Universidade Estadual de Campinas

Instituto de Matemática Estatística e Computação Científica

Departamento de Matemática

Extensões Cúbicas Cíclicas

por

Rosemberg Pereira Serrano[†]

Mestrado em Matemática - Campinas - SP

Orientador: Prof. Dr. Antonio Paques

[†]Este trabalho contou com apoio financeiro da CAPES.

Extensões Cúbicas Cíclicas

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Rosemberg Pereira Serrano** e aprovada pela comissão julgadora.

Campinas, 28 de fevereiro de 2003.

Prof. Dr. **Antonio Paques**.

Orientador

Banca examinadora:

Prof. Dr. Antonio Paques.

Prof. Dra. Ires Dias.

Prof. Dr. Plamen Emilov Koshlukov.

Dissertação apresentada ao Instituto de Matemática Estatística e Computação Científica, **IMECC**, como requisito parcial para obtenção do título de **MESTRE EM MATEMÁTICA**.

.

A minha família que soube compreender
e aceitar minha ausência durante a
elaboração deste trabalho.

Agradecimentos

Na realização desse trabalho muitas pessoas colaboraram de maneira direta ou indireta, e é com satisfação e alegria que revelo a minha gratidão, em especial:

• *À Deus, por tudo.*

• *Aos meus pais e irmãos por confiarem em mim, pelo abraço e sorriso amigo em cada vez que eu voltava, pelo incentivo aos estudos e, principalmente, porque que devo a eles tudo que sou. Enfim, obrigado por vocês existirem.*

• *Gostaria de agradecer carinhosamente a Patricia Silva de Paula minha futura esposa pelo incansável apoio, carinho e paciência.*

• *À Universidade Estadual de Campinas, UNICAMP, ao instituto de matemática, por ter permitido realizar meus estudos de Pós-Graduação.*

• *Aos meus amigos de república Alex, Andrés, Carla, Cleusiane, Élcio, Fabíola, Fernando, Gilmar, Ivanilde, Josiane, Lidermir, Miguel, Nilda, Rogério e Silvia, por ter proporcionado neste tempo longe de casa e da família uma acolhedora e divertida convivência.*

• *Aos meus colegas, em especial ao Alcindo, Dirceu, Evandro, Gilmar, Karine, Lucélia e Vanessa pela ajuda e companheirismo.*

• *Ao Fernando Santos pela ajuda no Latex.*

• *À Cidinha, Tânia e Ednaldo pela torcida e por me ajudarem a resolver os problemas burocráticos.*

• *Finalmente, meu especial agradecimento ao Professor Dr. Antonio Paques, pela oportunidade, paciência e confiança depositada. Seu rigor e disciplina, ensinou-me que a única forma de conhecer é descobrir, e que fazer descobrir é a única forma de ensinar.*

A satisfação está no esforço e não apenas na realização final.

M.K.Gandhi

(1869-1948)

Sumário

Resumo

Este trabalho é um estudo descritivo das extensões cúbicas cíclicas de um corpo K de característica arbitrária, isto é, das extensões galoisianas de K cujo grupo de Galois é cíclico de ordem três. Este estudo foi feito para três diferentes casos:

- para corpos de característica diferente de três, usando a teoria de Kummer,
- para corpos de característica qualquer, sem recorrer às teorias de Kummer e Artin-Schreier e
- para o corpo dos números racionais, usando a trigonometria.

Abstract

This work is a descriptive study of the cyclic cubic extensions of a K field of arbitrary characteristic, that is, of the Galois extensions of K whose Galois group is cyclic of order three. This study was made to three different cases:

- for any field with characteristic different from three, using Kummer theory,
- for any field with any characteristic, without appealing to the Kummer and Artin-Schreier theories, and
- for the rational numbers field, using trigonometry.

Lista de Símbolos

- K, F — Corpos
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — Conjuntos dos números inteiros, racionais, reais, complexos
- $F|K$ — Extensão de corpos
- $[F : K]$ — Grau de $F|K$
- $Gal(F|K)$ — Grupo de Galois da extensão $F|K$
- $\overline{K}$ — Fecho algébrico de K
- $< \sigma >$ — Grupo cíclico gerado por σ
- $F^{<\tau>}$ — Corpo fixo do grupo $< \tau >$
- $T_{F|K}$, $N_{F|K}$ — Aplicações traço de $F|K$, norma de $F|K$
- $K[X]$ — Anel de polinômios em uma variável X com coeficientes em K
- $K^{\star}$ — Grupo multiplicativo dos elementos não nulos de K
- (f) — Ideal principal gerado por f
- f — Elemento de $K[X]$
- $K(\alpha)$ — Corpo gerado por K e α
- $Ker(T_{F|K})$ — Núcleo da aplicação $T_{F|K}$
- $\bigoplus$ — Soma direta

- $\simeq$ Isomorfos
- S^1 Círculo unitário
- $\mathbb{Z}[\zeta]$ Monóide comutativo
- $|z|$ Módulo do número complexo z
- mod 3 Módulo 3
- $W(\mathbb{Q})$ Subgrupo do grupo multiplicativo das unidades de $\mathbb{Q}G$
- G Grupo cíclico de ordem 3
- $\mathbb{Q}G$ Álgebra de grupo racional
- $\mathcal{C}(\mathbb{Q})$ O conjunto $\{(t_1, t_2) \in \mathbb{Q} \times \mathbb{Q} \mid t_1 + t_2 = 3(t_1^2 + t_1 t_2 + t_2^2)\}$
- $S(\mathbb{Q})$ Intersecção de $\mathbb{Q}[\zeta]$ com S^1, i.é, o conjunto $\{\lambda \in \mathbb{Q}[\zeta] \mid N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(\lambda) = 1\}$
- $\times$ Produto cartesiano
- $\sim$ Equivalência
- $R^\star$ Conjunto dos elementos não nulo de um anel comutativo R
- arg(z) Argumento do número complexo z
- H_t Polinômio auxiliar
- $Alg_K(E, F)$ Homomorfismo de K-álgebras de E em F
- Δ Determinante de Vandermonde de ordem 3
- $\mathcal{C}_3(F)$ F-álgebra das matrizes circulantes 3×3, com entradas em F
- FG F-álgebra de grupo
- $(\alpha^{i+j})_{0 \leq i,j \leq 2}$ Matriz i, j com entradas em F
- T_B Aplicação F-linear definida pela matriz B
- Δ_j Determinante obtido de Δ substituindo a j-ésima linha
- $\varphi|_K$ Restrição de φ a K
- $\#(K)$ Cardinalidade de K

- K', F' — Corpo gerado por K e ζ, corpo gerado por F e ζ
- $[v]$ — Classe de equivalência de v
- V — Conjunto das classes de equivalência $[v]$ representadas pelos elementos $v \in \mathbb{Z}[\zeta]$

Introdução

Este trabalho, quase que essencialmente, gira em torno do polinômio

$$f_k = X^3 + kX^2 - (k+3)X + 1 \in K[X],$$

onde K é um corpo qualquer. Este polinômio tem como sua principal peculiaridade o fato de que seu discriminante é sempre um quadrado para qualquer escolha de k em K. De fato, o seu discriminante é igual a $(k^2+3k+9)^2$. Notem que se a característica de K é distinta de 3 (resp. igual a 3) então $k^2+3k+9=0$ se e somente se $\dfrac{k}{3}$ é uma raiz cúbica primitiva da unidade (resp. k=0). Por outro lado é muito simples verificar que f_k é redutível sobre K se e somente se $k = \dfrac{f_0(\lambda)}{\lambda - \lambda^2}$, para algum $\lambda \in K\backslash\{0,1\}$.

Desta forma vemos que $F_k = \dfrac{K[X]}{(f_k)}$ é um corpo extensão cúbica cíclica de K (isto é, F_k é uma extensão galoisiana de K, cujo grupo $Gal(F_k|K)$ dos K-automorfismos de F_k é cíclico de ordem 3), sempre que o k escolhido for diferente de $\dfrac{f_0(\lambda)}{\lambda - \lambda^2}$, para todo $\lambda \in K\backslash\{0,1\}$ e $\dfrac{k}{3}$ não for uma raiz cúbica primitiva da unidade (resp. $k \neq 0$) se a característica de K for distinta de 3 (resp. igual a 3). Esta é portanto uma forma simples e elementar de se construir exemplos de extensões cúbicas cíclicas de um corpo K qualquer. O interessante é que **toda extensão cúbica cíclica de um corpo K qualquer é do tipo $\mathbf{F_k}$, para algum $\mathbf{k \in K}$**. Esta foi a principal motivação para a realização deste trabalho.

O polinômio f_k aparece na literatura, acreditamos que pela primeira vez, nos trabalhos de D. Shanks [11] ("The simplest cubic fields", 1974) e de T. Cusick [2] ("Finding fundamental units in cubic fields", 1982) respectivamente sobre o número de classes e sobre unidades fundamentais em corpos cúbicos racionais.

Em 1994, P. Morton [8] realizou um estudo sobre extensões cúbicas cíclicas F de um corpo K de característica distinta de 2 em termos de polinômios que descrevem os automorfismos não triviais de F. Como resultado principal desse seu trabalho ele demonstrou que F é do tipo F_k. Neste seu trabalho o autor fez uso extensivo do programa computacional Mathematica para demonstrar alguns dos seus resultados.

Em 1996, R. Chapman [1] apresentou novas demonstrações, bem mais simples para os principais resultados de Morton, utilizando apenas à Teoria de Kummer.

Em 1987, I. Kersten e J. Michaliček [6] provaram, usando argumentos absolutamente elementares e sem fazer uso da Teoria de Kummer, que toda extensão cúbica cíclica de um corpo K de característica distinta de 3 é do tipo F_k.

Em 1989, A. Paques e A. Solecki [9] apresentaram um estudo das extensões cúbicas cíclicas racionais, sob um ponto de vista geométrico, enfatizando em especial os aspectos trigonométricos desses corpos. Para tanto eles fizeram o uso do fato que toda extensão cúbica cíclica de um corpo K possui uma base normal auto-dual.

O presente trabalho é resultado de um estudo detalhado dos artigos [1], [6] e [9] acima mencionados e está dividido em 6 seções, incluindo-se a introdução.

Na seção de preliminares, apresentamos alguns resultados relativos a existência de base normal e de base normal auto-dual, necessários para obtermos alguns dos resultados das seções 2 e 3.

Nas seções 1, 2 e 3 tratamos sobre os artigos [1], [6] e [9], respectivamente.

Na seção 4 discutimos condições necessárias e suficientes para decidir quando duas extensões cúbicas cíclicas são isomorfas; em particular, quando dois polinômios do tipo f_k determinam a mesma extensão F_k. Esta seção está baseada no trabalho de C. Dragos [3], o qual contém testes efetivos para decidir rapidamente quando dois polinômios normais determinam a mesma extensão, envolvendo unicamente fatoração de polinômios e cálculo de determinantes .

Preliminares

Bases Normais

Esta seção é dedicada aos resultados referentes à existência de base normal e base normal auto-dual para extensões cúbicas cíclicas, que será utilizada no próximo capítulo, principalmente nas seções 2 e 3. Evidentemente os resultados que listaremos aqui valem em geral para qualquer corpo extensão galoisiana finita de um corpo K mas, por uma questão de simplicidade das demonstrações que iremos apresentar e de concordância com o tema do trabalho todo, nos restringiremos apenas ao caso cúbico.

Nesta seção K é um corpo qualquer. Sejam F uma extensão cúbica cíclica de K e σ um gerador do grupo $Gal(F|K)$. Dizemos que F tem uma **base normal** sobre K se existe um elemento $z \in F$ tal que $\{z, \sigma(z), \sigma^2(z)\}$ é uma base para o K-espaço vetorial F. Também costumamos dizer, neste caso, que o elemento z **gera** uma base normal de F sobre K.

Denotamos por FG a F-álgebra do grupo G , isto é, FG como F-espaço vetorial tem base G e como álgebra tem multiplicação induzida pela multiplicação de G. A ação de G sobre F induz naturalmente uma ação de G sobre FG da seguinte forma $\sigma : \sum_{0 \leq i \leq 2} \lambda_i \sigma^i \mapsto \sum_{0 \leq i \leq 2} \sigma(\lambda_i)\sigma^i$.

