 58.

Nos teoremas a seguir usaremos as seguintes hipóteses: sejam A um domínio de Dedekind e K seu corpo de frações, K de característica zero. Sejam $K' \supset K$ uma extensão Galoisiana de grau n com G o grupo de Galois de K' sobre K e A' o fecho integral de A em K' .

Teorema 19. *Se p é um ideal primo de A então os ideais primos P_i de A' que aparecem na fatoração de $A'p$ como produto de ideais primos de A' são todos conjugados. Eles possuem o mesmo índice de ramificação f e o mesmo grau de inércia e . Assim*

$$A'p = \left(\prod_{i=1}^q P_i \right)^e$$

e $n = efq$.

Demonstração: [6], pág. 89.

Definição 20. *Seja P_i um ideal primo sobre p . O conjunto D dos $\sigma \in G$ tais que $\sigma(P_i) = P_i$ é chamado de grupo de decomposição de P_i . O subgrupo normal I de D composto dos elementos de G que satisfazem $\sigma(x) - x \in P_i$ para todo $x \in A'$ é chamado de subgrupo de inércia de P_i .*

Teorema 21. *Seja P' um ideal maximal de A' e assumamos que A/p é finito ou de característica zero. Então A'/P' é uma extensão Galoisiana de grau f de A/p e a aplicação $\sigma \rightarrow \bar{\sigma}$ é um homomorfismo sobrejetor de D no grupo de Galois de A'/P' sobre A/p . Além disso, $|I| = e$. Assim*

$$\frac{D}{I} \cong \text{Gal}(A'/P'/A/p).$$

Demonstração: [6] pág. 90.

Corolário 22. *Um ideal primo p de A não se ramifica em A' se, e somente se, o grupo de inércia I de P' é trivial para todo P' sobre p .*

1.2 O corpo $\mathbb{Q}_p$

Definição 23. *Seja $(G, +, \leq)$ um grupo ordenado e ∞ um símbolo formal satisfazendo $g + \infty = \infty$ e $g < \infty$ para todo $g \in G \cup \{\infty\}$. Uma valorização v de um corpo K com valores em G é uma aplicação $v : K \rightarrow G$ que satisfaz*

- $v(xy) = v(x) + v(y)$;

- $v(x + y) \geq \min\{v(x), v(y)\}$;
- $v(x) = \infty \Leftrightarrow x = 0$.

Se v é identicamente zero em K^* dizemos que a valorização v é trivial.

Se G é um subgrupo discreto de $\mathbb{R}$ (por exemplo $\mathbb{Z}$), dizemos que v é uma valorização discreta e chamamos K de corpo de valorização discreta.

O conjunto $A = \{x \in K \text{ tal que } v(x) \geq 0\}$ é um anel local, chamado de anel de valorização de K (anel de valorização discreta, no caso de v ser discreta). Seu ideal maximal é o conjunto $M = \{x \in K \text{ tal que } v(x) > 0\}$, que é principal; qualquer gerador deste ideal é chamado de uniformizante local de v .

Exemplo 24. Seja $p \in \mathbb{Z}$ primo. Dado $x \in \mathbb{Q}$ podemos escrever $x = p^n \cdot \frac{r}{s}$, com $n \in \mathbb{Z}$ e $\frac{r}{s} \in \mathbb{Q}$ tal que $(p, r) = (p, s) = 1$. Defina $v_p(x) = n$. Isso define uma valorização discreta em $\mathbb{Q}$.

Uma construção análoga é obtida se tomarmos $p(x) \in k[x]$, onde k é um corpo e $p(x)$ é irredutível. Dado $f(x) \in k[x]$ podemos escrever $f(x) = p(x)^n \cdot \frac{r(x)}{s(x)}$, com $n \in \mathbb{Z}$ e com $r(x), s(x) \in k[x]$ tais que $(p(x), r(x)) = (p(x), s(x)) = 1$. Definimos $v_{p(x)} = n$, que é uma valorização discreta em $k(x)$.

Usando a valorização podemos definir uma norma em um corpo:

Definição 25. Seja v uma valorização em um corpo k . Defina uma norma em k por:

$$|x|_v = p^{-v(x)}$$

onde $p \in \mathbb{Z}$ é primo e $p^{-\infty} = 0$.

É fácil ver que $|\cdot|_p$ define uma norma em k .

Obtemos assim nossa primeira definição de $\mathbb{Q}_p$. Seja $\mathbb{Q}$ o corpo dos números racionais, $v_p(x)$ uma valorização definida como no exemplo 24 e $|x|_v = p^{-v_p(x)}$ uma norma em $\mathbb{Q}$. Observe que $(\mathbb{Q}, |\cdot|_{v_p})$ não é um espaço métrico completo.

Definição 26. $\mathbb{Q}_p$ é o completamento do espaço métrico $(\mathbb{Q}, |\cdot|_v)$.

Outra maneira de definir $\mathbb{Q}_p$ é através do limite projetivo.

Definição 27. Um conjunto parcialmente ordenado $(I, \leq)$ é direto se dado qualquer par $i, j \in I$, existe $k \in I$ tal que $i \leq k$ e $j \leq k$.

Definição 28. Seja $(I, \leq)$ um conjunto ordenado direto. Um sistema projetivo de grupos (ou anéis, ou espaços topológicos,...) é uma família de grupos $(G_i)_{i \in I}$ e aplicações $\phi_{ji} : G_j \rightarrow G_i$, $i \leq j$, tais que

1. $\phi_{ii} = id_{G_i}$, para todo $i \in I$;
2. $\phi_{ki} = \phi_{ji} \circ \phi_{kj}$ para toda tripla $i \leq j \leq k$ em I .

O limite projetivo sobre um sistema projetivo é um grupo (ou anel, ou espaço topológico,...)

$$G = \varprojlim_{i \in I} G_i$$

junto com aplicações $\phi_i : G \rightarrow G_i$ tais que o diagrama

$$\begin{array}{ccc} G & \xrightarrow{\phi_j} & G_j \\ & \searrow \phi_i & \downarrow \phi_{ji} \\ & & G_i \end{array}$$

comuta pra todo $i \leq j$.

O limite projetivo é caracterizado pela seguinte propriedade universal: dado um grupo T e morfismos $g_i : T \rightarrow G_i$ tais que $g_i = \phi_{ji} \circ g_j$ para todo $i \leq j$, então existe um único $g : T \rightarrow G$ tal que $g_i = \phi_i \circ g$ para todo $i \in I$.

Uma construção para G é como o subgrupo do produto $\prod_{i \in I} G_i$ das uplas "coerentes", isto é,

$$G = \{(\sigma_i) \in \prod_{i \in I} G_i \mid \phi_{ji}(\sigma_j) = \sigma_i \text{ para todo } i \leq j\}.$$

Definimos $\mathbb{Z}_p$, o anel dos inteiros p-ádicos como:

$$\mathbb{Z}_p = \varprojlim_{n \in \mathbb{N}} \frac{\mathbb{Z}}{(p^n)} \cong \{(f_n) \in \prod_{n \in \mathbb{N}} \frac{\mathbb{Z}}{(p^n)} \mid f_m \equiv f_n \pmod{p^n} \text{ para todo } n \geq m\}$$

Seja $f = (f_n) \in \mathbb{Z}_p$, escolha F_n o único representante de $f_n \in \frac{\mathbb{Z}}{(p^n)}$ com $0 \leq F_n \leq p^n$.

Escrevendo F_n na base p temos

$$F_n = a_0 + a_1p + a_2p^2 + \dots + a_{n-1}p^{n-1}, \quad 0 \leq a_i < p.$$

Para todo $m \leq n$ é possível escolher F_m , um único representante de f_m tal que $0 \leq F_m \leq p^m$. Como $F_m = F_n \pmod{p^m}$ temos

$$F_m = a_0 + a_1p + a_2p^2 + \dots + a_{m-1}p^{m-1}, \quad 0 \leq a_i < p.$$

Podemos ver F_m como F_n truncado no $(m+1)$ -ésimo termo. Logo um inteiro p-ádico corresponde unicamente a sequência de inteiros da forma

$$(a_0, a_0 + a_1p, a_0 + a_1p + a_2p^2, \dots) \quad 0 \leq a_i < p$$

que é mais usualmente denotado por

$$a_0 + a_1p + a_2p^2 + \dots \quad \text{com } 0 \leq a_i < p.$$

Definição 29. $\mathbb{Q}_p$ é o corpo de frações de $\mathbb{Z}_p$

Em $\mathbb{Q}_p$ podemos definir a valorização $v(f) = n \in \mathbb{Z}$ se f possui a fatoração $f = p^n \cdot u$ com $u \in \mathbb{Z}_p^*$. Note que se $f = a_0 + a_1p + a_2p^2 + \dots$ com $0 \leq a_i < p$ então $v(f) = \min\{n \in \mathbb{Z} \mid a_n \neq 0\}$.