Denotamos por $\mathcal{C}_3(F)$ a F-álgebra das matrizes circulantes 3×3, com entradas em F, isto é das matrizes do tipo $\begin{pmatrix} \lambda_0 & \lambda_1 & \lambda_2 \\ \lambda_2 & \lambda_0 & \lambda_1 \\ \lambda_1 & \lambda_2 & \lambda_0 \end{pmatrix}$, com $\lambda_i \in F,\ 0 \leq i \leq 2$. É imediato verificar que FG e $\mathcal{C}_3(F)$ são F-álgebras isomorfas via a aplicação $\varphi : FG \to \mathcal{C}_3(F)$ dada por

$\varphi(\sum_{0\leq i\leq 2}\lambda_i\sigma^{-i}) = \begin{pmatrix}\lambda_0 & \lambda_1 & \lambda_2\\ \lambda_2 & \lambda_0 & \lambda_1\\ \lambda_1 & \lambda_2 & \lambda_0\end{pmatrix}$.

Lema P.1. *Sejam F uma extensão cúbica cíclica de K, σ um gerador do grupo $G = Gal(F|K)$ e $z_i \in F$, $0 \leq i \leq 2$. As seguintes afirmações são eqüivalentes:*

(i) *$\{z_0, z_1, z_2\}$ é uma base de F sobre K e $z_i = \sigma^i(z_0)$, $0 \leq i \leq 2$.*

(ii) *A matriz $(\sigma^{i+j}(z_0))_{0\leq i,j\leq 2}$ é invertível em $\mathcal{C}_3(F)$.*

(iii) *O elemento $\upsilon = z_0 + z_1\sigma^2 + z_2\sigma \in FG$ é invertível e $\sigma(\upsilon) = \upsilon\sigma$.*

Demonstração.

(i)$\Rightarrow$ (ii) É sabido da Álgebra Linear que uma matriz quadrada, com entradas em um determinado corpo, é invertível se e somente se suas linhas (ou colunas) são linearmente independentes sobre esse corpo. Supor que as linhas da matriz $(\sigma^{i+j}(z_0))_{0\leq i,j\leq 2}$ são linearmente dependentes sobre F implicará na existência de elementos $\lambda_0, \lambda_1, \lambda_2 \in F$, não todos nulos tais que

$$\sum_{0\leq i\leq 2}\lambda_i\sigma^i(z_0) = 0, \qquad \sum_{0\leq i\leq 2}\lambda_i\sigma^i(z_1) = 0 \qquad \text{e} \qquad \sum_{0\leq i\leq 2}\lambda_i\sigma^i(z_2) = 0.$$

Conseqüentemente, desde que $\{z_0, z_1, z_2\}$ é uma base de F sobre K,

$$\sum_{0\leq i\leq 2}\lambda_i\sigma^i(x) = 0, \text{ para todo } x \in F, \text{ ou seja, } \sum_{0\leq i\leq 2}\lambda_i\sigma^i = 0,$$

o que contraria a independência linear dos automorfismos σ^i sobre F (Lema de Dedekind, [10], Lemma 55) . Portanto a matriz $(\sigma^{i+j}(z_0))_{0\leq i,j\leq 2}$ é invertível.

(ii)$\Rightarrow$ (iii) É imediato desde que FG e $\mathcal{C}_3(F)$ são F-álgebras isomorfas .

(iii)$\Rightarrow$ (i) Se $\upsilon = z_0 + z_1\sigma^2 + z_2\sigma \in FG$, de $\sigma(\upsilon) = \upsilon\sigma$ decorre que $z_i = \sigma^i(z_0)$, $0 \leq i \leq 2$. Resta mostrar que $\{z_0, z_1, z_2\}$ é uma base de F sobre K.

De υ invertível em FG segue que a matriz $B = (\sigma^{i+j}(z_0))_{0\leq i,j\leq 2}$ é invertível em $\mathcal{C}_3(F)$. Logo a aplicação F-linear $T_B : F^3 \to F^3$ definida por B é um isomorfismo. Então,

para todo $\lambda \in F$, existe $(\lambda_0, \lambda_1, \lambda_2) \in F^3$ tal que $(\lambda, \sigma(\lambda), \sigma^2(\lambda)) = T_B(\lambda_0, \lambda_1, \lambda_2)$. Disto decorre que

$$\lambda = \sum_{0 \leq i \leq 2} \lambda_i z_i \qquad \text{e} \qquad (T_B)^{-1}(\lambda, \sigma(\lambda), \sigma^2(\lambda)) = (\lambda_0, \lambda_1, \lambda_2).$$

Por outro lado $(T_B)^{-1} = T_{B^{-1}}$ e se $y_1, y_2, y_3 \in F$ formam a primeira coluna de B^{-1} pode ser visto facilmente que $B^{-1} = (\sigma^j(y_i))_{0 \leq i,j \leq 2}$. Logo obtemos

$$\lambda_i = \sum_{0 \leq j \leq 2} \sigma^j(\lambda y_i) \in F^{Gal(F|K)} = K, \quad \text{para todo} \quad 0 \leq i \leq 2 \ .$$

Isto mostra que $z_0,\ z_1,\ z_2$ geram F como K-espaço vetorial e portanto constituem uma base. □

Embora seja de costume que toda extensão galoisiana finita de um corpo qualquer possui base normal, enfatizaremos esse resultado no caso específico das extensões cúbicas cíclicas, com uma demonstração bastante elementar, fazendo uso do Teorema 2.4.

Teorema P.2. *Toda extensão cúbica cíclica de K possui base normal.*

Demonstração. Sejam F uma extensão cúbica cíclica de K e σ um gerador do grupo $Gal(F|K)$.

Devemos mostrar que existe $z \in F$ tal que $\{z_i = \sigma^i(z) \mid 0 \leq i \leq 2\}$ é base de F sobre K. Conforme o Lema P.1 é suficiente encontrar $z \in F$ tal que $(\sigma^{i+j}(z))_{0 \leq i,j \leq 2}$ é uma matriz invertível.

Observemos que $\det(\sigma^{i+j}(z))_{0 \leq i,j \leq 2} = 3N_{F|K}(z) - T_{F|K}(z^3)$, onde $N_{F|K} = \prod_{i=0}^{2} \sigma^i$ denota a norma de F sobre K. Desde que

$$T_{F|K}(z^3) - 3N_{F|K}(z) = T_{F|K}(z)[T_{F|K}(z^2) - T_{F|K}(z\sigma(z))]$$

e

$$T_{F|K}(z^2) = T_{F|K}(z)^2 - 2T_{F|K}(z\sigma(z))$$

obtemos

$$\det(\sigma^{i+j}(z))_{0\leq i,j\leq 2} = T_{F|K}(z)[3T_{F|K}(z\sigma(z)) - T_{F|K}(z)^2].$$

Por outro lado, pelo Teorema 2.4 existe $\alpha \in F$ tal que $F = K(\alpha) \simeq \frac{K[X]}{(f_k)}$, com $k = -T_{F|K}(\alpha) \neq 0$. Então

$$f_k = X^3 + kX^2 - (k+3)X + 1 = (X-\alpha)(X-\sigma(\alpha))(X-\sigma^2(\alpha)),$$

donde segue-se que $T_{F|K}(\alpha\sigma(\alpha)) = -(k+3)$ e portanto, pelo Lema 2.1 (ii) temos $T_{F|K}(\alpha)^2 - 3T_{F|K}(\alpha\sigma(\alpha)) = k^2 + 3k + 9 \neq 0$. Portanto basta tomar $z = \alpha$. □

Uma base normal $\{z_0, z_1, z_2\}$ de uma extensão cúbica cíclica $F|K$ é dita **auto-dual** se ela for sua própria dual em relação à forma traço $T_{F|K} : F \to K$, isto é, se $T_{F|K}(z_0) = 1$ e $T_{F|K}(z_i z_j) = 0$.

Teorema P.3. *Toda extensão cúbica cíclica de K possui uma base normal auto-dual.*

Demonstração. Sejam F uma extensão cúbica cíclica de K e σ um gerador do grupo $G = Gal(F|K)$.

Por Teorema P.2 existe $z \in F$ tal que $\{z_i = \sigma^i(z) \mid 0 \leq i \leq 2\}$ é uma base normal de F sobre K. Então, pelo Lema P.1 o elemento $\upsilon = z_0 + z_1\sigma^2 + z_2\sigma$ é invertível em FG e $\sigma(\upsilon) = \upsilon\sigma$.

Consideremos agora o elemento $\nu = \upsilon^{-1}l(\upsilon) = \nu_0 + \nu_1\sigma^2 + \nu_2\sigma$, onde $l : KG \to KG$ é o isomorfismo de K-álgebras dado por $l(\sigma^j) = \sigma^{-j}$. Note que l é uma involução , isto é, $l^{-1} = l$. Note também que ν é invertível em FG. Ainda,

$$\sigma(\upsilon^{-1}) = \sigma(\upsilon)^{-1} = (\upsilon\sigma)^{-1} = \upsilon^{-1}\sigma^{-1} = \upsilon^{-1}\sigma^2$$

e

$$\sigma(l(\upsilon)) = l(\sigma(\upsilon)) = l(\upsilon\sigma) = l(\upsilon)l(\sigma) = l(\upsilon)\sigma^2$$

e portanto $\sigma(\nu) = \nu\sigma$.

Isto mostra, conforme Lema P.1, que $\nu_i = \sigma^i(\nu_0)$ e que $\{\nu_0, \nu_1, \nu_2\}$ é uma base normal de F sobre K.

Finalmente de

$$\begin{aligned} T_{F|K}(\nu_0^2) + T_{F|K}(\nu_0\nu_1)\sigma^2 + T_{F|K}(\nu_0\nu_1)\sigma &= \nu l(\nu) \\ &= (\upsilon^{-1}l(\upsilon))l(\upsilon^{-1}l(\upsilon)) \\ &= (\upsilon^{-1}l(\upsilon))(l(\upsilon)^{-1}\upsilon) \\ &= 1 \end{aligned}$$

obtemos

$$T_{F|K}(\nu_0^2) = 1 \qquad \text{e} \qquad T_{F|K}(\nu_0\nu_1) = 0.$$

Então $T_{F|K}(\nu_0)^2 = T_{F|K}(\nu_0^2) + 2T_{F|K}(\nu_0\nu_1) = 1$ e portanto $T_{F|K}(\nu_0) = \pm 1$ (resp. 1) se a característica de K é distinta de 2 (resp. 2). Portanto $\{\nu_0, \nu_1, \nu_2\}$ ou $\{-\nu_0, -\nu_1, -\nu_2\}$ é a base normal auto-dual pretendida. □

Observação P.4. Conforme o Teorema 2.4 do Capítulo 1, em toda extensão cúbica cíclica F de K existe um elemento α tal que $F = K(\alpha)$, com $k = -T_{F|K}(\alpha) \neq 0$ e cujo polinômio mínimo sobre K é f_k. Na demonstração do Teorema P.2 vimos que esse mesmo elemento gera uma base normal de F sobre K. Aplicando agora a este elemento α o algorítmo desenvolvido no Teorema P.3 para construir uma base normal auto-dual a partir de uma base normal, obtemos a base normal auto-dual $\{z, \sigma(z), \sigma^2(z)\}$, com $z = \dfrac{1}{d}(3\alpha^2 + 2k\alpha - (k+3))$, com $d = k^2 + 3k + 9$, onde σ denota um gerador do grupo $Gal(F|K)$.

Proposição P.5. *Sejam F uma extensão cúbica cíclica de K e $\{z_0, z_1, z_2\}$ uma base normal auto-dual de F sobre K. Então existem elementos $t_1, t_2 \in K$ tais que*

$$\begin{aligned} t_1 + t_2 &= 3(t_1^2 + t_1t_2 + t_2^2), \\ z_0^2 &= (1 - t_1 - t_2)z_0 + t_1z_1 + t_2z_2, \\ z_0z_1 &= t_1z_0 + t_2z_1 - (t_1 + t_2)z_2. \end{aligned}$$

Demonstração. A multiplicação por z_0 determina uma operador K-linear de F, cuja matriz em relação à base $Z = \{z_0, z_1, z_2\}$ é dada por $\begin{pmatrix} r_0 & s_0 & s_1 \\ r_1 & s_1 & s_2 \\ r_2 & s_2 & s_0 \end{pmatrix}$ onde $z_0^2 = r_0 z_0 + r_1 z_1 + r_2 z_2$ e $z_0 z_1 = s_0 z_0 + s_1 z_1 + s_2 z_2$. Como a base Z é normal auto-dual obtemos

$$\begin{pmatrix} z_0 & z_1 & z_2 \\ z_2 & z_0 & z_1 \\ z_1 & z_2 & z_0 \end{pmatrix} \begin{pmatrix} r_0 & s_0 & s_1 \\ r_1 & s_1 & s_2 \\ r_2 & s_2 & s_0 \end{pmatrix} \begin{pmatrix} z_0 & z_2 & z_1 \\ z_1 & z_0 & z_2 \\ z_2 & z_1 & z_0 \end{pmatrix} = \begin{pmatrix} z_0 & 0 & 0 \\ 0 & z_2 & 0 \\ 0 & 0 & z_1 \end{pmatrix}$$

e conseqüentemente

$$\begin{pmatrix} r_0 & s_0 & s_1 \\ r_1 & s_1 & s_2 \\ r_2 & s_2 & s_0 \end{pmatrix} = \begin{pmatrix} z_0 & z_2 & z_1 \\ z_1 & z_0 & z_2 \\ z_2 & z_1 & z_0 \end{pmatrix} \begin{pmatrix} z_0 & 0 & 0 \\ 0 & z_2 & 0 \\ 0 & 0 & z_1 \end{pmatrix} \begin{pmatrix} z_0 & z_1 & z_2 \\ z_2 & z_0 & z_1 \\ z_1 & z_2 & z_0 \end{pmatrix}$$

ou

$$\begin{pmatrix} r_0 & s_0 & s_1 \\ r_1 & s_1 & s_2 \\ r_2 & s_2 & s_0 \end{pmatrix} = \begin{pmatrix} T_{F|K}(z_0^3) & T_{F|K}(z_0^2 z_1) & T_{F|K}(z_0 z_1^2) \\ T_{F|K}(z_0^2 z_1) & T_{F|K}(z_0 z_1^2) & 3N_{F|K}(z_0) \\ T_{F|K}(z_0 z_1^2) & 3N_{F|K}(z_0) & T_{F|K}(z_0^2 z_1) \end{pmatrix}$$

Sejam $t_1 = T_{F|K}(z_0^2 z_1)$ e $t_2 = T_{F|K}(z_0 z_1^2)$. De $T_{F|K}(z_0) T_{F|K}(z_0 z_1) = 0$ obtemos $3N_{F|K}(z_0) = -t_1 - t_2$.

De $T_{F|K}(z_0)^3 = 1$ obtemos $T_{F|K}(z_0^3) = 1 - 3(t_1 + t_2) - 6N_{F|K}(z_0) = 1 - t_1 - t_2$. Assim,

$$z_0^2 = (1 - t_1 - t_2) z_0 + t_1 z_1 + t_2 z_2 \qquad \text{e} \qquad z_0 z_1 = t_1 z_0 + t_2 z_1 - (t_1 + t_2) z_2$$

Finalmente de $(z_0 z_1) z_2 = z_0 (z_1 z_2)$ obtemos $t_1 + t_2 = 3(t_1^2 + t_1 t_2 + t_2^2)$. □

Capítulo 1

Extensões Cúbicas Cíclicas

1 Descrição de extensões cúbicas cíclicas - via o uso de raiz da unidade

Nesta seção K denota um corpo de característica distinta de 3 que não possui raiz cúbica primitiva da unidade.

Começamos por observar que toda extensão cúbica cíclica de K pode ser imersa em uma extensão cíclica de grau 6 de K. Para tanto consideremos o corpo $K' = K(\zeta)$, onde ζ denota uma raiz cúbica primitiva da unidade em algum fecho algébrico $\overline{K}$ de K. Como é sabido $K'|K$ é uma extensão quadrática , cujo gerador τ do grupo $Gal(K'|K)$ é dado por $\tau : \zeta \mapsto \zeta^2$. Agora, sejam $F|K$ uma extensão cúbica cíclica e $F' = F(\zeta)$. É imediato ver que $F'|K$ é uma extensão de grau 6 que contém K' e corpo de raízes de um polinômio separável sobre K, ou seja, $F'|K$ é uma extensão galoisiana . Como $F|K$ é extensão cúbica cíclica, o subgrupo de $Gal(F'|K)$ gerado pelo F-automorfismo τ' de F' induzido por τ é necessariamente normal e, por conseqüência, $Gal(F'|K)$ é cíclico. Além disso $F'|K'$ é uma extensão cúbica cíclica e $(F')^{<\tau'>} = F$ é a única extensão cúbica cíclica de K contida em F'.

Notem que para o nosso propósito poderíamos ter considerado uma extensão quadrática qualquer de K. A escolha de K' é conveniente pois nos permitirá o uso da Teoria

de Kummer ([7], Ch.2, §7) para obtermos uma boa descrição da extensão cúbica cíclica $F'|K'$, assim como da extensão cíclica $F'|K$ e, por conseqüência, da extensão $F|K$, conforme veremos nos resultados a seguir.

No que segue denotaremos por $T_{K'|K}(\lambda) = \lambda + \overline{\lambda}$ e $N_{K'|K}(\lambda) = \lambda\overline{\lambda}$ as correspondentes aplicações traço e norma de K' sobre K, onde $\overline{\lambda} = \tau(\lambda)$, para todo $\lambda \in K'$. O grupo multiplicativo dos elementos não nulos de um corpo L qualquer, tanto nesta como nas demais seções, será sempre denotado por $L^\star$.

Proposição 1.1. *Seja $F' \supset K'$ uma extensão de grau 6 de K. Então $F'|K$ é uma extensão cíclica se e somente se $F' = K'(\beta)$ com $\beta^3 = \delta^2\overline{\delta}$, onde $\delta \in K'^\star$ e $\delta^2\overline{\delta}$ não é um cubo em K'.*

Demonstração. Suponha que $F'|K$ é uma extensão cíclica de grau 6 e sejam σ e τ os geradores de $Gal(F'|K)$ de ordem 3 e 2 respectivamente. Note que τ restrito a K' é o gerador de $Gal(K'|K)$ conforme descrito acima. Pela teoria de Kummer aplicada ao corpo K', temos que $F' = K'(\beta)$ onde $\beta^3 = \alpha \in K'^\star$, $\alpha \notin (K'^\star)^3$ e $\sigma(\beta) = \zeta\beta$. Desde que σ e τ comutam entre si obtemos

$$\sigma\tau(\beta) = \tau\sigma(\beta) = \tau(\zeta\beta) = \tau(\zeta)\tau(\beta) = \overline{\zeta}\tau(\beta).$$

Se $r = \beta\tau(\beta)$ então

$$\tau(r) = \tau(\beta(\tau(\beta))) = \tau(\beta)\tau^2(\beta) = \tau(\beta)\beta = r$$

e

$$\sigma(r) = \sigma(\beta\tau(\beta)) = \sigma(\beta)\sigma(\tau(\beta)) = \zeta\beta\overline{\zeta}\tau(\beta) = \beta\tau(\beta) = r.$$

Portanto $r \in K$. E,

$$r^3 = (\beta\tau(\beta))^3 = \beta^3\tau(\beta)^3 = \beta^3\tau(\beta^3) = \alpha\tau(\alpha) = N_{K'|K}(\alpha).$$

Se colocarmos $\delta = \dfrac{\alpha}{r}$ então

$$N_{K'|K}(\delta) = \frac{N_{K'|K}(\alpha)}{N_{K'|K}(r)} = \frac{r^3}{r^2} = r$$

e

$$\delta^2\overline{\delta} = \frac{\alpha^2\overline{\alpha}}{r^2 r} = \frac{\alpha N_{K'|K}(\alpha)}{r^3} = \frac{\alpha r^3}{r^3} = \alpha = \beta^3$$

e assim F' está na forma exigida.

Reciprocamente, suponha que $\delta \in K'^{\star}$ e $\delta^2\overline{\delta} \notin (K'^{\star})^3$. Então $F' = K'(\beta)$ onde $\beta^3 = \delta^2\overline{\delta}$ é uma extensão cúbica de K' cujo grupo de Galois é gerado por σ com $\sigma(\beta) = \zeta\beta$. Se $\beta' = \dfrac{N_{K'|K}(\delta)}{\beta}$ então

$$\beta'^3 = \left(\frac{N_{K'|K}(\delta)}{\beta}\right)^3 = \frac{N_{K'|K}(\delta)^3}{\beta^3} = \frac{(\delta\overline{\delta})^3}{\delta^2\overline{\delta}} = \frac{\delta^3\overline{\delta}^3}{\delta^2\overline{\delta}} = \delta\overline{\delta^2} = \tau(\delta^2\overline{\delta}).$$

Isto nos permite estender o K-automorfismo τ de K' a um K-automorfismo de F' via $\tau(\beta) = \beta'$. Como

$$\tau(\beta') = \tau\left(\frac{N_{K'|K}(\delta)}{\beta}\right) = \tau\left(\frac{\delta\overline{\delta}}{\beta}\right) = \frac{\tau(\delta\overline{\delta})}{\tau(\beta)} = \frac{\overline{\delta}\delta}{\beta'} = \beta$$

então τ tem ordem 2. Igualmente,

$$\tau\sigma(\beta) = \tau(\zeta\beta) = \tau(\zeta)\tau(\beta) = \overline{\zeta}\beta' = \frac{\overline{\zeta}N_{K'|K}(\delta)}{\beta} = \sigma(\frac{N_{K'|K}(\delta)}{\beta}) = \sigma\tau(\beta),$$

e daí vemos que σ e τ comutam. Como σ tem ordem 3, então a extensão $F'|K$ é cíclica de grau 6. E assim completamos a demonstração. □

Agora para cada $\delta \in K'^{\star}$ seja $F'_\delta = K'(\beta)$ com $\beta^3 = \delta^2\overline{\delta}$. Se $\delta^2\overline{\delta} \notin (K'^{\star})^3$ então $F'_\delta|K$ contém uma subextensão cúbica cíclica $F_\delta|K$. De fato, pela Proposição 1.1, $F'_\delta|K$ é uma extensão cíclica de grau 6 e, pelos comentários anteriores, $F'_\delta|K$ contém uma única extensão cúbica cíclica de K. A seguinte proposição identifica as extensões cúbicas cíclicas de K.

Proposição 1.2. *Se* $\delta^2\overline{\delta} \notin (K'^{\star})^3$ *então* $F_\delta = K(\theta)$, *onde* $\theta \in F_\delta$ *tem polinômio mínimo* $f_\delta = X^3 - 3N_{K'|K}(\delta)X - N_{K'|K}(\delta)T_{K'|K}(\delta)$ *sobre* K.

Demonstração. Primeiramente note que $F_\delta = (F'_\delta)^{\langle\tau\rangle}$, onde $\tau \in Gal(F'_\delta|K)$ é o único elemento de ordem 2. Consideremos agora $\theta = \beta + \tau(\beta) \in F'_\delta$. Claramente $\theta \in F_\delta$ e, por conseguinte, $F_\delta \supseteq K(\theta)$. Por outro lado, é fácil ver que $X^2 - \theta X + N_{K'|K}(\delta)$ é o polinômio mínimo de β sobre $K(\theta)$. Logo, $[F'_\delta : K(\theta)] = 2 = [F'_\delta : F_\delta]$ e conseqüentemente $K(\theta) = F_\delta$. Disto decorre que o polinômio mínimo de θ sobre K tem grau $[F_\delta : K] = 3$. Por outro lado,

$$\begin{aligned}
\theta^3 &= (\beta + \tau(\beta))^3 \\
&= \beta^3 + \tau(\beta)^3 + 3\beta\tau(\beta)(\beta + \tau(\beta)) \\
&= \delta^2\overline{\delta} + \tau(\delta^2\overline{\delta}) + 3N_{K'|K}(\delta)\theta \\
&= \delta^2\overline{\delta} + \overline{\delta^2}\delta + 3N_{K'|K}(\delta)\theta \\
&= N_{K'|K}(\delta)T_{K'|K}(\delta) + 3N_{K'|K}(\delta)\theta.
\end{aligned}$$

e portanto

$$\theta^3 - 3N_{K'|K}(\delta)\theta - N_{K'|K}(\delta)T_{K'|K}(\delta) = 0,$$

de onde segue-se que $X^3 - 3N_{K'|K}(\delta)X - N_{K'|K}(\delta)T_{K'|K}(\delta) \in K[X]$ é o polinômio mínimo de θ sobre K. Isto conclui a demonstração. □

A proposição seguinte nos dá uma descrição das raízes do polinômio

$$f_\delta = X^3 - 3N_{K'|K}(\delta)X - N_{K'|K}(\delta)T_{K'|K}(\delta)$$

ou, em outras palavras, descreve a ação do gerador σ do grupo $Gal(F'_\delta|K')$ sobre o subcorpo $K(\theta)$. Note que a restrição do K-automorfismo σ ao subcorpo $F_\delta = K(\theta)$ é o gerador do grupo $Gal(F_\delta|K)$, o qual também denotaremos por σ.