$\mathbb{Q}_p$ é um espaço métrico completo com a norma $|x|_{(v)} = q^{-v(x)}$, $q \in \mathbb{Z}$ primo.

Teorema 30. (Lema de Hensel.)

Seja K um corpo de valorização completo com anel de valorização de A . Seja M seu ideal maximal e $f(x) \in A[x]$ um polinômio mônico de grau n sobre A . Para cada polinômio $h(x) \in A[x]$, denotaremos por $\bar{h}$ a redução do polinômio módulo M . Se $\alpha(x)$ e $\alpha'(x)$ são mônicos e relativamente primos sobre A/M de grau r e $n - r$ respectivamente, tais que $\bar{f}(x) = \alpha(x)\alpha'(x)$, então existem dois polinômios mônicos $g(x), g'(x) \in A[x]$, relativamente primos, de graus r e $n - r$ respectivamente, tais que $\bar{g}(x) = \alpha(x)$ e $\bar{g}'(x) = \alpha'(x)$ e $f(x) = g(x)g'(x)$.

Demonstração: [10], pg. 279.

Corolário 31. Mantendo a notação do teorema e tomando v como a valorização de K , se $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ é um polinômio irredutível em $K[x]$ então

$$\min_{1 \leq i \leq n} \{v(a_i)\} = \min\{v(a_0), v(a_n)\}.$$

Em particular, se $a_n = 1$ e $a_0 \in A$ então $a_i \in A$ para todo i .

Demonstração: Escolha i o menor inteiro tal que o mínimo de $\{v(a_j), 0 \leq j \leq n\}$ seja atingido. Suponha que $0 < i < n$ e defina $p(x) = a_i^{-1}f(x)$. Como $v(a_i) \leq v(a_j)$ então $v(a_i^{-1} \cdot a_j) = v(a_j) - v(a_i) \geq 0$, logo $p(x) \in A[x]$. Além disso $\bar{p}(x) \neq 0$ em A/M , pois o coeficiente de x^i é igual a 1. Para todo elemento em que o mínimo não é atingido em f o corresponde em $\bar{p}$ se anula, e isso acontece para todo $j < i$, pela definição de i . Então $\bar{p}(x) = x^i g_0(x)$, com $g_0(0) = 1$ e g_0 e x^i primos entre si (g_0 é não constante pois $i < n$ e $g_0 \neq \bar{p}$ pois $i > 1$). Logo, pelo lema de Hensel, $p(x)$ se fatora de maneira não trivial e portanto $f(x)$ não é irredutível.

1.3 Corpos locais e suas extensões

Nesta seção nos restringiremos a valorizações em corpos locais.

Definição 32. Um corpo local é uma extensão finita L , de $\mathbb{Q}_p$ ou de $F_p((t))^1$.

O primeiro resultado sobre corpos locais é que a extensão de uma valorização é única e podemos explicitar sua fórmula a partir da valorização do corpo base.

¹ $F_p((t)) =$ corpo de frações de $(F_p[[t]])$, onde $F_p[[t]] \cong \varprojlim_{n \in \mathbb{N}} \frac{F_p[t]}{(t^n)}$, F_p o corpo de p elementos

Teorema 33. *Seja K um corpo local com valorização v e L uma extensão finita de K . Então existe uma única valorização w em L estendendo v . Ela é dada por*

$$w(x) = \frac{1}{[L : K]} \cdot v(N_{L/K}(x)) \quad \text{para } x \in L.$$

Além disso, L é completo com respeito a w .

Demonstração: Seja O_K o anel de valorização de K e B o fecho integral de O_K em L .

1. Vamos mostrar que

$$B = \{x \in L \mid N_{L/K}(x) \in O_K\}. \quad (1.1)$$

Como O_K é DFU então O_K é integralmente fechado em K , logo se $x \in B$ então $N_{L/K}(x) \in B \cap K = O_K$, logo $B \subseteq \{x \in L \mid N_{L/K}(x) \in O_K\}$.

Seja $x \in L$ tal que $N_{L/K}(x) \in O_K$, isto é $v(N_{L/K}(x)) \geq 0$. Seja $f(t) = t^n + a_{n-1}t^{n-1} + \dots + a_2t^2 + a_1t + a_0$ o polinômio minimal de x sobre K . Usando a definição 5, $N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x)$, e o fato de a_0 ser o produto das raízes do polinômio minimal, temos $N_{L/K}(x) = \pm a_0^m, m > 0$. Logo $v(a_0) \geq 0$. Pelo corolário 31 concluimos que $f(t) \in O_K[t]$, ou seja $x \in B$.

2. Vamos mostrar que a fórmula (1.1) define de fato uma valorização em L . Sejam $x, y \in L$

- $w(x.y) = \frac{1}{[L:K]} \cdot w(N_{L/K}(x.y)) = \frac{1}{[L:K]} \cdot (w(N_{L/K}(x)) + w(N_{L/K}(y))) = w(x) + w(y)$
- $w(x) = \infty \Leftrightarrow v(N_{L/K}(x)) = \infty \Leftrightarrow N_{L/K}(x) = 0 \Leftrightarrow x = 0$
- Observe que se $w(x) \geq 0$ então $w(1+x) \geq 0$. De fato,

$$w(x) = \frac{v(N_{L/K}(x))}{[L : K]} \geq 0 \Rightarrow x \in B \Rightarrow 1+x \in B \Rightarrow w(1+x) \geq 0.$$

Portanto, se $w(x) \geq w(y) \Rightarrow (x/y) \geq 0 \Rightarrow w(1+x/y) \geq 0 \Rightarrow w(y+x) \geq w(y) = \min\{w(x), w(y)\}$.

3. Unicidade:

Suponha que exista w' uma outra valorização em L estendendo w . Então existe um elemento $b \in L$ tal que $w(b) \geq 0$ e $w'(b) < 0$ ([2], pág. 26). Note que $b \in B$. Seja $f(t) = t^n + a_{n-1}t^{n-1} + \dots + a_1t + a_0$ o polinômio minimal de b sobre K . Como O_K é integralmente fechado $f(t) \in O_K[t]$ ([6], pág. 38). Como $w(b^n) < w(a_i b^i)$, $1 \leq i \leq n$, temos:

$$0 \leq v(a_0) = w'(a_0) = w'(-b^n - a_{n-1}b^{n-1} - \dots - a_1b) = w(b^n) < 0.$$

O que é um absurdo.

4. (L, w) é um espaço métrico completo:

Sejam $\omega_1, \dots, \omega_n$ uma base de L sobre K e $(x_i)_{i \geq 1}$ uma sequência de Cauchy em L . Escreva cada termo da sequência na base escolhida: $x_i = y_{i1}\omega_1 + \dots y_{in}\omega_n, y_{ij} \in K$.

Como K é completo e L é de dimensão finita sobre K , então todas as normas de L são equivalentes.

Usando a norma do sup considere a sequência $(y_{ij})_{i \geq 1}$. Mostremos que ela é de Cauchy: seja $\epsilon > 0$, como $(x_i)_{i \geq 1}$ é de Cauchy

$$\sup_{1 \leq k \leq n} \{|y_{ik} - y_{jk}|\} = |x_i - x_j| < \epsilon$$

Logo, fixado l temos

$$|y_{il} - y_{jl}| \leq \sup_{1 \leq k \leq n} \{|y_{ik} - y_{jk}|\} < \epsilon$$

Como K é completo então cada sequência $(y_{ij})_{i \geq 1}$ converge para $y_j \in K$ e portanto, $(x_{ij})_{i \geq 1}$ converge para $x = y_1\omega_1 + \dots y_n\omega_n$ em L . ■

A seguir definiremos o índice de ramificação e o grau de inércia para corpos locais.