Proposição 1.3. *Se $\delta = a + b\overline{\zeta} \in K'$ com $\delta^2\overline{\delta} \notin (K'^\star)^3$ e $\sigma \in Gal(F'_\delta|K')$ é tal que $\sigma : \beta \mapsto \zeta\beta$ então $b \in K^\star$ e*

$$\sigma(\theta) = \frac{1}{b}[\theta^2 - a\theta - 2N_{K'|K}(\delta)] \tag{1.1}$$

$$\sigma^2(\theta) = \frac{1}{b}[-\theta^2 + (a-b)\theta + 2N_{K'|K}(\delta)]. \tag{1.2}$$

Demonstração. Desde que $\delta^2\overline{\delta} \notin (K'^{\star})^3$ necessariamente $b \neq 0$. Agora, dado $\theta = \beta + \tau(\beta) \in F_\delta$ temos

$$\begin{aligned}\theta^2 &= (\beta + \tau(\beta))^2 \\ &= \beta^2 + \tau(\beta)^2 + 2\beta\tau(\beta) \\ &= \beta^2 + \tau(\beta^2) + 2N_{K'|K}(\delta).\end{aligned}$$

De $\beta^3 = \delta^2\overline{\delta}$ obtemos

$$\theta^2 = \frac{\delta^2\overline{\delta}}{\beta} + \tau(\frac{\delta^2\overline{\delta}}{\beta}) + 2N_{K'|K}(\delta).$$

Por outro lado, $\tau(\delta^2\overline{\delta}) = \overline{\delta}^2\delta$, $\delta\overline{\delta} = N_{K'|K}(\delta)$ e $\tau(\beta) = \dfrac{N_{K'|K}(\delta)}{\beta}$. Logo,

$$\theta^2 = \frac{\delta N_{K'|K}(\delta)}{\beta} + \frac{\overline{\delta}N_{K'|K}(\delta)}{\tau(\beta)} + 2N_{K'|K}(\delta) = \delta\tau(\beta) + \overline{\delta}\beta + 2N_{K'|K}(\delta).$$

Como $\delta = a + b\overline{\zeta}$, temos

$$\begin{aligned}\theta^2 &= (a + b\overline{\zeta})\tau(\beta) + (a + b\zeta)\beta + 2N_{K'|K}(\delta) \\ &= a\tau(\beta) + b\overline{\zeta}\tau(\beta) + a\beta + b\zeta\beta + 2N_{K'|K}(\delta) \\ &= a(\tau(\beta) + \beta) + b(\overline{\zeta}\tau(\beta) + \zeta\beta) + 2N_{K'|K}(\delta) \\ &= a\theta + b\sigma(\theta) + 2N_{K'|K}(\delta).\end{aligned}$$

Portanto,

$$\sigma(\theta) = \frac{1}{b}[\theta^2 - a\theta - 2N_{K'|K}(\delta)].$$

Finalmente, como o coeficiente do termo em X^2 do polinômio mínimo de θ sobre K é nulo, então $\sigma^2(\theta) + \sigma(\theta) + \theta = 0$ e

$$\begin{aligned}\sigma^2(\theta) &= -\theta - \sigma(\theta) \\ &= -\theta - \frac{1}{b}[\theta^2 - a\theta - 2N_{K'|K}(\delta)] \\ &= \frac{1}{b}[-\theta^2 + (a - b)\theta + 2N_{K'|K}(\delta)],\end{aligned}$$

o que conclui a demonstração. □

Do que vimos acima, as extensões cúbicas cíclicas de K são todas do tipo

$$F_\delta = \frac{K[X]}{(f_\delta)}, \text{ com } \delta \in K'^{\star} \text{ tal que } \delta^2\overline{\delta} \notin (K'^{\star})^3.$$

Contudo esta é uma descrição que para ser executável requer determinar os elementos $\delta \in K'^{\star}$ que satisfaz a condição $\delta^2\overline{\delta} \notin (K'^{\star})^3$, a qual é eqüivalente à irredutibilidade do polinômio f_δ sobre K.

Na seqüência buscaremos encontrar elementos $\delta \in K'^{\star}$ "convenientemente mais simples" e que descrevam a mesma extensão F_δ. O objetivo aqui é demonstrar, como uma conseqüência imediata dos resultados até agora obtidos, que a extensão F_δ é do tipo $F_k = \dfrac{K[X]}{(f_k)}$, com $f_k = X^3 + kX^2 - (k+3)X + 1$ para algum $k \in K$. Aparentemente esta é uma forma mais simples de descrever as extensões cúbicas cíclicas de K. Para tanto necessitamos antes de um critério que nos permita decidir quando dois elementos de $K'^{\star}$, do tipo acima descrito, determinam a mesma extensão cúbica cíclica de K. Novamente a Teoria de Kummer nos dá a resposta desejada, conforme veremos na proposição seguinte.

Proposição 1.4.

(i) *Se $\delta \in K'^{\star}$ então $\delta^2\overline{\delta}$ é um cubo em K' se e somente se $\delta \in K^{\star}(K'^{\star})^3$.*

(ii) *Dados $\delta, \delta' \in K'^{\star}\backslash K^{\star}(K'^{\star})^3$, $F_\delta = F_{\delta'}$ se e somente se $\dfrac{\delta}{\delta'} \in K^{\star}(K'^{\star})^3$ ou $\dfrac{\delta}{\overline{\delta'}} \in K^{\star}(K'^{\star})^3$.*

Demonstração.

(i) Se $\delta^2\overline{\delta} \in (K'^{\star})^3$ então $\delta^2\overline{\delta} = \eta^3$ para algum $\eta \in K'^{\star}$ e, conseqüentemente, $\delta = N_{K'|K}(\delta)^{-1}\eta^3 \in K^{\star}(K'^{\star})^3$. Reciprocamente, se $\delta = r\eta^3$, com $r \in K^{\star}$ e $\eta \in K'^{\star}$ então $\delta^2\overline{\delta} = (r\eta^3)^2\overline{(r\eta^3)} = r^3\eta^6\overline{\eta}^3 = (r\eta^2\overline{\eta})^3 \in (K'^{\star})^3$.

(ii) Claramente $F_\delta = F_{\delta'}$ se e somente se $F'_\delta = F'_{\delta'}$ ou, pela teoria de Kummer, se e somente se $\dfrac{\delta^2\overline{\delta}}{(\delta'^2\overline{\delta'})^{\pm 1}} \in (K'^{\star})^3$. Mas por (i) $\dfrac{\delta^2\overline{\delta}}{(\delta'^2\overline{\delta'})} = \left(\dfrac{\delta}{\delta'}\right)^2\overline{\left(\dfrac{\delta}{\delta'}\right)} \in (K'^{\star})^3$ se e somente se $\dfrac{\delta}{\delta'} \in K^{\star}(K'^{\star})^3$. Similarmente, $(\delta^2\overline{\delta})(\delta'^2\overline{\delta'}) = (\delta\delta')^2\overline{(\delta\delta')} \in (K'^{\star})^3$ se e somente se $\delta\delta' \in K^{\star}(K'^{\star})^3$ se e somente se $\dfrac{\delta}{\overline{\delta'}} = N_{K'|K}(\delta')^{-1}\delta\delta' \in K^{\star}(K'^{\star})^3$. □

A Proposição 1.4 nos permite agora obter o teorema seguinte, o qual é o principal resultado desta seção.

Teorema 1.5. *Toda extensão cúbica cíclica de K é do tipo $F_k = K[X]/(f_k)$, onde $f_k = X^3+kX^2-(k+3)X+1$, com $k \in K$ tal que $k \neq \dfrac{\lambda^3-3\lambda+1}{\lambda-\lambda^2}$, para todo $\lambda \in K,\ \lambda \neq 0,1$. Além disso, o discriminante de f_k é $(k^2+3k+9)^2$ e o gerador σ do grupo $Gal(F_k|K)$ é dado por $\sigma(x) = x^2 + kx - (k+2)$ ou $\sigma(x) = -x^2 - (k+1)x + 2$, onde $x = X + (f_k)$.*

Demonstração. Seja $F|K$ uma extensão cúbica cíclica. Então, conforme as Proposições 1.1 e 1.2, $F = F_\delta = K(\theta)$, com $\delta = a + b\overline{\zeta} \in K'^\star$ satisfazendo $\delta^2\overline{\delta} \notin (K'^\star)^3$ e com θ tendo $f_\delta = X^3 - 3N_{K'|K}(\delta)X - N_{K'|K}(\delta)T_{K'|K}(\delta)$ como polinômio mínimo sobre K. Claramente $b \neq 0$ e, por Proposição 1.4, $F_\delta = F_{b^{-1}\delta}$. Logo podemos supor que $\delta = -\dfrac{k}{3}+\overline{\zeta}$, com $k = -\dfrac{3a}{b}$. Desta forma temos

$$T_{K'|K}(\delta) = -\frac{1}{3}(2k+3), \qquad N_{K'|K}(\delta) = \frac{1}{9}(k^2+3k+9)$$

e

$$f_\delta = X^3 - \frac{1}{3}(k^2+3k+9)X + \frac{1}{27}(2k^3+9k^2+27k+27).$$

Agora, substituindo θ por $\theta_1 = \theta - \dfrac{k}{3}$ obtemos

$$F_\delta = K(\theta_1) \quad \text{e} \quad f_k = X^3 + kX^2 - (k+3)X + 1$$

como polinômio mínimo de θ_1 sobre K. A irredutibilidade de f_k sobre K implica necessariamente $k \neq \dfrac{\lambda^3-3\lambda+1}{\lambda-\lambda^2}$ para todo $\lambda \in K,\ \lambda \neq 0,1$. Finalmente decorre da Proposição 1.3 que $\sigma(\theta) = \theta^2 + \dfrac{k}{3}\theta - \dfrac{2}{9}(k^2+3k+9)$ e por conseguinte $\sigma(\theta_1) = \theta_1^2 + k\theta_1 - (k+2)$. Da mesma forma obtemos $\sigma^2(\theta_1) = -\theta_1^2 - (k+1)\theta_1 + 2$, o que conclui a demonstração. □

2 Descrição de extensões cúbicas cíclicas - sem o uso de raiz da unidade

O propósito desta seção é dar uma descrição bem mais elementar, para toda extensão cúbica cíclica de K idêntica àquela estabelecida no Teorema 1.5, porém, sem recorrer ao uso de raiz cúbica primitiva da unidade e nem à Teoria de Kummer .

Nesta seção assumiremos que K é um corpo qualquer sem nenhuma restrição adicional. Começaremos com o lema abaixo, cuja demonstração pode ser verificada facilmente por cálculo direto. Como é usual também nesta seção $\overline{K}$ denotará um fecho algébrico de K.

Lema 2.1. *Sejam* $k \in K$, $f_k = X^3 + kX^2 - (k+3)X + 1 \in K[X]$ *e* $\alpha \in \overline{K}$ *uma raiz de* f_k. *Então* $\alpha \neq 0, 1$ *e se* $\alpha_0 = \alpha$, $\alpha_1 = \dfrac{1}{1-\alpha}$ *e* $\alpha_2 = \dfrac{\alpha - 1}{\alpha}$ *temos:*

(i) $f_k = (X - \alpha_0)(X - \alpha_1)(X - \alpha_2)$ *em* $\overline{K}[X]$,

(ii) $(\alpha_0 - \alpha_1)(\alpha_0 - \alpha_2)(\alpha_1 - \alpha_2) = -(k^2 + 3k + 9)$,

(iii) *se a característica de* K *é distinta de* 3 *(resp. igual a* 3*)* $\alpha_i - \alpha_j = 0$, *para algum* $i \neq j$, *se e somente se* $\dfrac{k}{3}$ *é uma raiz cúbica primitiva da unidade (resp.* $k = 0$*) se e somente se* $f_k = (X + \dfrac{k}{3})^3$ *(resp.* $(X+1)^3$*)* ,

(iv) f_k *é redutível sobre* K *se e somente se* $k = \dfrac{\lambda^3 - 3\lambda + 1}{\lambda - \lambda^2}$, *para algum* $\lambda \in K \backslash \{0, 1\}$. □

O seguinte corolário é uma conseqüência imediata dos itens (i), (ii) e (iii) do Lema 2.1.

Corolário 2.2. *Assuma que* f_k *é irredutível em* $K[X]$ *e seja* $\alpha \in \overline{K}$ *uma raiz de* f_k. *Então* $K(\alpha)$ *é uma extensão cúbica cíclica de* K *e o gerador* σ *do grupo* $Gal(K(\alpha)|K)$ *é dado por* $\sigma(\alpha) = \dfrac{1}{1-\alpha}$ *ou* $\sigma(\alpha) = \dfrac{\alpha - 1}{\alpha}$. □

Reciprocamente temos o seguinte teorema.

Teorema 2.3. *Toda extensão cúbica cíclica de K é do tipo $F_k = \frac{K[X]}{(f_k)}$, para algum $k \in K$ tal que $k \neq \frac{\lambda^3 - 3\lambda + 1}{\lambda - \lambda^2}$, para todo $\lambda \in K\backslash\{0,1\}$. Além disso, o discriminante de f_k é $(k^2+3k+9)^2$ e o gerador σ do grupo $Gal(F_k|K)$ é dado por $\sigma(x) = x^2 + kx - (k+2)$ ou $\sigma(x) = -x^2 - (k+1)x + 2$, onde $x = X + (f_k)$.*

Demonstração. Seja F uma extensão cúbica cíclica de K e considere a forma traço $T_{F|K} : F \to K$ dada por $T_{F|K} : z \mapsto z + \sigma(z) + \sigma^2(z)$, para todo $z \in F$. Da separabilidade de F sobre K decorre que $T_{F|K}$ é sobrejetivo e portanto $F = K \bigoplus Ker(T_{F|K})$. Logo $\dim_K Ker(T_{F|K}) = 2$. Seja $\{u, v\} \subset Ker(T_{F|K})$ uma base de $Ker(T_{F|K})$ sobre K.

Para cada $0 \neq y \in Ker(T_{F|K})$ considere $\alpha_y = 1 + \frac{\sigma(y)}{y} = -\frac{\sigma^2(y)}{y}$. É fácil ver que $\alpha_y \in K$ se e somente se $\alpha_y^2 - \alpha_y + 1 = 0$ e conseqüentemente $\alpha_y^3 + 1 = 0$. Então, se a característica de K for 3 (resp. distinta de 3), $\alpha_y \in K$ se e somente se $\alpha_y = -1$ (resp. $-\alpha_y$ é uma raíz cúbica primitiva da unidade). Além disso, para quaisquer dois elementos não nulos $y, z \in Ker(T_{F|K})$, $\alpha_y = \alpha_z$ se e somente se $z = \lambda y$, para algum $\lambda \in K$. Agora é fácil ver que pelo menos um dos elementos $\alpha_u, \alpha_v, \alpha_{u+v}$ não pertence a K, qualquer que seja a característica de K.

Disto concluímos então que sempre existe $y \in Ker(T_{F|K})$, $y \neq 0$, tal que $\alpha = \alpha_y \notin K$.

Seja $k = -T_{F|K}(\alpha)$. Agora é imediato verificar, por cálculo direto, que

$$(X - \alpha)(X - \sigma(\alpha))(X - \sigma^2(\alpha)) = f_k,$$

$\sigma(\alpha) = \frac{1}{1-\alpha} = -\alpha^2 - (k+1)\alpha + 2$ e $\sigma^2(\alpha) = \frac{\alpha - 1}{\alpha} = \alpha^2 + k\alpha - (k+2)$. O discriminante de f_k igual a $(k^2+3k+9)^2$ é uma conseqüência do Lema 2.1 (ii). Desde que $\alpha \notin K$, f_k é o polinômio mínimo de α sobre K e $F = K(\alpha)$, o que conclui a demonstração. □

É importante observar que o elemento $k = -T_{F|K}(\alpha)$ construído na demonstração do teorema acima não é necessariamente não nulo. Este é o caso, por exemplo, em $F = \frac{\mathbb{Q}[X]}{(X^3 - 3X + 1)}$, com $\alpha = X + (X^3 - 3X + 1)$.

No que segue mostraremos que é sempre possível escolher $\alpha \in F$ tal que $F = K(\alpha) \simeq \dfrac{K[X]}{(f_k)} = F_k$, com $k = -T_{F|K}(\alpha) \neq 0$.

Teorema 2.4. *Sejam F uma extensão cúbica cíclica de K e σ um gerador do grupo $Gal(F|K)$. Então existe $\alpha \in F$ tal que $F = K(\alpha)$, $k = -T_{F|K}(\alpha) \neq 0$ e f_k é o seu polinômio mínimo sobre K.*

Demonstração. Já sabemos, pelo Teorema 2.3, que existe $u \in F$ tal que $F = K(u)$, cujo polinômio mínimo sobre K é do tipo f_l, para algum $l \in K$. Obviamente, se $l \neq 0$ nada há a demonstrar. Este é o caso (necessariamente) quando a característica de K é 3 (veja Lema 2.1).

Suponhamos então que $l = 0$. Logo a característica de K é necessariamente distinta de 3, $u^3 = 3u - 1$, $\sigma(u) = u^2 - 2$ e $\sigma^2(u) = -u^2 - u + 2$. Mais ainda, é imediato verificar que todo elemento do $Ker(T_{F|K})$ é da forma $au + b\sigma(u)$, com $a, b \in K$.

Mostremos que $\alpha = 1 + \dfrac{\sigma(u)}{u} \notin Ker(T_{F|K})$. De fato, se existem $a, b \in K$ tais que $\alpha = au + b\sigma(u)$ então

$$u + \sigma(u) = au^2 + bu\sigma(u) = a(\sigma(u) + 2) + b(u - 1)$$

ou

$$u + \sigma(u) = (2a - b) + bu + a\sigma(u).$$

Como u, $\sigma(u) \in Ker(T_{F|K})$ e são linearmente independentes sobre K e $3 \neq 0$ em K segue que $a = b = 1$ e $0 = 2a - b = 1$, o que é um absurdo.

Portanto $T_{F|K}(\alpha) \neq 0$. Da independência linear de $1,\ u,\ u^2$ sobre K decorre trivialmente que $\alpha \notin K$ e por conseguinte $F = K(\alpha)$ e f_k, com $k = -T_{F|K}(\alpha)$, é o polinômio mínimo de α sobre K, conforme os mesmos argumentos já vistos na demonstração do teorema anterior. □

Se F é uma extensão cúbica cíclica de K e σ denota um gerador do grupo $Gal(F|K)$, uma base de F sobre K do tipo $\{z,\ \sigma(z),\ \sigma^2(z)\}$, para algum $z \in F$, é chamada uma **base**

normal de F sobre K e o elemento z é chamado **gerador** de uma base normal de F sobre K. De acordo com o Lema P.1 do Apêndice, o elemento $\alpha \in F$ tal que $F = K(\alpha)$ e $T_{F|K}(\alpha) \neq 0$, construído no Teorema 2.4 acima é um exemplo de elemento primitivo de uma extensão que ao mesmo tempo gera uma base normal dessa extensão (veja Teorema P.2 das Preliminares). Em geral isso não ocorre.

Para encerrar esta seção reapresentaremos a descrição de extensões cúbicas cíclicas conforme a Teoria de Kummer (resp. Artin-Schreier) como uma conseqüência imediata dos resultados acima obtidos.

Como é sabido, na Teoria de Kummer (resp. Artin-Schreier) o corpo base K é assumido possuir raiz cúbica primitiva da unidade (resp. característica 3) e as extensões cúbicas cíclicas de K são descritas em função de um polinômio cúbico do tipo $X^3 - a$ (resp. $X^3 - X - b$), com $a \in K^\star \backslash (K^\star)^3$ (resp. $b \in K \backslash \{x^3 - x \mid x \in K\}$). Na descrição que daremos a seguir apresentaremos esse elemento a (resp. b) em função de um mesmo parâmetro $k \in K$ sujeito a uma única restrição: $k \neq 0, \dfrac{\lambda^3 - 3\lambda + 1}{\lambda - \lambda^2}$, para todo $\lambda \in K \backslash \{0, 1\}$. De uma certa forma esse resultado unifica aquelas duas teorias.

Teorema 2.5.

(i) **[Kummer]** *Suponhamos que a característica de K é distinta de 3 e K possui uma raiz cúbica primitiva ζ da unidade. Se F é uma extensão cúbica cíclica de K então F é do tipo $\dfrac{K[X]}{(X^3 - a(k))}$, com $a(k) = (3\zeta^2 - k)(k^2 + 3k + 9)$ e $k \neq 0, \dfrac{\lambda^3 - 3\lambda + 1}{\lambda - \lambda^2}$, para todo $\lambda \in K \backslash \{0, 1\}$. E, neste caso, se σ é um gerador do grupo $Gal(F|K)$ então $\sigma(x) = \zeta x$ ou $\sigma(x) = \zeta^2 x$, onde $x = X + (X^3 - a(k))$.*

(ii) **[Artin-Schreier]** *Se a característica de K é igual a 3 e F é uma extensão cúbica cíclica de K então F é do tipo $\dfrac{K[X]}{(X^3 - X - b(k))}$, com $b(k) = \dfrac{1}{k}$ e $k \neq 0, \dfrac{\lambda^3 - 3\lambda + 1}{\lambda - \lambda^2}$, para todo $\lambda \in K \backslash \{0, 1\}$. E, neste caso, se σ é um gerador do grupo $Gal(F|K)$ então $\sigma(x) = x + 1$ ou $\sigma(x) = x + 2$, onde $x = X + (X^3 - X - b(k))$.*

Demonstração. Se F é uma extensão cúbica cíclica de K então, conforme Teorema 2.4, existe $\alpha \in F$ tal que $F = K(\alpha)$, $k = -T_{F|K}(\alpha) \neq 0$ e cujo polinômio mínimo sobre K é f_k.

E, por Lema 2.1, $k \neq \dfrac{\lambda^3 - 3\lambda + 1}{\lambda - \lambda^2}$, para todo $\lambda \in K\backslash\{0,1\}$, $\sigma(\alpha) = \dfrac{\alpha - 1}{\alpha}$ e $\sigma^2(\alpha) = \dfrac{1}{1-\alpha}$.

Na seqüência $N_{F|K} : F \to K$ denota a aplicação norma de F sobre K definida por $N_{F|K}(x) = x\sigma(x)\sigma^2(x)$, para todo $x \in F$.

(i) A característica de K é distinta de 3 e $\zeta \in K$ é uma raiz cúbica primitiva da unidade. Seja $z = \alpha + \zeta\sigma^2(\alpha) + \zeta^2\sigma(\alpha)$. É imediato verificar que $\sigma(z) = \zeta z$ e $\sigma^2(z) = \zeta^2 z$. Portanto $z \notin K$ e por conseguinte $F = K(z)$. Finalmente, de

$$z^3 = T_{F|K}(\alpha^3) + 6N_{F|K}(\alpha) + 3\zeta^2 T_{F|K}(\alpha^2\sigma(\alpha)) + 3\zeta T_{F|K}(\alpha\sigma(\alpha)^2),$$

$$T_{F|K}(\alpha^3) = -k(k^2 + 3k + 9) - 3, \qquad N_{F|K}(\alpha) = -1,$$

$$T_{F|K}(\alpha^2\sigma(\alpha)) = k^2 + 3k + 6 \qquad \text{e} \qquad T_{F|K}(\alpha\sigma(\alpha)^2) = -3$$

obtemos $z^3 = a(k)$, com $a(k) = (3\zeta^2 - k)(k^2 + 3k + 9)$.

(ii) A característica de K é 3. Seja $z = \dfrac{1}{k}(\alpha - \sigma(\alpha))$. É imediato que

$$T_{F|K}(z) = 0, \qquad T_{F|K}(z\sigma(z)) = -1 \qquad \text{e} \qquad N_{F|K}(z) = \frac{1}{k}.$$

Portanto $z^3 - z - \dfrac{1}{k} = 0$. De $\sigma(z) = \dfrac{1}{k}(\sigma(\alpha) - \sigma^2(\alpha)) = \dfrac{1}{k}(\sigma(\alpha) + k + \alpha + \sigma(\alpha)) = z + 1$ decorre que $z \notin K$ e portanto $F = K(z)$. □

3 Descrição de extensões cúbicas cíclicas racionais - uma versão geométrica

O propósito nesta seção é apresentar, via a trigonometria, os aspectos geométricos que dão origem a uma extensão cúbica cíclica racional. Em toda esta seção o corpo K é assumido ser o corpo $\mathbb{Q}$ dos números racionais. Portanto toda extensão cúbica cíclica racional aqui considerada é, conforme a literatura, o corpo de raízes $F \subset \mathbb{R}$ de um polinômio cúbico a coeficientes racionais e cujo discriminante é um quadrado racional ([10], Theorem 78).