Definição 34. *Sejam K um corpo local com valorização v , L uma extensão finita de K e w a extensão única de v a L . Sejam π e Π os uniformizantes locais e k e l os corpos residuais de K e L , respectivamente. Definimos o índice de ramificação, $e_{L/K}$, da extensão $L \supset K$ como o índice da imagem de v como subgrupo da imagem de w :*

$$e_{L/K} = [w(L^*) : v(K^*)]$$

Observe que, como v é a restrição de w , podemos ver k como subcorpo de l . O grau de inércia, $f_{L/K}$, da extensão $L \supset K$ é o grau da extensão de corpos:

$$f_{L/K} = [l : k].$$

Afirmção 35. *Seguindo a notação da definição 34, temos:*

$$\pi = u.\Pi^{e_{L/K}}, \text{ para } u \in L \text{ e } w(u) = 0.$$

Demonstração: Como $\pi \in (\Pi)$ escreva $\pi = u.\Pi^e$, tal que Π não divida u . Logo $w(u) = 0$. Logo $w(\pi) = ew(\Pi)$. Basta mostrar que $\{0, v(\Pi), 2v(\Pi), \dots, (e-1)v(\Pi)\}$ é um sistema de representantes para $H = w(L^*)/v(K^*)$. Dado $x + v(K^*) \in H$ qualquer, podemos escrever $w(x) = w(u\Pi^m)$, para algum $m \geq 0$. Usando o algoritmo da divisão

temos $m = q.e + s$ com $q \in \mathbb{Z}$ e $0 \leq s < e$. Assim, $w(x) = q.w(\Pi^e) + sw(\Pi)$. Portanto $w(x) \equiv sw(\Pi) \pmod{v(K^*)}$ com $0 \leq s < e$. ■

Como o índice de subgrupo e o grau de extensões de corpos são multiplicativos então o índice de ramificação e o grau de inércia também são. Dadas extensões finitas de corpos locais $M \supset L \supset K$ temos

$$e_{M/K} = e_{M/L} \cdot e_{L/K} \quad \text{e} \quad f_{M/K} = f_{M/L} \cdot f_{L/K}.$$

Definição 36. Uma extensão de corpos locais $L \supset K$ é não-ramificada se seu índice de ramificação é 1, $e_{L/K} = 1$. Uma extensão de corpos locais é totalmente ramificada se o índice de ramificação é $[L : K]$.

Lema 37. Seja K um corpo local com valorização v . Defina a norma $|x|_p = p^{-v(x)}$ com p primo. Valem as seguintes propriedades:

1. $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.
2. A série $\sum_n f_n$ converge em $K \Leftrightarrow |f_n| \rightarrow 0$.

Demonstração: 1- Imediato da definição de valorização.

2- ($\Rightarrow$) vale para todo espaço métrico

($\Leftarrow$) Seja n_0 tal que $|f_n|_p < \epsilon$ para todo $n > n_0$. Então, se $m > n > n_0$ temos

$$\left| \sum_{i=1}^m f_i - \sum_{j=1}^n f_j \right|_p = |f_m - f_{m-1} + \dots + f_{n+2} + f_{n+1}|_p \leq \max_{n+1 \leq i \leq m} \{|f_i|_p\} < \epsilon$$

Logo $\sum_n f_n$ é de Cauchy e, como K é completo, $\sum_n f_n$ converge. ■

Os anéis de valorização dos corpos locais são casos particulares de domínios de Dedekind ([6] pág. 44). No caso dos Corpos Locais os ideais maximais de O_K surgem a partir dos anéis de valorização de K . Fixada uma extensão de L de K existe uma única valorização w de L que estende v de K . Assim, suspeitamos que o mesmo aconteça com os primos acima de (π) . Isso fica explicitado no teorema:

Teorema 38. Seja $L \supset K$ uma extensão de corpos locais de grau n . Seja v a valorização em K e w sua única extensão a L . Denote por O_K e O_L os anéis de valorização de v e w . Sejam π e Π os uniformizantes locais de v e w , e k e l os corpos residuais de A e B respectivamente. Então:

- O índice de ramificação e o grau de inércia da extensão $L \supset K$ são finitos;
- O_L é o fecho integral de O_K em L e é O_K -módulo livre de posto n ;
- Uma base de O_L como O_K -módulo é dada por $\{w_i \Pi^j | 1 \leq i \leq f, 0 \leq j < e\}$, onde $w_1, \dots, w_f \in O_L$ são representantes de uma base de l sobre k ;

- Em particular, temos a relação

$$ef = n.$$

Demonstração: Para facilitar as contas vamos normalizar $v(\pi) = 1$, então $w(\Pi) = 1/e$. Sejam $\omega_1, \dots, \omega_r \in O_L$ cujas imagens em l são independentes sobre k , queremos mostrar que o conjunto $\{\omega_i \Pi^j \text{ tal que } 1 \leq i \leq r, 0 \leq j \leq e\}$ é linearmente independente (l.i.) sobre K .

Suponha $\sum_{i,j} a_{ij} \omega_i \Pi^j = 0$ com $a_{ij} \in K$ não todos nulos. Multiplique a equação, eliminando os denominadores, de maneira que $a_{ij} \in O_K$ e pelo menos um deles seja uma unidade. Seja j_0 o menor inteiro tal que $a_{ij_0} \in O_K^*$ para pelo menos um i . Logo $\sum_i a_{ij_0} \omega_i \neq 0 \pmod{\Pi}$, pois os elementos que são unidades não pertencem a Π e ω_i 's são l.i mod Π . Então

$$w\left(\sum_i a_{ij} \omega_i \Pi^j\right) > w\left(\sum_i a_{ij_0} \omega_i \Pi^{j_0}\right) = \frac{j_0}{e}, \forall j \neq j_0.$$

Justificando a afirmação acima:

- se $j > j_0$:

$$w\left(\sum_i a_{ij} \omega_i \Pi^j\right) = w\left(\Pi^j \left(\sum_i a_{ij} \omega_i\right)\right) = jw(\Pi) + w\left(\sum_i a_{ij}\right) > j_0 w(\Pi) + w\left(\sum_i a_{ij}\right) \geq j_0 w(\Pi) = w\left(\sum_i a_{ij_0} \omega_i \Pi^{j_0}\right),$$

- se $j < j_0$ então $\sum_i a_{ij} \omega_i \in \pi O_L$, logo

$$w\left(\sum_i a_{ij} \omega_i \Pi^j\right) = \sum_i u_{ij} \omega_i \cdot \pi \Pi^j = w(\Pi^{j+e} (\sum v_{ij} \omega_i)) = (j+e)w(\Pi) + w(\sum v_{ij} \omega_i) > 1 \geq \frac{j_0}{e}.$$

Portanto $\sum_{i,j} a_{ij} \omega_i \Pi^j > 0$, que é uma contradição. Observe que:

1. Afirmação 1: $w(b) \geq 1 \Leftrightarrow b \in \pi O_L$. De fato,

$$-w(b) \geq 1 \Rightarrow b = u \Pi^m \Rightarrow \frac{m}{e} \geq 1 \Rightarrow m \geq e \Rightarrow b = u \Pi^{e+\xi} = (u \Pi^\xi) \pi.$$

$$-b = \pi O_L \Rightarrow b = \pi b' = \Pi^e b' \Rightarrow w(b) = w(\Pi^e) + w(b') = 1 + w(b') \geq 1.$$

2. Afirmação 2: $O_L/\pi O_L$ é gerado sobre k pelas imagens de $\omega_i \Pi^j$ com $1 \leq i \leq f$ e $1 \leq j \leq e$. De fato, pelo item anterior podemos considerar $b \in O_L - \pi O_L$ tal que $0 \leq w(b) < 1$. Temos que b é da forma $b = u \Pi^j$ com $j = e.w(b)$ e $u \in O_L^*$ uma unidade. Como $\{\omega_1, \dots, \omega_f\}$ é base de l sobre k , podemos encontrar $a_{ij} \in O_K$ tal que $u \equiv \sum_i a_{ij} \omega_i \pmod{\Pi}$. Portanto $b = \Pi^j (\sum_i a_{ij} \omega_i + b' \Pi) = \sum_i a_{ij} \omega_i \Pi^j + b''$, com $w(b'') \geq \frac{j+1}{e} > w(b)$. Se $w(b'') \geq 1$ acabou, caso contrário repito o processo para b'' , e assim por diante até que $w(b^{(k)}) \geq 1$.

Mostremos que todo elemento $b \in O_L$ pode ser escrito como uma combinação O_K -linear de $\{\omega_i \Pi^j \text{ tal que } 1 \leq i \leq f, 0 \leq j \leq e\}$ (de maneira única, pois o conjunto é l.i.).

Seja $b \in O_L$ qualquer, pelas observações anteriores podemos escrever

$$b = c_0 + b_1\pi,$$

com c_0 gerado pelo conjunto $\{\omega_i\Pi^j \text{ tal que } 1 \leq i \leq f, 0 \leq j \leq e\}$. O mesmo vale para b_1 :

$$b = c_0 + c_1\pi + b_2\pi^2,$$

com c_1 gerado pelo conjunto $\{\omega_i\Pi^j \text{ tal que } 1 \leq i \leq f, 0 \leq j \leq e\}$. Prosseguindo indutivamente:

$$b = c_0 + c_1\pi + \dots + c_n\pi^n + b_{n+1}\pi^{n+1}.$$

Como o a norma do último termo vai para zero, $|b_{n+1}\pi^{n+1}| \rightarrow 0$, então pelo lema 37 $b = \sum_{i=0}^{\infty} c_i$. Logo b é O_K -gerado pelo conjunto $\{\omega_i\Pi^j \text{ tal que } 1 \leq i \leq r, 0 \leq j \leq e\}$. Portanto, O_L é um O_K -módulo livre de posto ef .