Conforme veremos na seqüência, toda extensão cúbica cíclica F de $\mathbb{Q}$ é do tipo $F = \mathbb{Q}(\alpha)$ com α qualquer um dos cossenos dos ângulos γ_j, $0 \leq j \leq 2$, tais que os três pontos $e^{\mathbf{i}\gamma_j}$ do círculo unitário $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ determinam um triângulo eqüilátero. E também veremos que um triângulo com vértices $\zeta^j e^{\mathbf{i}\gamma}, 0 \leq j \leq 2$, onde $\zeta \in \mathbb{C}$ é uma raiz cúbica primitiva da unidade, corresponde a uma extensão cúbica cíclica de $\mathbb{Q}$ se $\gamma \neq 0, \pi$ e para $\Gamma = 3\gamma$ os cossenos dos três ângulos $\Gamma + j\frac{2\pi}{3}$ são números racionais. Mais ainda, todos os ângulos Γ satisfazendo essa condição serão explicitamente descritos em termos de elementos de $\mathbb{Z}[\zeta]$.

Teorema 3.1. *Toda extensão cúbica cíclica F de $\mathbb{Q}$ é do tipo $F = \frac{\mathbb{Q}[X]}{(f)}$, com $f = X^3 - 3X - a$, para algum $a \in \mathbb{Q}$. Além disso, existe $\Gamma \in \frac{\mathbb{R}}{2\pi\mathbb{Z}}$ tal que $a = 2\cos(\Gamma)$ e $2\cos(\frac{\Gamma}{3} + j\frac{2\pi}{3})$, com $0 \leq j \leq 2$, são todas as raízes de f.*

Demonstração. Seja σ um gerador do grupo $Gal(F|\mathbb{Q})$. Conforme Teorema P.3 das Preliminares, existem elementos $z_0 = z$, $z_1 = \sigma(z)$, e $z_2 = \sigma^2(z)$ em F tais que $z_0 + z_1 + z_2 = 1$ e $z_0z_1 + z_1z_2 + z_2z_0 = 0$. Então se $c = z_0z_1z_2$ temos $(X - z_0)(X - z_1)(X - z_2) = X^3 - X^2 - c$.

Tomando $\alpha = 3z - 1 \in F$ vemos que $\frac{\alpha}{3}$ é raiz do polinômio $X^3 - \frac{1}{3}X - \frac{2}{27} - c$. Logo α é raiz do polinômio $f = X^3 - 3X - a$, com $a = 2 + 27c$. Desde que $\alpha \notin \mathbb{Q}$ então $F = \mathbb{Q}(\alpha)$ e f é o seu polinômio mínimo sobre $\mathbb{Q}$.

Por outro lado, o discriminante do polinômio f é dado pelo determinante da matriz $(T_{F|\mathbb{Q}}(\alpha^{i+j}))_{0\leq i,j\leq 2}$. Calculando esse determinante vemos que ele é igual a $27(4 - a^2)$ e desde

que ele é um quadrado não nulo em $\mathbb{Q}$, pois $F|\mathbb{Q}$ é cúbica cíclica ([10], Theorem 78), então necessariamente $a^2 < 4$ ou $|\frac{a}{2}| < 1$. Agora, tomando $\Gamma = \arccos(\frac{a}{2})$ e usando a relação trigonométrica $2\cos(\Gamma) = (2\cos(\frac{\Gamma}{3}))^3 - 3(2\cos(\frac{\Gamma}{3}))$ vemos que $2\cos(\frac{\Gamma}{3} + j\frac{2\pi}{3}) \in \mathbb{R}$ são todas as raízes de f, obviamente em F pois α é uma delas. □

Para a segunda parte do nosso propósito nesta seção, conforme anunciado acima, necessitamos de alguma preparação preliminar. Observamos que os resultados auxiliares, que apresentaremos a seguir, são válidos mais geralmente para anéis comutativos com elemento identidade quaisquer, conforme pode ser visto, por exemplo, em [5], [9] e [12].

Sejam G um grupo cíclico de ordem 3 e gerador σ, $\mathbb{Q}G$ a correspondente álgebra de grupo racional e $W(\mathbb{Q}) = \{\upsilon \in \mathbb{Q}G \mid \upsilon l(\upsilon) = 1\}$, onde $l : \mathbb{Q}G \to \mathbb{Q}G$ é o isomorfismo de $\mathbb{Q}$-álgebras dado por $l(\sigma^j) = \sigma^{-j}$. Claramente $W(\mathbb{Q})$ é um subgrupo do grupo multiplicativo das unidades de $\mathbb{Q}G$.

Lema 3.2. *Sejam* $\upsilon = \upsilon_0 + \upsilon_1\sigma^2 + \upsilon_2\sigma \in \mathbb{Q}G$, $t_1(\upsilon) = \upsilon_0^2\upsilon_1 + \upsilon_1^2\upsilon_2 + \upsilon_2^2\upsilon_0$ *e* $t_2(\upsilon) = \upsilon_0\upsilon_1^2 + \upsilon_1\upsilon_2^2 + \upsilon_2\upsilon_0^2$. *Se* $\upsilon \in W(\mathbb{Q})$ *então* $t_1(\upsilon) + t_2(\upsilon) = 3(t_1(\upsilon)^2 + t_1(\upsilon)t_2(\upsilon) + t_2(\upsilon)^2)$.

Demonstração. Comecemos por observar que se $\upsilon \in W(\mathbb{Q})$, então da relação $\upsilon l(\upsilon) = 1$ decorre que $\sum_{0\le i\le 2} \upsilon_i = 1$ e $\sum_{0\le i\le 2} \upsilon_i\upsilon_{i+1(\mathrm{mod}\,3)} = 0$. Conseqüentemente de

$$(\sum_{0\le i\le 2} \upsilon_i)(\sum_{0\le i\le 2} \upsilon_i\upsilon_{i+1(\mathrm{mod}\,3)}) = 0 \qquad \text{e} \qquad (\sum_{0\le i\le 2} \upsilon_i)^3 = 1$$

obtemos

$$t_1(\upsilon) + t_2(\upsilon) = -3\upsilon_0\upsilon_1\upsilon_2 \qquad \text{e} \qquad \sum_{0\le i\le 2} \upsilon_i^3 = 1 - t_1(\upsilon) - t_2(\upsilon),$$

respectivamente. Além disso,

$$\begin{aligned} t_1(\upsilon)t_2(\upsilon) &= (\upsilon_0^2\upsilon_1 + \upsilon_1^2\upsilon_2 + \upsilon_2^2\upsilon_0)(\upsilon_0\upsilon_1^2 + \upsilon_1\upsilon_2^2 + \upsilon_2\upsilon_0^2) \\ &= 3\upsilon_0^2\upsilon_1^2\upsilon_2^2 + \upsilon_0\upsilon_1\upsilon_2(\upsilon_0^3 + \upsilon_1^3 + \upsilon_2^3) + (\upsilon_0^3\upsilon_1^3 + \upsilon_0^3\upsilon_2^3 + \upsilon_1^3\upsilon_2^3) \\ &= \upsilon_0\upsilon_1\upsilon_2(\upsilon_0^3 + \upsilon_1^3 + \upsilon_2^3 + 3\upsilon_0\upsilon_1\upsilon_2) + (\upsilon_0^3\upsilon_1^3 + \upsilon_0^3\upsilon_2^3 + \upsilon_1^3\upsilon_2^3) \\ &= -\frac{1}{3}(t_1(\upsilon) + t_2(\upsilon))[1 - 2(t_1(\upsilon) + t_2(\upsilon))] + (\upsilon_0^3\upsilon_1^3 + \upsilon_0^3\upsilon_2^3 + \upsilon_1^3\upsilon_2^3). \end{aligned}$$

E de

$$\begin{aligned}
v_0^3v_1^3 &= -v_0^2v_1^2(v_0v_2+v_1v_2) = -v_0^3v_1^2v_2 - v_0^2v_1^3v_2,\\
v_0^3v_2^3 &= -v_0^2v_2^2(v_0v_1+v_1v_2) = -v_0^3v_1v_2^2 - v_0^2v_1v_2^3,\\
v_1^3v_2^3 &= -v_1^2v_2^2(v_0v_1+v_0v_2) = -v_0v_1^3v_2^2 - v_0v_1^2v_2^3,
\end{aligned}$$

obtemos

$$\begin{aligned}
v_0^3v_1^3 + v_0^3v_2^3 + v_1^3v_2^3 &= -v_0v_1v_2[(v_0^2v_1+v_1^2v_2+v_2^2v_0)+(v_0v_1^2+v_1v_2^2+v_2v_0^2)]\\
&= \frac{1}{3}(t_1(v)+t_2(v))^2.
\end{aligned}$$

Conseqüentemente,

$$t_1(v)t_2(v) = -\frac{1}{3}(t_1(v)+t_2(v)) + (t_1(v)+t_2(v))^2$$

e finalmente

$$\begin{aligned}
3(t_1(v)^2 + t_1(v)t_2(v) + t_2(v)^2) &= 3(t_1(v)+t_2(v))^2 - 3t_1(v)t_2(v)\\
&= t_1(v)+t_2(v).
\end{aligned}$$

E assim completamos a demonstração. □

Consideremos a aplicação $\tau : \mathbb{Q}G \to \mathbb{Q}\times\mathbb{Q}$ dada por $\tau(v) = (t_1(v), t_2(v))$, onde

$$t_1(v) = v_0^2v_1 + v_1^2v_2 + v_2^2v_0 \qquad \text{e} \qquad t_2(v) = v_0v_1^2 + v_1v_2^2 + v_2v_0^2,$$

para todo $v = v_0 + v_1\sigma^2 + v_2\sigma \in \mathbb{Q}G$.

Pelo Lema 3.2 a restrição de τ a $W(\mathbb{Q})$ induz uma aplicação

$$\tau^* : W(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}) := \{(t_1,t_2) \in \mathbb{Q}\times\mathbb{Q} \mid t_1+t_2 = 3(t_1^2+t_1t_2+t_2^2)\}.$$

Observemos que $\mathcal{C}(\mathbb{Q})$ tem uma estrutura de grupo abeliano, induzida pela τ^*, cuja operação é dada por

$$(t_1,t_2)\star(s_1,s_2) = (u_1,u_2)$$

com

$$u_1 = t_1 + s_1 - 6t_1s_1 - 3t_1s_2 - 3t_2s_1 + 3t_2s_2$$

e

$$u_2 = t_2 + s_2 - 6t_2s_2 - 3t_2s_1 - 3t_1s_2 + 3t_1s_1.$$

Vê-se claramente que o par $(0,0)$ é o elemento neutro e que $(t_1,t_2)^{-1} = (t_2,t_1)$ é o inverso para operação "$\star$". Além disso, também pode-se ver que τ^* é um homomorfismo de grupos .

E desde que $\tau^*(1-3(t_1+t_2)+3t_1\sigma^2+3t_2\sigma) = (t_1,t_2)$ para todo par $(t_1,t_2) \in \mathcal{C}(\mathbb{Q})$, vemos também que τ^* é sobrejetivo. Com isto demonstramos a seguinte proposição.

Proposição 3.3. *A aplicação $\tau^* : W(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q})$ conforme definidos acima é um epimorfismo de grupos.* □

Para o que se segue denotaremos $S(\mathbb{Q}) = \mathbb{Q}[\zeta] \bigcap S^1$, onde $\zeta \in \mathbb{C}$ é uma raíz cúbica primitiva da unidade. Note que $N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(a+b\zeta) = |a+b\zeta|^2$, para todo $a,b \in \mathbb{Q}$. Logo $S(\mathbb{Q}) = \{\lambda \in \mathbb{Q}[\zeta] \mid N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(\lambda) = 1\}$.

Definimos uma aplicação $\chi : \mathbb{Q}G \to \mathbb{Q}[\zeta]$ dada por $\chi(\sum_{0\leq i\leq 2} a_i\sigma^{-i}) = \sum_{0\leq i\leq 2} a_i\zeta^{-i}$, a qual é claramente um homomorfismo de anéis . Mais ainda, se $v \in W(\mathbb{Q})$ então $\chi(v) \in S(\mathbb{Q})$. Logo a restrição de χ a $W(\mathbb{Q})$ induz um homomorfismo de grupos $\chi^* : W(\mathbb{Q}) \to S(\mathbb{Q})$, dada por $\chi^*(\lambda_0+\lambda_1\sigma^2+\lambda_2\sigma) = (\lambda_0-\lambda_1)+(\lambda_2-\lambda_1)\zeta$. Essa aplicação é claramente injetiva e se $a+b\zeta \in S(\mathbb{Q})$ então $w = \frac{1}{3}[(1+2a-b)+(1-a-b)\sigma^2+(1-a+2b)\sigma] \in W(\mathbb{Q})$ e $\chi^*(w) = a+b\zeta$, ou seja, χ^* é de fato um isomorfismo de grupos . Com isto demonstramos a seguinte proposição.

Proposição 3.4. *A aplicação $\chi^* : W(\mathbb{Q}) \to S(\mathbb{Q})$ tal que $\chi^*(\lambda_0+\lambda_1\sigma^2+\lambda_2\sigma) = (\lambda_0-\lambda_1)+(\lambda_2-\lambda_1)\zeta$ é um isomorfismo de grupos.* □

À semelhança do caso de corpos, adotaremos também a notação $R^\star$ para indicar o conjunto dos elementos não nulos de um anel comutativo R qualquer, mesmo que R não seja um corpo.

No que se seguirá o particular anel R que consideraremos é o anel $\mathbb{Z}[\zeta]$. Note que $\mathbb{Z}[\zeta]^\star$, com a multiplicação induzida de $\mathbb{Z}[\zeta]$, é um monóide comutativo cancelativo , isto é, $\mathbb{Z}[\zeta]^\star$ é fechado para a multiplicação de $\mathbb{Z}[\zeta]$, a qual é associativa, comutativa e para a qual vale a lei do cancelamento e $1 = 1 + 0\zeta \in \mathbb{Z}[\zeta]^\star$.

Sobre esse monóide definimos a seguinte relação de eqüivalência : $(a+b\zeta) \sim (c+d\zeta)$ se e somente se existem $\lambda, \lambda' \in \mathbb{Z}^\star$ tais que $\lambda(a + b\zeta) = \lambda'(c + d\zeta)$, quaisquer que sejam $a, b, c, d \in \mathbb{Z}$.

Denotamos por $V = \dfrac{\mathbb{Z}[\zeta]^\star}{\mathbb{Z}^\star}$ o conjunto das classes de equivalência $[v]$ representadas pelos elementos $v \in \mathbb{Z}[\zeta]^\star$. Esse conjunto V tem naturalmente uma estrutura de grupo comutativo induzida pela multiplicação de $\mathbb{Z}[\zeta]^\star$. O elemento neutro para a multiplicação de V é $[1] = [\lambda]$, para qualquer $\lambda \in \mathbb{Z}^\star$ e se $v = a + b\zeta \in \mathbb{Z}[\zeta]^\star$ então $[v]^{-1} = [\overline{v}]$, com $\overline{v} = (a - b) - b\zeta$.

Observemos agora que para todo $v \in \mathbb{Z}[\zeta]^\star$ temos

$$\frac{v^2}{N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v)} \in \mathbb{Q}[\zeta] \qquad \text{e} \qquad N_{\mathbb{Q}[\zeta]|\mathbb{Q}}\left(\frac{v^2}{N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v)}\right) = 1,$$

ou seja $\dfrac{v^2}{N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v)} \in S(\mathbb{Q})$.

Além disso $v \in \mathbb{Z}^\star$ se e somente se $N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v) = v^2$. Isto nos permite, portanto, definir uma aplicação $\varphi : V \to S(\mathbb{Q})$, dada por $[v] \mapsto \dfrac{v^2}{N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v)}$, para todo $v \in \mathbb{Z}[\zeta]^\star$, a qual é injetiva e obviamente um homomorfismo de grupos.

Veremos que φ é um isomorfismo mostrando a sua sobrejetividade. Para tanto, dado $\omega = \cos(\alpha) + \mathbf{i}\,\mathrm{sen}(\alpha) \in S(\mathbb{Q})$ é suficiente encontrar $z \in \mathbb{Q}[\zeta]$ cujo argumento $\arg(z)$ é $\dfrac{\alpha}{2}$. De fato, encontrado tal z, temos primeiramente $v = \lambda z \in \mathbb{Z}[\zeta]^\star$ para algum $\lambda \in \mathbb{Z}^\star$ e $\arg(v) = \arg(z) = \dfrac{\alpha}{2}$. Em seguida observemos que $v = N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v)\left(\cos(\frac{\alpha}{2}) + \mathbf{i}\,\mathrm{sen}(\frac{\alpha}{2})\right)$ e portanto $\dfrac{v^2}{N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v)} = N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v)\omega$. Como $N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(\omega) = 1 = N_{\mathbb{Q}[\zeta]|\mathbb{Q}}\left(\dfrac{v^2}{N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v)}\right)$ então $N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v) = 1$ e $\varphi([v]) = \omega$.

Finalmente tomando $z = 1 + \omega$ temos $z \in \mathbb{Q}[\zeta]$ e $\arg(z) = \dfrac{\alpha}{2}$. Para visualizar esta última afirmação é suficiente construir o paralelogramo de vértices $0,\ 1,\ \omega$ e $1 + \omega$. Isto conclui a demonstração da seguinte proposição.

Proposição 3.5. *A aplicação $\varphi : V \to S(\mathbb{Q})$ conforme definida acima é um isomorfismo de grupos.* □

Segundo a Proposição P.5 das Preliminares, toda extensão cúbica cíclica de $\mathbb{Q}$ determina um elemento de $\mathcal{C}(\mathbb{Q})$ e portanto, pelas Proposições 3.3 e 3.4, um elemento de $S(\mathbb{Q})$. A recíproca veremos nos resultados seguintes.

Lema 3.6. $S(\mathbb{Q}) = \{e^{\mathbf{i}\Gamma} \in S^1 \mid \cos(\Gamma + j\frac{2\pi}{3}) \in \mathbb{Q},\ 0 \leq j \leq 2\}$.

Demonstração. Se $z \in S(\mathbb{Q})$ então $z = e^{\mathbf{i}\Gamma} = \cos(\Gamma) + \mathbf{i}\,\mathrm{sen}(\Gamma)$, para algum $\Gamma \in \dfrac{\mathbb{R}}{2\pi\mathbb{Z}}$ e $z = a + b\zeta$, com $a, b \in \mathbb{Q}$. Então $\cos(\Gamma) = a - \dfrac{b}{2} \in \mathbb{Q}$ e desde que $\sqrt{3}\,\mathrm{sen}(\Gamma) = \dfrac{3b}{2} \in \mathbb{Q}$ temos também $\cos(\Gamma \pm j\frac{2\pi}{3}) \in \mathbb{Q}$. Reciprocamente, $\cos(\Gamma + j\frac{2\pi}{3}) \in \mathbb{Q}$, para todo $0 \leq j \leq 2$, implica $\sqrt{3}\,\mathrm{sen}(\Gamma) \in \mathbb{Q}$. Logo $\zeta\sqrt{3}\,\mathrm{sen}(\Gamma) \in \mathbb{Q}[\zeta]$ de onde decorre que $\mathbf{i}\,\mathrm{sen}(\Gamma) \in \mathbb{Q}[\zeta]$ e portanto $\cos(\Gamma) + \mathbf{i}\,\mathrm{sen}(\Gamma) \in \mathbb{Q}[\zeta]$. □

Teorema 3.7. *Seja $e^{\mathbf{i}\Gamma} \in S(\mathbb{Q})\backslash\{\pm 1\}$. Então*

$$\mathbb{Q}(\cos(\frac{\Gamma}{3})) = \frac{\mathbb{Q}[X]}{(X^3 - 3X - a)},\ \ \textit{com}\ \ a = \frac{2s^2 - 2st - t^2}{s^2 - st - t^2}\ \ \textit{e}\ \ \varphi[s + t\zeta] = e^{\mathbf{i}\Gamma}.$$

Além disso $\mathbb{Q}(\cos(\dfrac{\Gamma}{3}))$ é uma extensão cúbica cíclica de $\mathbb{Q}$.

Demonstração. Conforme a Proposição 3.5, se $e^{\mathbf{i}\Gamma} \in S(\mathbb{Q})$ existe $v = s + t\zeta \in \mathbb{Z}[\zeta]^\star$ tal que $\varphi([v]) = e^{\mathbf{i}\Gamma}$. Disto decorre imediatamente que $N_{\mathbb{Q}[\zeta]|\mathbb{Q}}(v) = 1$ e $\arg(v) = \dfrac{\Gamma}{2}$. Então $s + t\zeta = \cos(\dfrac{\Gamma}{2}) + \mathbf{i}\,\mathrm{sen}(\dfrac{\Gamma}{2})$, de onde decorre, em particular, que $\mathrm{tg}(\dfrac{\Gamma}{2}) = \dfrac{\sqrt{3}\,t}{2s - t}$. Usando o fato de que $\cos(\Gamma) = \dfrac{1 - \mathrm{tg}^2(\frac{\Gamma}{2})}{1 + \mathrm{tg}^2(\frac{\Gamma}{2})}$ obtemos $a = 2\cos(\Gamma) = \dfrac{2s^2 - 2st - t^2}{s^2 - st + t^2}$. Desde que, por hipótese, $e^{\mathbf{i}\Gamma} \neq \pm 1$ então $\Gamma \neq 0, \pi$ e conseqüentemente $\cos(\dfrac{\Gamma}{3}) \neq \pm\dfrac{1}{2}, 1$. Por outro lado pode-se verificar facilmente que esses são os únicos possíveis valores racionais que podem ser assumidos por $\cos(\dfrac{\arg(z)}{3})$, para todo $z \in S(\mathbb{Q})$. Portanto $\cos(\dfrac{\Gamma}{3}) \notin \mathbb{Q}$.

Agora, pelos mesmos argumentos usados no Teorema 3.1, concluímos que $X^3 - 3X - a$, com $a = 2\cos(\Gamma)$, é o polinômio mínimo de $2\cos(\frac{\Gamma}{3})$ e $\mathbb{Q}(\cos(\frac{\Gamma}{3})) = \frac{\mathbb{Q}[X]}{(X^3 - 3X - a)}$ é um corpo, obviamente extensão cúbica de $\mathbb{Q}$.

Finalmente observe que o discriminante de $X^3 - 3X - a$ é igual a $108 - 27a^2 = 108 - 27(4\cos^2(\Gamma)) = 108(1 - \cos^2(\Gamma)) = 108\,\mathrm{sen}^2(\Gamma) = (6\sqrt{3}\,\mathrm{sen}(\Gamma))^2$. Desde que $\sqrt{3}\,\mathrm{sen}(\Gamma) \in \mathbb{Q}$ pelo Lema 3.6 , então o discriminante do polinômio $X^3 - 3X - a$ é um quadrado em $\mathbb{Q}$ e portanto $\mathbb{Q}(\cos(\frac{\Gamma}{3}))$ é uma extensão cúbica cíclica de $\mathbb{Q}$. □

4 Quando duas extensões cúbicas cíclicas são isomorfas?

Na seção 1 demos uma resposta a esta questão, via a Teoria de Kummer, no caso em que a característica de K é distinta de 3. Nesta seção consideraremos o caso geral sem qualquer restrição sobre a característica de K.

Os resultados que aqui serão apresentados são especializações ao caso cúbico de resultados mais gerais devidos a C. Dragos [3]. Os resultados de Dragos são muito interessantes pois são testes efetivos que permitem dar resposta rapidamente à pergunta título. Particularmente no caso cúbico, esses testes envolvem somente fatoração de polinômios (mais especificamente um único polinômio de grau 9) ou o cálculo de variações do determinante de Vandermonde de ordem 3.

Começamos esta seção observando que a pergunta título só tem sentido se o corpo de base K for infinito. Recordemos que se K for finito, então $\#(K) = p^n$ para algum primo p e algum inteiro $n \geq 1$ e toda extensão cúbica de K é necessariamente cíclica e corpo de raízes do polinômio $X^{p^{3n}} - X$. Conseqüentemente quaisquer duas extensões cúbicas de um corpo finito K qualquer são sempre isomorfas e nada há a considerar neste caso.

Portanto, nesta seção K denotará sempre um corpo infinito. Em tudo o que se seguirá $F_k = K(\alpha)$ e $F_l = K(\beta)$ denotarão duas extensões cúbicas cíclicas de K e f_k e f_l os respectivos polinômios mínimos de α e β sobre K. Denotaremos igualmente por σ os geradores dos grupos $Gal(F_k|K)$ e $Gal(F_l|K)$ respectivamente.

Sejam $\alpha_i = \sigma^i(\alpha)$ e $\beta_i = \sigma^i(\beta)$, $0 \leq i \leq 2$. Como K é infinito sempre existe $t \in K^\star$ tal que $t \neq \dfrac{\alpha_i - \alpha_{i'}}{\beta_j - \beta_{j'}}$, para quaisquer índices $i \neq i'$ e $j \neq j'$.

Para um tal t consideremos o polinômio $H_t = \prod_{0 \leq i,j \leq 2} (X - (\alpha_i + t\beta_j))$.

Por construção H_t é claramente um polinômio com coeficientes em K e separável sobre K.

O teorema seguinte nos dá um efetivo teste para decidir se os parâmetros k e l determinam a mesma extensão cúbica cíclica de K em função da irredutibilidade, ou não,

do polinômio H_t sobre K.