Agora, dado $l \in L$ qualquer, seja m suficientemente grande tal que $l\pi^m \in O_L$, logo $l\pi^m = \sum_{i,j} a_{ij}\omega_i\Pi^j$, como L é corpo $l = \pi^{-m}(\sum_{i,j} a_{ij}\omega_i\Pi^j)$. Portanto $ef = n$. ■

Nos teoremas seguintes desta seção usaremos a seguinte notação:

$$O_K = \text{anel de valorização de } v = \{x \in K | v(x) \geq 0\}.$$

$$m_K = \text{ideal maximal de } O_K = \{x \in O_K | v(x) > 0\}.$$

Teorema 39. *Sejam K um corpo local e $L \supset K$ uma extensão não-ramificada finita. Seja K' uma extensão arbitrária finita de K . Se $L' = LK'$ é o compositum de L e K' (em algum fecho algébrico de K) então $L' \supset K'$ é não-ramificada.*

Demonstração: Sejam k, k', l e l' os corpos residuais de K, K', L e L' respectivamente. Como O_L é finitamente gerado como O_K -módulo então $O_L = O_K[\theta]$ com $\theta \in O_L$ tal que $\bar{\theta} \in l$ é um elemento primitivo sobre k . Como O_L é integral sobre O_K , temos que θ é integral sobre O_K e sobre $O_{K'}$, que são anéis integralmente fechados, logo os polinômios minimais $p(x)$ e $q(x)$ de θ sobre K e K' pertencem a $O_K[x]$ e $O_{K'}[x]$ respectivamente. Além disso, a imagem de $\bar{p}(x) \in k[x]$ é o polinômio minimal de $\bar{\theta}$, se não fosse assim, teríamos uma fatoração de $\bar{p}(x) \in k(x)$ em fatores de grau maior que 1, o que implicaria, pelo lema de Hensel, que $p(x)$ pode ser fatorado. Logo $\deg(p(x)) = \deg(\bar{p}(x)) = [L : K] = [l : k]$. Como $q(x)|p(x)$ em $O_{K'}[x]$ então $\bar{q}(x)|\bar{p}(x)$ em $k'[x]$. Como k é um corpo perfeito então $\bar{p}(x)$, e consequentemente $\bar{q}(x)$, é separável. Como $q(x)$ é irredutível então pelo lema de Hensel $\bar{q}(x)$ é irredutível em $k'[x]$ e portanto é o polinômio minimal de $\bar{\theta} \in l'$ sobre k' . Portanto, como $L' = K'(\theta)$ temos que

$$f_{L'/K} \geq [k'(\bar{\theta}) : k'] = \deg(\bar{q}(x)) = \deg(q(x)) = [L' : K'].$$

Por outro lado, $f_{L'/K'} \leq [L'/K']$ em geral, então vale a igualdade, provando que $L' \supset K'$ é não ramificada. ■

Definição 40. *Sejam $L \supset K$ uma extensão Galoisiana de corpos locais com $G = \text{Gal}(L/K)$, O_L o anel de valorização de L e m_L seu ideal maximal. O grupo de decomposição de L/K é o grupo*

$$D_{L/K} = \{\sigma \in G \text{ tal que } \sigma(m_L) = m_L\}.$$

O grupo de inércia de L/K , é o subgrupo normal do grupo de $D_{L/K}$ dado por

$$I = \{\sigma \in D_{L/K} \text{ tal que } \sigma(x) - x \in m_L \text{ para todo } x \in O_L\}.$$

Teorema 41. *Seja $L \supset K$ uma extensão Galoisiana de corpos locais com $G = \text{Gal}(L/K)$ e seja $l \supset k$ a extensão dos correspondentes corpos residuais. Seja I o grupo de inércia desta extensão. Denote por $\bar{\sigma} \in \text{Gal}(l/k)$ o automorfismo induzido por $\sigma \in G$ em l , o corpo residual do anel de valorização de L . Então*

1. *A aplicação $\sigma \rightarrow \bar{\sigma}$ induz um isomorfismo entre G/I e $\text{Gal}(l/k)$. Em particular temos $|I| = e_{L/K}$.*
2. *O corpo fixo por I , $M = L^I$, é a extensão maximal não-ramificada de K contida em L . Em particular, M é Galoisiana sobre K com grupo de Galois cíclico $G/I \cong \text{Gal}(l/k)$.*

Dado o teorema anterior temos o seguinte diagrama:

$$\begin{array}{ccc} & L & \\ \text{totalmente ramificada} & \downarrow e & \\ & M & \\ \text{não-ramificada} & \downarrow f & \\ & K & \end{array}$$

Demonstração:

1. Defina a aplicação $\phi : G \rightarrow \text{Gal}(l/k)$ dada por $\phi(\tau) = \bar{\tau}$. Mantendo a notação do teorema 39 considere $\theta \in O_L$ tal que $k(\bar{\theta}) = l$. Seja $p(x) \in O_K[x]$ o polinômio minimal de θ e $q(x) \in k[x]$ o polinômio minimal de $\bar{\theta}$. Logo $q(x) | \bar{p}(x)$ em $k[x]$. Segue que todas as raízes de $q(x)$ são da forma $\bar{a}$ com $p(a) = 0$ e $a \in K$.

Todo elemento $\tau_0 \in \text{Gal}(l/k)$ é determinado por sua ação em $\bar{\theta}$, que é o elemento primitivo da extensão. Suponha que $\tau_0(\bar{\theta}) = \bar{\theta}^j$ para algum $j \geq 0$, tome $\tau \in G$ tal que $\tau(\theta) = \theta^j$, então $\phi(\tau) = \tau_0$. Portanto ϕ é sobrejetora. Além disso,

$$\ker \phi = \{\tau \in G \text{ tal que } \tau(x) = x, \forall x \in l = O_L/m_L\} = I.$$

Portanto ϕ induz um isomorfismo $\frac{G}{I} \cong \text{Gal}(l/k)$.

Temos $e_{L/K} \cdot f_{L/K} = |G| = |I| \cdot |\text{Gal}(l/k)| = |I| \cdot f_{L/K}$.

2. Seja k' o corpo residual de $M = L^I$. Por definição o grupo de inércia da extensão $M \supset L$ é:

$$I' = \{\tau \in \text{Gal}(L/M) \text{ tal que } \tau(x) - x \in m_L, \forall x \in O_L\}.$$

Claramente $I' \subset I$ e dado $\sigma \in I$, σ fixa M pela definição de M , logo $\sigma \in I'$. Então $e_{L/K} = e_{L/M}$. Segue que $f_{L/M} = 1$, o seja M e L possuem o mesmo corpo residual l , logo $f_{M/K} = f_{L/K}$. Assim, M é uma extensão Gaolisiana de grau $f_{L/K}$. Como o índice de ramificação é multiplicativo então $e_{M/K} = 1$, provando que M é a extensão maximal ramificada de K contida em L . ■

1.4 Regra do sinal de Descartes

Teorema 42. *Regra do sinal de Descartes [7]*

O número de raízes reais positivas de um polinômio com coeficientes reais é igual ao número de trocas de sinal na lista dos seus coeficientes ou é menor que esse número por um múltiplo de 2. Como as raízes negativas da equação $f(x) = 0$ são raízes positivas de $f(-x) = 0$ a regra também serve para contar as raízes negativas.

Demonstração: Seja f um polinômio de grau n . Sem perda de generalidade podemos supor

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad a_0 \neq 0.$$

Definimos:

- $V[f(x)]$ = O número de variações de sinal dos coeficientes,
- $P[f(x)]$ = O número de raízes positivas de $f(x)$.

Analisemos o caso linear. Suponha $f(x) = x + a_0$ cuja raiz é $-a_0$, que é positiva quando a_0 é negativo e vice-versa.

Sinal de a_0	$V[f(x)]$	$P[f(x)]$
+	0	0
-	1	1

Observe que:

$$\text{Se } a_0 < 0 \text{ então } V[f(x)] \text{ é ímpar e se } a_0 > 0 \text{ então } V[f(x)] \text{ é par.} \quad (1.2)$$

Mostraremos, por indução sobre o grau do polinômio f , que:

$$\text{Se } a_0 < 0 \text{ então } P[f(x)] \text{ é ímpar e se } a_0 > 0 \text{ então } P[f(x)] \text{ é par.} \quad (1.3)$$

Seja $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, a_0 \neq 0$. O caso $n = 1$ segue do caso linear. Agora suponha que a hipótese de indução é válida para todo polinômio de grau menor que n

- Se $a_0 < 0$.

Como $f(0) = a_0 < 0$ e f é contínua então f tem uma raiz no intervalo $(0, +\infty)$. Podemos fatorar $f(x) = (x - p)g(x)$ com $p > 0$ e $\deg(g) < \deg(f)$. Se c é o termo constante de g então $c > 0$ ($-cp = a_0$). Logo $P[g(x)]$ é par e conseqüentemente

$$P[f(x)] = P[(x - p)g(x)] = P[g(x)] + 1$$

é ímpar.

- Se $a_0 > 0$.

Se f não possui raízes positivas o resultado é válido.

Se f possui uma raiz positiva podemos fatorar $f(x) = (x - p)g(x)$ com $p > 0$ e $\deg(g) < \deg(f)$. Se c é o termo constante de g então $c < 0$ ($-cp = a_0$). Logo $P[g(x)]$ é ímpar e conseqüentemente

$$P[f(x)] = P[(x - p)g(x)] = P[g(x)] + 1.$$

Portanto $P[f(x)]$ é par.

Portanto, por (1.2) e (1.3), $V[f(x)]$ e $P[f(x)]$ diferem por um múltiplo inteiro de 2.

Mostremos por indução sobre $V[f(x)]$ que dado $p > 0$ real então $V[f(x)(x - p)] > V[f(x)]$.

Se $V[f(x)] = 0$, isto é, todos os coeficientes são maiores ou iguais a zero, então $V[f(x)(x - p)] > 0$, pois o termo constante de $f(x)(x - p)$ é negativo. Suponha o resultado válido para todo polinômio $h(x)$ com $V[h(x)] < l$ e seja $f(x)$ tal que $V[f(x)] = l > 0$. Seja $k = \max\{j, \text{ tal que } a_j < 0\}$, ou seja, a primeira troca de sinal da esquerda para direita. Então

$$\begin{aligned} f(x)(x - p) &= (x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0)(x - p) \\ &= \underbrace{(x^n + \dots + a_{k+1}x^{k+1})(x - p)}_I + \underbrace{(a_kx^k + \dots + a_1x + a_0)(x - p)}_{II}. \end{aligned}$$

Temos:

(I) $= x^{n+1} + \dots - pa_{k+1}x^{k+1}$ tem uma troca de sinal,

(II) $= a_{k+1}x^{k+1} + \dots + a_0p$ que por hipótese de indução possui mais de l trocas de sinal.

Portanto, na lista dos coeficientes de $f(x)(x - p)$ há pelo menos $l + 1$ trocas de sinal.

Concluindo: seja $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, $a_0 \neq 0$. Se $p_1, p_2, \dots, p_m$ são raízes positivas de $f(x)$, então $f(x) = N(x)(x - p_1)(x - p_2) \cdots (x - p_m)$, onde $N(x)$ não possui raízes positivas (mas pode ter trocas de sinal).

$$\begin{aligned}
V[N(x)(x - p_1)(x - p_2) \cdots (x - p_m)] &\geq V[N(x)(x - p_1)(x - p_2) \cdots (x - p_{m-1})] + 1 \\
&\geq V[N(x)(x - p_1)(x - p_2) \cdots (x - p_{m-2})] + 2 \\
&\geq \cdots \\
&\geq V[N(x)(x - p_1)] + m - 1 \\
&\geq V[N(x)] + m \\
&\geq m.
\end{aligned}$$

Portanto

$$V[f(x)] \geq m = P[f(x)].$$

■

O polinômio $x^n - x^{n-1} - \dots - x - 1$

2.1 Origem do polinômio

A sequência de Fibonacci é bem conhecida: 1, 1, 2, 3, 5, 8..., obtida somando os dois termos anteriores para se obter o próximo. Podemos formalizar essa definição: fixando elementos iniciais a_0 e a_1 , a sequência de Fibonacci é dada por:

$$a_n = a_{n-2} + a_{n-1}.$$

Defina $b_n = \frac{a_{n+1}}{a_n}$. A sequência $\{b_n\}$ converge e vale a fórmula $b_{n+1}b_n = b_n + 1$. Logo o limite da sequência satisfaz

$$x^2 = x + 1,$$

que é o caso $n=2$ do polinômio que investigamos. Se generalizarmos a sequência de Fibonacci e ao invés de somarmos os dois termos anteriores, somarmos k deles, temos:

$$a_{n+k} = a_{n+k-1} + a_{n+k-2} + \dots + a_n.$$

Prosseguindo como no caso anterior definimos a sequência $b_n = \frac{a_{n+1}}{a_n}$.

Observe que:

$$\frac{a_{n+k}}{a_n} = \frac{a_{n+k}}{a_{n+k-1}} \frac{a_{n+k-1}}{a_{n+k-2}} \dots \frac{a_{n+1}}{a_n} = b_{n+k-1}b_{n+k-2}\dots b_{n+1}b_n. \quad (2.1)$$

Além disso,

$$\frac{a_{n+k}}{a_n} = \frac{a_{n+k-1}}{a_n} + \frac{a_{n+k-2}}{a_n} + \dots + \frac{a_{n+1}}{a_n} + \frac{a_n}{a_n}. \quad (2.2)$$

Usando (2.1) e (2.2) temos:

$$b_{n+k-1}b_{n+k-2}\dots b_{n+1}b_n = b_{n+k-2}b_{n+k-3}\dots b_n + b_{n+k-3}b_{n+k-4}\dots b_n + \dots + b_{n+1}b_n.$$

Portanto se $\{b_n\}$ converge então converge para uma raiz de

$$x^k - x^{k-1} - x^{k-2} - \dots - x - 1$$

que é o polinômio que estudaremos.

Defina

$$f_n(x) = x^n - x^{n-1} - \dots - x - 1, n \geq 2$$

e

$$g_n(x) = (x-1)f_n(x) = x^{n+1} - 2x^n + 1, n \geq 2.$$

O polinômio $g_n(x)$ será muito utilizado já que, com exceção de $x = 1$, possui as mesmas raízes de $f_n(x)$.

2.2 Raízes, irredutibilidade e discriminante

Seja $n \geq 2$. Então $f_n(1) = -(n-1)$ e $f_n(2) = g_n(2) = 1$. Logo existe uma raiz, que chamaremos de ϕ_n , entre 1 e 2. Pela regra do sinal de Descartes essa é a única raiz positiva de $f_n(x)$, (teorema 42). Para verificar as raízes negativas usaremos essa regra aplicada à $g_n(-x) = (-x)^{n+1} - 2(-x)^n + 1$. Se n é par $g_n(-x)$ tem uma troca de sinal e portanto uma raiz negativa, logo $f_n(x)$ tem uma raiz negativa (entre -1 e 0 pois $f_n(-1) = 1$ e $f_n(0) = -1$). Se n é ímpar $g_n(-x)$ não tem troca de sinal, logo $f_n(x)$ também não e portanto, ϕ_n é a única raiz real de $f_n(x)$.

Teorema 43. [4] *Sejam f_n e $g_n \in \mathbb{C}[z]$ tal que $f_n(z) = z^n - z^{n-1} - \dots - z - 1$ e $g_n(z) = (z-1)f_n(z)$, para $n \geq 2$. Então*

1. f_n possui um zero real ϕ_n tal que $1 < \phi_n < 2$.

2. Toda raiz $z \neq \phi_n$ de $f_n(x)$ em $\mathbb{C}$ verifica

$$|z| < 1.$$

3. Os zeros de $f_n(z)$ são simples.

Demonstração: 1) Segue da primeira parte desta seção.

2) Como ϕ_n é o único zero real positivo de f_n então, dado $x \in \mathbb{R}$,

$$x > \phi_n \Rightarrow f_n(x) > 0 \text{ e } 0 < x < \phi_n \Rightarrow f_n(x) < 0. \quad (2.3)$$

Além disso, como as duas únicas raízes reais positivas de g_n são 1 e ϕ_n temos

$$x > \phi_n \Rightarrow g_n(x) > 0 \text{ e } 1 < x < \phi_n \Rightarrow g_n(x) < 0. \quad (2.4)$$

Suponha que f_n possua uma raiz complexa z_0 com $|z_0| > |\phi_n|$ então $z_0^n = z_0^{n-1} + \dots + z_0 + 1$. Daí $|z_0|^n \leq |z_0|^{n-1} + \dots + |z_0| + 1$. Portanto $f_n(|z_0|) = |z_0|^n - |z_0|^{n-1} - \dots - |z_0| - 1 \leq 0$. Contradição por (2.3).

Suponha que f_n possua uma raiz complexa z_0 com $1 < |z_0| < \phi_n$, logo

$$g_n(z_0) = z_0^{n+1} - 2z_0^n + 1 = 0 \Rightarrow 2z_0^n = z_0^{n+1} + 1 \Rightarrow 2|z_0|^n = |z_0|^{n+1} + 1 \leq |z_0|^{n+1} + 1.$$

Portanto $g(|z_0|) \geq 0$. Contradição por (2.4).

Assim as raízes de f_n estão no disco fechado de raio 1 centrado no zero ou no círculo de raio $|\phi_n|$ e centro zero.

Seja $z_0 \neq \phi_n$ uma raiz de f_n .

- Se $|z_0| = 1$ então $2 = 2|z_0|^n = |z_0|^{n+1} + 1 \leq |z_0|^{n+1} + 1 = 2$.