Antes de enunciarmos o teorema observemos que se $F_k \simeq F_l$ então existe $\alpha' \in F_l$ (resp. $\beta' \in F_k$) tal que $f_k(\alpha') = 0$ (resp. $f_l(\beta') = 0$) e $K(\alpha') = F_l$ (resp. $K(\beta') = F_k$). Portanto para decidir quando as extensões F_k e F_l são isomorfas é suficiente decidir quando elas são iguais.

Para quaisquer duas extensões de E e F de K denotaremos por $Alg_K(E, F)$ o conjunto dos homomorfismos de K-álgebras de E em F.

Teorema 4.1. *As extensões cúbicas cíclicas F_k e F_l são iguais (a menos de isomorfismo) se e somente se H_t possui um fator irredutível de grau 3 em $K[X]$. Em particular, neste caso, H_t é um produto de três fatores irredutíveis de grau 3 em $K[X]$.*

Demonstração. Primeiramente, mostraremos que o polinômio H_t tem um fator irredutível de grau 3 em $K[X]$. Por hipótese, para cada $0 \leq j \leq 2$, $K(\alpha) = K(\beta_j)$. Portanto $K \subset K(\alpha + t\beta_j) \subset K(\alpha)$. Note que $\#Alg_K(K(\alpha), \overline{K}) = [K(\alpha) : K] = 3$, onde $\overline{K}$ denota um fecho algébrico de K.

Decorre da escolha do elemento $t \in K^\star$ que $\sigma^i|_{K(\alpha+t\beta_j)} \neq \sigma^{i'}|_{K(\alpha+t\beta_j)}$, para todo $i \neq i'$.

Logo

$$\begin{aligned} 3 = \#Alg_K(K(\alpha), \overline{K}) &\leq \#Alg_K(K(\alpha + t\beta_j), \overline{K}) \\ &= [K(\alpha + t\beta_j) : K] \leq [K(\alpha) : K] = 3 \end{aligned}$$

e conseqüentemente

$$3 = \#Alg_K(K(\alpha + t\beta_j), \overline{K}) = [K(\alpha + t\beta_j) : K].$$

Portanto o polinômio mínimo h_j de $\alpha + t\beta_j$ sobre K, que é um fator irredutível de H_t em $K[X]$, tem grau 3. Assim temos mostrado que $H_t = h_0 h_1 h_2$.

Reciprocamente, seja $h \in K[X]$ um fator irredutível de H_t de grau 3. Mostremos que $F_k = F_l$. Suponhamos por absurdo que não e tomemos uma raiz $\alpha_i + t\beta_j$ de h. Logo,

$\beta_j \notin K(\alpha_i)$. Então $K(\alpha_i) \subsetneq K(\alpha_i, \beta_j)$ e para cada $0 \leq s \leq 2$ existe um isomorfismo $\tau_s : K(\alpha_i, \beta_j) \to K(\alpha_i, \beta_{j+s})$ tal que $\tau_s|_{K(\alpha_i)} = \mathrm{id}_{K(\alpha_i)}$ e $\tau_s(\beta_j) = \beta_{j+s}$. Portanto, para cada $0 \leq s \leq 2$ o elemento $\alpha_i + t\beta_{j+s}$ é raiz do polinômio h em $K(\alpha_i, \beta_{j+s}) = K(\alpha_i, \beta_j)$.

Por outro lado, para cada $0 \leq r \leq 2$, o elemento $\sigma^r(\alpha_i + t\beta_j) = \alpha_{i+r} + t\beta_{j+r}$ também é raiz do polinômio h em $K(\alpha_i, \beta_j)$.

Desde que esses elementos são todos distintos concluímos que o número de raízes do polinômio h em $K(\alpha_i, \beta_j)$ é estritamente superior ao seu grau, o que é uma contradição. □

Consideremos agora o seguinte determinante, o qual é não nulo devido à separabilidade de F_k sobre K.

$$\Delta = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \end{vmatrix} = \prod_{0 \leq i < j \leq 2} (\alpha_j - \alpha_i) = -(k^2 + 3k + 9) \ .$$

Os próximos resultados envolvem relações entre determinantes obtidos a partir de Δ por substituição de linhas e permutação cíclica das mesmas.

Já para o resultado seguinte iremos considerar os determinantes Δ_j, $0 \leq j \leq 2$, obtidos de Δ substituindo a j-ésima linha de Δ pela linha $(\beta_0, \beta_1, \beta_2)$.

Teorema 4.2. *As seguintes afirmações são eqüivalentes:*

(i) $F_k = F_l$.

(ii) *Para cada* $0 \leq i \leq 2$, *existe* $a_i \in K$ *tal que* $\Delta_i = a_i \Delta$.

(iii) *Para cada* $0 \leq i \leq 2$, $\Delta_i \in K$.

Demonstração.

(i)⇒(ii) Suponhamos que $F_k = F_l$. Logo a menos de uma eventual permutação de índices, se necessário, podemos supor que $K(\alpha_i) = K(\beta_i)$. Portanto podemos afirmar que

existe um polinômio $h = a_0 + a_1X + a_2X^2 \in K[X]$ tal que $\beta_i = h(\alpha_i) = a_0 + a_1\alpha_i + a_2\alpha_i^2$ para todo $0 \leq i \leq 2$.

Assim vemos que combinando linearmente as demais linhas de Δ_i, segundo os coeficientes do polinômio h e convenientemente de forma a eliminar termos em α_i^j, com $j \neq i$, obtemos a i-ésima linha de Δ_i igual a i-ésima linha de Δ multiplicada por a_i. Portanto $\Delta_i = a_i\Delta$.

(ii)$\Leftrightarrow$(iii) Imediato.

(iii)$\Rightarrow$(i) Comecemos considerando o K-espaço vetorial K^3 e o $\overline{K}$-espaço vetorial $\overline{K}^3$, onde $\overline{K}$ denota um fecho algébrico de K. Como $\Delta \neq 0$ os vetores $v_0 = (1, 1, 1)$, $(v_1 = \alpha_0, \alpha_1, \alpha_2)$ e $v_2 = (\alpha_0^2, \alpha_1^2, \alpha_2^2)$ são linearmente independentes sobre $\overline{K}$. Conseqüentemente formam uma base de $\overline{K}^3$ sobre $\overline{K}$.

Logo $(\beta_0, \beta_1, \beta_2) = c_0v_0 + c_1v_1 + c_2v_2$, com $c_i \in \overline{K}$. Pela regra de Cramer vemos então que $c_i = \dfrac{\Delta_i}{\Delta} \in K$. Isto mostra em particular que $\beta = \beta_0 = c_0 + c_1\alpha + c_2\alpha^2 \in K(\alpha)$, ou seja, $F_k = F_l$. □

Consideremos agora os determinantes obtidos de Δ_2 por permutação circular de suas linhas

$$A_0 = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \end{vmatrix}, \qquad A_1 = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_2 & \beta_0 & \beta_1 \end{vmatrix} \qquad \text{e} \qquad A_2 = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 & \beta_0 \end{vmatrix}$$

Teorema 4.3. *$F_k = F_l$ se e somente se $A_i \in K$, para todo $0 \leq i \leq 2$.*

Demonstração. Começamos por observar que, pelo Teorema 2.4, podemos supor k e l não nulos. Conseqüentemente α e β são também geradores de base normal respectivamente de F_k e F_l sobre K.

Suponhamos que $F_k = F_l$. Desde que $\Delta \in K$ então Δ_0, Δ_1, $\Delta_2 \in K$ pelo Teorema

4.2. Conseqüentemente $A_0 = \Delta_2 \in K$. De

$$A_0 + A_1 + A_2 = \begin{vmatrix} 1 & 1 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 \\ -l & -l & -l \end{vmatrix} = 0$$

vemos que para obtermos o desejado é suficiente mostrarmos que $A_1 \in K$.

Como $\beta_2 \in K(\beta_0)$ existe um polinômio $g = c_0 + c_1X + c_2X^2 \in K[X]$ tal que $\beta_2 = g(\beta_0)$ e por conseqüência $\beta_0 = \sigma(g(\beta_0)) = g(\beta_1)$ e $\beta_1 = \sigma^2(g(\beta_0)) = g(\beta_2)$. Repetindo raciocínio semelhante ao usado na demonstração de (i)⇒(ii) do Teorema 4.2 obtemos $A_1 = c_1\Delta \in K$.

Reciprocamente é suficiente mostrarmos que Δ_0, $\Delta_1 \in K$, pois $\Delta \in K$ e $\Delta_2 = A_0$. O resultado então segue pelo Teorema 4.2.

Comecemos mostrando que $\Delta_1 \in K$. Desde que α gera uma base normal de F_k sobre K então

$$\alpha_1^2 = c_0\alpha_0 + c_1\alpha_1 + c_2\alpha_2, \quad \text{com} \quad c_i \in K, \quad 0 \leq i \leq 2.$$

Conseqüentemente

$$\alpha_2^2 = c_0\alpha_1 + c_1\alpha_2 + c_2\alpha_0, \qquad \alpha_0^2 = c_0\alpha_2 + c_1\alpha_0 + c_2\alpha_1$$

e

$$\Delta_1 = -(c_0A_0 + c_1A_1 + c_2A_2) \in K.$$

Resta mostrarmos que $\Delta_0 \in K$. Conforme já vimos na demonstração do Teorema 4.2, os vetores $v_0 = (1, 1, 1)$, $v_1 = (\alpha_0, \alpha_1, \alpha_2)$ e $v_2 = (\alpha_0^2, \alpha_1^2, \alpha_2^2)$ constituem uma base de $\overline{K}^3$ sobre $\overline{K}$. Então

$$(\beta_0, \beta_1, \beta_2) = b_0v_0 + b_1v_1 + b_2v_2, \quad \text{com} \quad b_0, b_1, b_2 \in \overline{K}.$$

Dessa igualdade obtemos

$$\beta_0 = b_0 + b_1\alpha_0 + b_2\alpha_0^2$$

$$\beta_1 = b_0 + b_1\alpha_1 + b_2\alpha_1^2$$

$$\beta_2 = b_0 + b_1\alpha_2 + b_2\alpha_2^2.$$

Usando novamente a regra de Cramer obtemos $b_1 = \dfrac{\Delta_1}{\Delta} \in K$ e $b_2 = \dfrac{\Delta_2}{\Delta} \in K$. Portanto $\beta_0 - \beta_1 = (b_1(\alpha_0 - \alpha_1) + b_2(\alpha_0^2 - \alpha_1^2)) \in F_k \bigcap F_l$ e então $F_k = F_l$ ou $F_k \bigcap F_l = K$. Se ocorrer a segunda alternativa teremos $\beta_0 - \beta_1 = \lambda$, para algum $\lambda \in K$ e conseqüentemente também $\beta_1 - \beta_2 = \sigma(\beta_0 - \beta_1) = \sigma(\lambda) = \lambda$. Isto implicará $\beta_0 - 2\beta_1 + \beta_2 = (\beta_0 - \beta_1) - (\beta_1 - \beta_2) = 0$, contrariando a independência linear dos $\beta_i,\ 0 \leq i \leq 2$. □

Referências Bibliográficas

[1] R. J. Chapman, *Automophism polynomials in cyclic cubic extensions*, J. Number Theory **61** (1996), 283-291.

[2] T. Cusick, *Finding fundamental units in cubic fields*, Math. Proc. Cambridge Philos. Soc. **92** (1982), 385-389.

[3] Ch. Dragos, *On normal polynomials and polynomials which generate the same extension*, J. Number Theory **34** (1990), 271-275.

[4] I. Kersten und J. Michaliček, *Kubische Galoiserweiterungen mit Normalbasis*, Comm. in Algebra **9** (1981), 1863-1871.

[5] I. Kersten und J. Michaliček, *Galoiserweiterungen der Ordnung p mit Normalbasis*, Comm. in Algebra **10** (1982), 695-718.

[6] I. Kersten and J. Michaliček, *A characterization of Galois fields extensions of degree 3*, Comm. in Algebra **15** (1987), 927-933.

[7] P. J. McCarthy, *Algebraic extensions of fields*, Dover Pub., Inc., 1966.

[8] P. Morton, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory **49** (1994), 183-208.

[9] A. Paques and A. Solecki, *A contribution to rational cubic extensions*, Comm. in Algebra **17** (1989), 1981-1987.

[10] J. Rotman, *Galois Theory*, Springer Verlag (1990).

[11] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137-1152.

[12] H. Wagner, *Charakterisierung von kubischen Galoiserweiterungen*, Regensburger Mathematische Schriften **16**, Universität Regensburg (1987), 75 pp.

Índice Alfabético