Uma propriedade conhecida de números complexos é: dado $a \in \mathbb{C}$ temos, $|a+1| = |a| + 1 \Leftrightarrow a \in \mathbb{R}$. Portanto, $z_0 \in \mathbb{R}$.

- Se $|z_0| = \phi_n$ então $\phi_n^{n+1} + 1 = 2\phi_n^n = 2|z_0|^n = |z_0|^{n+1} + 1 \leq |z_0|^{n+1} + 1 = \phi_n^{n+1} + 1$.

Pelo mesmo argumento do item anterior: $z_0 \in \mathbb{R}$.

Em ambos os casos concluímos que z_0 é real. Contradição, pois ϕ_n é a única raiz real positiva e as raízes reais negativas estão no intervalo $(-1, 0)$.

3) Suponha que z_0 é uma raiz múltipla de f_n , logo é uma raiz múltipla de g_n . Segue que g_n e g'_n tem uma raiz em comum. Mas as raízes de $g'_n(z) = (n+1)z^n - 2nz^{n-1}$ são 0 e $\frac{2n}{n+1}$ ambas racionais. Contradição pois a única raiz racional de g_n é 1. De fato, se $\frac{p}{q}$ é raiz de $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ então $p|a_n$ e $q|a_0$. ■

Corolário 44. *O polinômio $f_n(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração: Suponha que seja possível fatorar $f_n(x)$ em polinômios de grau maior ou igual a 1 em $\mathbb{Z}[x]$. Então $f_n(x) = \varphi(x)\psi(x)$, $\varphi, \psi \in \mathbb{Z}[x]$. Podemos supor $n \geq 4$ e $\deg(\varphi) \geq 2$, $\deg(\psi) \geq 2$ pois f_n não possui raízes inteiras. Seja ϕ_n a raiz positiva de f_n . Podemos supor $\varphi(\phi_n) = 0$. Pelo teorema 3, as raízes de f_n distintas de ϕ_n tem módulo menor que 1, então o mesmo acontece com as raízes de ψ . Então o termo constante de ψ , que é a multiplicação dessas raízes não está em $\mathbb{Z}$. Contradição. Logo $f_n(x)$ é irredutível em $\mathbb{Z}[x]$ e como f_n é primitivo então pelo lema de Gauss f_n é irredutível em $\mathbb{Q}[x]$.

Lema 45. *O discriminante D_n de $g_n(x)$ é*

$$D_n = (-1)^{\binom{n+1}{2}} [(n+1)^{n+1} - 2^{n+1} n^n].$$

Demonstração: Sejam $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ as raízes de $g_n(x)$ em $\mathbb{C}$. Por [1], pág. 81 temos:

$$D_n = (-1)^{\binom{n+1}{2}} \prod_{i=1}^{n+1} g'_n(\alpha_i).$$

Calculando:

$$g'_n(x) = (n+1)x^n - 2nx^{n-1} = x^{n-1}[(n+1)x - 2n].$$

Então

$$\prod_{i=1}^{n+1} g'_n(\alpha_i) = \prod_{i=1}^{n+1} \alpha_i^{n-1} [(n+1)\alpha_i - 2n].$$

Mas $\prod_{i=1}^{n+1} \alpha_i = (-1)^{n+1}$, pois α_i 's são as raízes de g_n .

Substituindo,

$$\prod_{i=1}^{n+1} \alpha_i^{n-1} [(n+1)\alpha_i - 2n] = \left(\prod_{i=1}^{n+1} \alpha_i \right)^{n-1} \prod_{i=1}^{n+1} [(n+1)\alpha_i - 2n] = ((-1)^{n+1})^{n-1} \prod_{i=1}^{n+1} [(n+1)\alpha_i - 2n],$$

colocando $-(n+1)$ em evidência e tirando do produtório temos,

$$((-1)^{n+1})^{n-1} \prod_{i=1}^{n+1} [(n+1)\alpha_i - 2n] = (-1)^{(n+1)(n-1)} (-1)^{n+1} (n+1)^{n+1} \prod_{i=1}^{n+1} \left[\frac{2n}{n+1} - \alpha_i \right],$$

usando que $g_n(x) = \prod_{i=1}^{n+1} (x - \alpha_i)$, temos

$$\prod_{i=1}^{n+1} g'_n(\alpha_i) = (n+1)^{n+1} g_n \left(\frac{2n}{n+1} \right), \text{ pois } n^2 + n \text{ é sempre par.}$$

Calculando

$$g_n \left(\frac{2n}{n+1} \right) = \left(\frac{2n}{n+1} \right)^{n+1} - 2 \left(\frac{2n}{n+1} \right)^n + 1 = \frac{1}{(n+1)^{n+1}} [(n+1)^{n+1} - 2^{n+1} n^n].$$

Portanto

$$D_n = (-1)^{\binom{n+1}{2}} [(n+1)^{n+1} - 2^{n+1} n^n]. \blacksquare$$

Lema 46. *O discriminante d_n de $f_n(x)$ é*

$$d_n = \frac{D_n}{(n-1)^2}.$$

Demonstração: Sejam $1 = \alpha_1, \alpha_2, \dots, \alpha_{n+1}$ raízes de $g_n(x)$. Usando a seguinte fórmula do determinante de g_n ([1] pág. 85):

$$D_n = (-1)^{\frac{(n+1)n}{2}} \prod_{i=1}^{n+1} \prod_{j \neq i} (\alpha_i - \alpha_j)^2.$$

Segue que

$$\begin{aligned}
 D_n &= (-1)^{\binom{n+1}{2}} \prod_{j=2}^{n+1} (1 - \alpha_j)^2 \prod_{i=2}^{n+1} \prod_{j \neq i} (\alpha_i - \alpha_j)^2 \\
 &= \left[\prod_{j=2}^{n+1} (1 - \alpha_j) \right]^2 (-1)^{\binom{n+1}{2}} \left[\prod_{i=2}^{n+1} \prod_{j \neq i} (\alpha_i - \alpha_j) \right]^2 \\
 &= (f_n(1))^2 d_n \\
 &= (n-1)^2 d_n.
 \end{aligned}$$

■

n	$ d_n $
2	5
3	$2^2.11$
4	563
5	$2^4.599$
6	205937
7	$2^6.84223$
8	1319.126913
9	$2^8.17.487.2851$
10	7.35616734267
11	$2^{10}.19.131.4550179$
12	10607.211723.267679
13	$2^{12}.6317.1328851967$
14	112589.219361.87132013
15	$2^{14}.241.2347.2879.5484307$
16	131.1103237.74329019184449
17	$2^{16}.83.2376011291.655308793$
18	12479.3119618081.1833387643403
19	$2^{18}.1439.4097227.4142481973103$
20	167.1840593902677.1981694167788721

Tabela 2.1: Fatoração de $|d_n|$.

2.3 O caso n par

Lema 47. *Seja $f(x) \in \mathbb{Z}[x]$. O grupo de Galois $\text{Gal}(f(x)/\mathbb{Q})$ é gerado pelos subgrupos de inércia de todos os primos que se ramificam em $L = \text{cf}(f(x))$.*

Demonstração: Seja I o subgrupo de $G = \text{Gal}(f(x)/\mathbb{Q})$ gerado pelos subgrupos de inércia dos primos que se ramificam em L . Pelo teorema 39 a extensão L^I não se ramifica. Como pelo teorema 18 toda extensão de $\mathbb{Q}$ se ramifica então $L^I = \mathbb{Q}$, ou seja, $I = G$. ■

Lema 48. ([5]). *Seja G um grupo de permutações do conjunto $\Omega = \{1, 2, \dots, n\}$ gerado por transposições. Se G é transitivo em Ω , então ele é todo o grupo de permutações S_n .*

Demonstração: Seja (ij) uma transposição contida em G e $k \in \{1, \dots, n\}$ qualquer. Como G é transitivo em S_n e gerado por transposições então existe $\sigma \in G$ tal que $\sigma = (ki_r)(i_r i_{r-1}) \cdots (i_2 i_1)(i_1 j)$. Podemos assumir, sem perda de generalidade, que os i'_m s, $1 \leq m \leq r$ são distintos.

-Se $i_m \neq i$ para $1 \leq m \leq r$ então $\sigma(ij)\sigma^{-1} = (ik)$.

-Se $i_m = i$ para algum m então G contém a permutação

$$\tau = (ki_r)(i_{r-1} i_{r-2}) \cdots (i_{m+2} i_{m+1})(i_{m+1} i).$$

Logo G contém $\tau(ij)\tau^{-1} = (jk)$ e portanto contém a permutação $(ij)(\tau(ij)\tau^{-1})(ij) = (ik)$. Em particular G contém o conjunto $\{(i1), (i2), \dots, (i, n-1)(in)\}$, que gera o S_n . ■

Teorema 49. *Seja $E_n = \text{cf}(f_n(x)/\mathbb{Q})$ o corpo de fatoração de f_n sobre $\mathbb{Q}$. Sejam p um primo de $\mathbb{Q}$ e P um primo de E_n acima de p . Se p não divide d_n então P não se ramifica, isto é, I_P é trivial. Se $p > 2$ e divide d_n então I_P é gerado por uma transposição ou I_P é trivial.*

Demonstração: Se p é um primo de $\mathbb{Q}$ que não divide d_n então $\bar{f}_n$ não tem raízes múltiplas em $\mathbb{F}_p$. Logo, podemos escrever $\bar{f}_n = \bar{f}_1 \cdots \bar{f}_m$ com $\bar{f}_i \in \mathbb{F}_p[x]$ mônicos e irredutíveis, $1 \leq i \leq m$. Podemos considerar $f_n(x) \in \mathbb{Z}_p[x]$, onde $\mathbb{Z}_p$ é o anel dos inteiros p -ádicos. Pelo lema de Hensel podemos levantar a fatoração de $\bar{f}_n$ à $\mathbb{Q}_p$. Assim existem polinômios $h_i(x) \in \mathbb{Q}_p[x]$, $1 \leq i \leq m$, tais que

- $\bar{h}_i = \bar{f}_i$;
- $\deg(\bar{f}_i) = \deg(h_i)$;
- h_i é mônico irredutível;

Mostremos que a extensão de $\mathbb{Q}_p$ gerada pelas raízes de h_i , $1 \leq i \leq m$, é não-ramificada.

Fixado h_i , $1 \leq i \leq m$, seja θ uma raiz de h_i . Como $\mathbb{Q}_p$ é um corpo local,

$$[\mathbb{Q}_p(\theta) : \mathbb{Q}_p] = ef$$

onde $e = e_{\mathbb{Q}_p(\theta)/\mathbb{Q}_p}$ é o índice de ramificação e $f = f_{\mathbb{Q}_p(\theta)/\mathbb{Q}_p}$ é o grau de inércia. Seja l o corpo residual de $\mathbb{Q}_p(\theta)$ e k o corpo residual de $\mathbb{Q}_p$ então $f = [l : k] = \deg(\bar{f}_i)$ pois $\bar{f}_i$ é irredutível e $\bar{f}_i(\bar{\theta}) = 0$. Portanto

$$f = [l : k] = \deg(\bar{f}_i) = \deg(h_i) = [\mathbb{Q}_p(\theta) : \mathbb{Q}_p] = ef.$$

Logo, $e = 1$.

Se θ' é outra raiz de h_i , usando o mesmo argumento temos que o índice de ramificação, e' , da extensão $\mathbb{Q}_p(\theta')/\mathbb{Q}_p$ é 1. Assim temos,

Logo $\mathbb{Q}_p(\theta, \theta')$ é um compositum de extensões não-ramificadas de $\mathbb{Q}_p$ e portanto é não ramificada (teorema 39). Prosseguindo com este argumento concluimos que a extensão N de $\mathbb{Q}_p$ gerada por todas as raízes de todos h_i 's, $1 \leq i \leq m$, é não-ramificada.

Assim, temos o diagrama:

Portanto o primo P não se ramifica.

Seja $p > 2$ um primo que divide o discriminante d_n . Suponha que p se ramifica em E_n .

Defina $h_n = (n+1)g_n(x) - xg'_n(x) = -2x^n + (n+1)$. Então as raízes de g e g' são raízes de h . Além disso, são raízes n -ésimas de $\frac{n+1}{2}$. O discriminante de $\bar{f}_n$ é zero em $\mathbb{F}_p$, portanto $\bar{f}_n$ tem uma raiz múltipla, digamos $\bar{\alpha}$. Mostremos que essa é a única raiz múltipla de $\bar{f}_n$. De fato, qualquer $\bar{\alpha}$ que é raiz múltipla de $\bar{f}_n$ satisfaz

$$\bar{\alpha}^n = \frac{\bar{n} + \bar{1}}{2}$$

e como $\bar{g}'_n(\bar{\alpha}) = \bar{0}$ temos

$$(\bar{n} + \bar{1})\bar{\alpha}^n - \bar{2}\bar{n}\bar{\alpha}^{n-1} = 0.$$

Como $\bar{\alpha} \neq \bar{0}$, pois $\bar{\alpha}$ é raiz de $\bar{g}_n$, temos

$$\bar{\alpha} = \frac{\bar{2}\bar{n}}{\bar{n} + \bar{1}}.$$

Desta última igualdade podemos tirar duas conclusões:

- $\bar{\alpha} \in \mathbb{F}_p$ é a única raiz múltipla de $\bar{g}_n$, e conseqüentemente de $\bar{f}_n$;
- $\bar{n} \neq 0$.

Para verificar que esta raiz é dupla usaremos o polinômio h . Note que

$\bar{h}'_n(x) = -2\bar{n}x^{n-1}$ só tem zero como raiz, logo $\bar{h}$ e $\bar{h}'$ não têm raízes em comum. Agora, se $\bar{g}_n$ possuisse uma raiz tripla então $\bar{h}_n$ teria uma raiz dupla. Logo $\bar{g}_n$ não tem raízes triplas. Logo $\bar{f}_n$ também não tem raízes triplas.

Portanto podemos fatorar $\bar{f}_n = \bar{f}_1\bar{f}_2 \cdots \bar{f}_m$ em $\mathbb{F}_p$, onde $\bar{f}_1(x) = (x - \bar{\alpha})^2$ e $\bar{f}_2 \cdots \bar{f}_m$ são mônicos irredutíveis. Se h_i , $1 \leq i \leq m$ é o levantamento de $\bar{f}_i$ em $\mathbb{Q}_p$, usando o argumento anterior, sabemos que a extensão de $\mathbb{Q}_p$ gerada pelas raízes de h_i , $i \geq 2$, é não-ramificada.

Seja $E_p = cf(f_n/\mathbb{Q}_p)$ o corpo de fatoração de f_n sobre $\mathbb{Q}_p$. Como p se ramifica em E_n então p se ramifica em E_p . Segue que $e_{E_p/\mathbb{Q}_p} \geq 2$. Observe que $e_{\mathbb{Q}_p(\alpha')/\mathbb{Q}_p} \geq 2$, onde α' é uma raiz de $h_1(x)$, pois se $e_{\mathbb{Q}_p(\alpha')/\mathbb{Q}_p} = 1$ então pelo teorema 39 temos $e_{E_p/\mathbb{Q}_p} = 1$. Pelo teorema 38,

$$2 = [\mathbb{Q}_p(\alpha') : \mathbb{Q}_p] = e_{\mathbb{Q}_p(\alpha')/\mathbb{Q}_p} \cdot f_{\mathbb{Q}_p(\alpha')/\mathbb{Q}_p}.$$

Portanto $e_{\mathbb{Q}_p(\alpha')/\mathbb{Q}_p} = 2$.

Pelo diagrama

temos $e_{E_p/\mathbb{Q}_p} = 2$.

Seja P um primo em E_n sobre p . Temos o diagrama

Sejam

- $D_P = \text{Gal}((E_n)_P/\mathbb{Q}_p)$ o grupo de decomposição de P ,
- I_P o subgrupo de inércia e T_P o subgrupo de inércia (que é o corpo fixo de I_P).

Como $N/\mathbb{Q}_p$ é uma extensão não-ramificada e pela teoria de corpos locais T_P é a extensão maximal não-ramificada, então $N \subset T_P$ e temos o seguinte diagrama

$$\begin{array}{c} (E_n)_P \\ | \\ T_P \\ | \\ N \\ | \\ \mathbb{Q}_p \end{array}$$

com $[(E_n)_P : T_P] = e_{(E_n)_P/\mathbb{Q}_p} = 2$. Então, pelo teorema 41, temos:

- $|I_P| = 2$
- I_P fixa as raízes de f_i , $i \geq 2$.

Sejam α', β raízes de $f_1(x)$. Como são raízes de um polinômio quadrático irreduzível, existe $\tau \in I_P \subset \text{Gal}((E_n)_P/\mathbb{Q}_p)$ tal que $\tau(\alpha') = \beta$ e τ fixa todas as outras raízes. Portanto τ é uma transposição. Portanto I_P é gerado por uma transposição. ■

Corolário 50. *Seja G_n o grupo de Galois de $f_n(x)$ sobre $\mathbb{Q}$. Então G_n contém uma transposição.*

Corolário 51. *Seja G_n o grupo de Galois de $f_n(x)$ sobre $\mathbb{Q}$. Se n é par então G_n é gerado por transposições.*

Demonstração: Se n é par então d_n é ímpar e $p = 2$ não se ramifica em E_n . Logo todos os primos que se ramificam tem seu subgrupo de inércia gerado por transposições. Pelo teorema 18 sempre existe um primo que se ramifica. Portanto o grupo de Galois é gerado por transposições.

Teorema 52. *Seja n um inteiro par. O grupo de Galois de f_n é o grupo de permutações de n símbolos S_n .*

Demonstração: Pelo lema 44, f_n é irreduzível e, portanto, $\text{Gal}(f_n)$ é transitivo e pelo corolário 51, $\text{Gal}(f_n)$ é gerado por transposições. Portanto pelo lema 48, $\text{Gal}(f_n) = S_n$. ■

2.4 O caso n primo

Seja p um número primo e $f_p(x) = x^p - x^{p-1} - \cdots x - 1$ a redução módulo p de $f_p(x)$. A seguir demonstraremos este polinômio é irreduzível sobre $\mathbb{F}_p$.

Lema 53. *Se p é um número primo então vale a seguinte fórmula em $\mathbb{F}_p[x]$:*

$$x^p \bar{f}_p\left(2 - \frac{1}{x}\right) = \bar{f}_p(x).$$

Demonstração: Uma igualdade bastante usada em álgebra é:

$$(x^n + x^{n-1} + \cdots + x + 1)(x - 1) = x^{n+1} - 1.$$

Em $\mathbb{F}_p$ vale $(x - 1)^p = x^p - 1$, então

$$\begin{aligned} \bar{f}_p(x) &= x^p - x^{p-1} - \cdots - x - 1 \\ &= x^p - \frac{x^p - 1}{x - 1} \\ &= x^p - \frac{(x - 1)^p}{x - 1} \\ &= x^p - (x - 1)^{p-1}. \end{aligned}$$

Logo,

$$\begin{aligned} x^p \bar{f}_p(2 - \frac{1}{x}) &= x^p((2 - \frac{1}{x})^p - (1 - \frac{1}{x})^{p-1}) \\ &= x^p(2 - \frac{1}{x^p}) - x(x - 1)^{p-1} \quad (x^p = x, \forall x \in \mathbb{Z}_p) \\ &= 2x^p - 1 - x(x - 1)^{p-1}. \end{aligned}$$

Como $g_p(x) = (x - 1)f_p(x) = x^{p+1} - 2x^p + 1$ então $2x^p - 1 = x^{p+1} - (x - 1)\bar{f}_p(x)$.

Portanto,

$$\begin{aligned} x^p \bar{f}_p(2 - \frac{1}{x}) &= x^{p+1} - (x - 1)\bar{f}_p(x) - x(x - 1)^{p-1} \\ &= x(x^p - (x - 1)^{p-1}) - (x - 1)\bar{f}_p(x) \\ &= \bar{f}_p(x). \end{aligned}$$

Lema 54. No anel quociente $R = \frac{\mathbb{Z}_p[x]}{(f_p(x))}$ temos $\xi^p = x$, onde

$$\xi = -x^{p-1} + x^{p-2} + \cdots + x + 3.$$

Além disso, x é invertível em R e $\xi = 2 - \frac{1}{x}$ (denotaremos a classe de equivalência somente por x).

Demonstração: Por definição, $g_p(x) = (x - 1)f_p(x)$. Como $x \neq 1$ então

$$x^{p+1} - 2x^p + 1 = 0. \tag{2.5}$$

Reescrevendo

$$x(x^p - 2x^{p-1}) = -1$$

Temos as seguintes igualdades:

$$\phi(\alpha_j^p) = (2 - \frac{1}{\alpha_j^p}) = (2 - \frac{1}{\alpha_j})^p = \alpha_j$$

$$\phi(\alpha_j^{p^2}) = (2 - \frac{1}{\alpha_j^{p^2}}) = ((2 - \frac{1}{\alpha_j})^p)^p = \alpha_j^p$$

$\vdots$

$$\phi(\alpha_j^{p^{n_j-1}}) = (2 - \frac{1}{\alpha_j^{p^{n_j-1}}}) = ((2 - \frac{1}{\alpha_j})^p)^{p^{n_j-2}} = \alpha_j^{p^{n_j-2}}$$

$$\phi(\alpha_j^{p^{n_j}}) = (2 - \frac{1}{\alpha_j^{p^{n_j}}}) = ((2 - \frac{1}{\alpha_j})^p)^{p^{n_j-1}} = \alpha_j^{p^{n_j-1}}$$

i) Segue que $\phi^k(\alpha_j^{p^i}) \neq \alpha_j^{p^i}$ para todo $k = 1, \dots, n_j - 1$ e $\phi^{n_j}(\alpha_j^{p^i}) = \alpha_j^{p^{i-n_j}} = \alpha_j^{p^i}$.

Portanto ϕ é um n_j -ciclo.

ii) Mostremos por indução que

$$\phi^k(\beta) = \frac{k - (k+1)\beta}{(k-1) - k\beta}.$$

Para $k = 1$:

$$\phi(\beta) = 2 - \frac{1}{\beta} = \frac{2\beta-1}{\beta} = \frac{1-(1+1)\beta}{(1-1)-1\beta}.$$

Supondo a fórmula válida para k :

$$\phi^{k+1}(\beta) = \phi^k(\phi(\beta)) = \phi^k(2 - \frac{1}{\beta}) = \frac{k-(k+1)(2-\frac{1}{\beta})}{(k-1)-k(2-\frac{1}{\beta})} = \frac{\beta k - (k+1)(2\beta-1)}{\beta(k+1) - k(2\beta-1)} = \frac{(k+1)-(k+2)\beta}{k-(k+1)\beta}.$$

Por i) e ii) temos $\phi^{n_j}(\alpha_j) = \alpha_j$, ou seja,

$$\frac{n_j - (n_j + 1)\alpha_j}{(n_j - 1) - n_j\alpha_j} = \alpha_j \Rightarrow n_j\alpha_j^2 - 2n_j\alpha_j + n_j = 0. \quad (2.8)$$

Como supomos $\bar{f}_p$ redutível então $0 < n_j < p$, isto é, $n_j \neq 0 \pmod{p}$. Dividindo a última igualdade por n_j obtemos:

$$\alpha_j^2 - 2\alpha_j + 1 = 0 \Rightarrow \alpha_j - 2 + \frac{1}{\alpha_j} = 0 \Rightarrow \alpha_j = 2 - \frac{1}{\alpha_j}.$$

Logo, por 2.7, $\alpha_j^p = (2 - \frac{1}{\alpha_j})^p = \alpha_j$.

Então α_j é raiz de $x^p - x$, ou seja, $\alpha_j \in \mathbb{F}_p$. O que não acontece, pois mostramos que $\bar{f}_p$ não tem raízes em $\mathbb{F}_p$. ■

Teorema 56. *Seja p um número primo. Então G , o grupo de Galois de $f_p(x)$, é o grupo simétrico S_p de p símbolos.*

Demonstração: Um subgrupo de S_p que contém uma transposição e um p -ciclo é o S_p , pois $S_p = \langle (12\dots n), (ij) \rangle, \forall i, j \in \{1, 2, \dots, p\}, i \neq j$. ([1], pág. 214). Pelo corolário 50, G contém uma transposição. Como

$$D_p = (-1)^{\binom{p+1}{2}}[(p+1)^{p+1} - 2^{p+1}p^p] \equiv (-1)^{\binom{p+1}{2}} \not\equiv 0 \pmod{p}$$

então p não divide D_p e, consequentemente não divide d_p . Logo p não se ramifica.

Pelo teorema 55 $\bar{f}_p$ é irredutível em $\mathbb{Z}_p$, então pelo lema de Hensel, f_p é irredutível em $\mathbb{Q}_p$ e isto implica que o grupo de Galois $Gal(f_p/\mathbb{Q}_p)$ é cíclico de ordem p . Logo G contém um p -ciclo e é, portanto, S_p . ■

Referências Bibliográficas

- [1] Garcia A. e Lequain Y.; Elementos de Álgebra. 4ed. Rio de Janeiro: IMPA,2006.
- [2] Gouvêa F.Q.; Primeiros Passos p-Ádicos, 17^o Colóquio Brasileiro de Matemática, IMPA.
- [3] Lang S.; Algebra. Third Edition, ADDISON-WESLEY PUBLISHING COMPANY.
- [4] Miller M.D.; On generalized Fabinacci Numbers, Amer. Math. monthly 78, (1971) 1108-1109.
- [5] Osada H.; The Galois Group of the Polynomials $x^n + ax^l + b$. Journal of Number Theory 25, 230-238(1987).
- [6] Samuel P.; Algebraic Theory of Numbers. HOUGHTON MIFFLIN COMPANY.
- [7] Scott E. B., Descartes'Rule of Signs. Texto tirado da página <http://cut-the-knot.org/fta/ROS2.shtml>.
- [8] Stewart I.N.; Galois theory. CHAPMAN & HALL/CRC MATHEMATICS.
- [9] Tengan E.; An invitation to Local Fields. Groups, Rings and Groups Rings 2008 UBATUBA/BRAZIL.
- [10] Zariski O. e Samuel P.; Commutative Algebra Vol II. Springer-Verlag.