UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

INSTITUTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

O Problema Inverso de Galois: Casos Cúbico e Quíntico

Dissertação de Mestrado

Edite Taufer

Porto Alegre, 10 de Abril de 2008.

Dissertação submetida por Edite Taufer[1] como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Orientador:

Professor Dr. Antonio Paques

Banca Examinadora:

Professor Dr. Alveri Alves Sant'Ana (UFRGS)

Professor Dr. João Roberto Lazzarin (UFSM)

Professor Dr. Miguel Angel Alberto Ferrero (UFRGS)

Data Da Defesa: 10 de Abril de 2008.

[1]Parcialmente apoiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

"Milhares de velas podem ser acesas por uma única sem que essa seja enfraquecida.
Felicidade não diminui por ser compartilhada."
— SIDDHARTHA GAUTAMA (563 AC - 483 AC)

Agradecimentos

À minha família, pois sem a ajuda deles, decididamente, eu não teria chegado até aqui. Em especial aos meus pais Loide e Telvi e ao meu tio Selito.

Minha gratidão incondicional a um anjo, meu orientador Antonio Paques por ter me dado esta oportunidade, com dedicação e esmero.

À Neda Gonçalves e Vera Bauer, que fizeram parte do alicerce de minha vida acadêmica, por elas tenho profunda gratidão e admiração.

Ao Programa de Pós-Graduação em Matemática, em especial ao Jaime e Cydara Ripoll, juntamente com o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) que muito me ajudaram para a realização deste sonho!

Quero também expressar minha gratidão a secretária do Programa, Rosane Reginatto, por sua enorme atenção e eficiência, não esquecendo do chima!!!

Aos meus colegas e amigos da pós-graduação, quero agradecer a todos, de modo especial ao Danesi. Lembro-me de muitos momentos críticos de nos acharmos incapazes porém, a felicidade nos sorria quando percebíamos o quanto nos desenvolvíamos intelectual e profissionalmente...

Muito, muitão Obrigada!!!

Resumo

Neste trabalho apresentamos uma forma descritiva, explícita e eficaz de obter polinômios de grau 3 (resp. 5) que realizem o grupo cíclico de ordem 3 (resp. 5) como grupo de Galois, sobre um corpo de característica distinta de 3 (resp. 5) e sem raíz cúbica (resp. quíntica) primitiva da unidade.

Abstract

In this work we present a effective way to obtain polynomials of degree 3 (resp. 5) whose Galois group is cyclic of order 3 (resp. 5) over any field of characteristic different from 3 (resp. 5) and not containing primitive cubic (resp. quintic) root of unity.

Introdução

"Por volta dos anos 1830 Galois descreveu um procedimento para associar um grupo finito G a um polinômio

$$f(X) = X^n + a_1X^{n-1} + ... + a_{n-1}X + a_n,$$

onde a_1, a_2, ..., a_n são números racionais. Este grupo (o qual é chamado de ***grupo de Galois*** de $f(X)$) "mede" a dificuldade em encontrar as raízes desse polinômio; em particular, nos diz se $f(X)$ pode ou não ser resolvido por meio de radicais. Os contemporâneos de Galois não entenderam a importância de suas idéias. Seus artigos mais importantes não foram aceitos para publicação e mais tarde foram perdidos pela Academia Francesa de Ciências. O próprio Galois foi morto em um duelo antes mesmo de atingir a idade de 21 anos.

A construção de Galois leva naturalmente a seguinte questão: ***Todo grupo finito pode ser realizado como o grupo de Galois de algum polinômio com coeficientes racionais?***

Embora não exista evidência de que o próprio Galois tenha posto esta questão, sentimo-nos a vontade para especular que ele bem poderia tê-lo feito em algum de seus artigos perdidos.

De qualquer forma, esta questão, que hoje é conhecida como o ***Problema Inverso de Galois***, tem se transformado em um dos mais famosos problemas não resolvidos em Matemática e é o foco de muitos pesquisadores ao longo dos últimos 150 anos. Entre os resultados de maior destaque dessa pesquisa estão as soluções positivas para grupos solúveis (Shafarevich, 1954) e para o grupo simples conhecido como "o monstro" (Thompson, 1984).

O interesse por este problema tem aumentado nestas duas últimas décadas,

como bem atesta a publicação de um razoável número de livros e atas de eventos científicos, tais como *Galois group over* $\mathbb{Q}$ editado por Y. Ihara, K. Ribet e J.P.Serre (1987); *Topics in Galois Theory* por J.P.Serre (1992); *Recent Developments in the Inverse Galois Problem* editado por M.D. Fried (1993); *Group as Galois group, an Introduction* por H.Völklein (1996); *Inverse Galois Theory* por G.Malle e B.H.Matzat (1999); e *Generic Polynomials. Construtive Aspects of the Inverse Galois Problem* por C.U.Jensen, A.Ledet e N.Yui (2002)".
(por Zinovy Reichstein)

O nosso objetivo neste trabalho é apresentar uma forma descritiva, explícita e eficaz de obter polinômios de grau 3 (resp. 5) que realizem o grupo cíclico de ordem 3 (resp. 5) como grupo de Galois, sobre um corpo de característica distinta de 3 (resp. 5) e sem raíz cúbica (resp. quíntica) primitiva da unidade.

O caso específico de corpos de característica distinta de um primo p e com raiz p-ésima primitiva da unidade (resp. de característica p) é tratado pela teoria clássica de Kummer (resp. Artin-Schreier-Witt) e pode ser encontrado em qualquer livro básico sobre teoria de corpos, algum deles mencionados na lista de referências bibliográficas deste texto.

Este trabalho está organizado da seguinte maneira.

O Capítulo 1 está dividido em três seções. Nas Seções 1.1 e 1.2 apresentamos, para conforto do leitor, uns poucos resultados básicos da teoria de corpos, alguns deles sem demonstração, que serão utilizados ao longo do texto. Na Seção 1.3 apresentamos uma teoria de Kummer sem raiz primitiva da unidade. Essa seção, inspirada em [2], apresenta uma maneira de como obter extensões cíclicas de grau primo p de um corpo de característica distinta de p e sem raiz p-ésima primitiva da unidade.

Nos Capítulos 2 e 3 especializamos os resultados da Seção 1.3 para extensões cúbicas e quínticas. Além de construir os polinômios que realizam essas extensões, fazemos uma detalhada discussão sobre a classificação dessas extensões em termos dos coeficientes desses polinômios. Em particular, os resultados do capítulo 2, embora apresentados de modo independente e com alguma originalidade, a maioria deles foi inspirada nos resultados dos artigos [1], [4], [5], [8] e [10].

Capítulo 1

Extensões Cíclicas de grau p

1.1 Resultados Básicos

Os resultados apresentados nesta seção são apenas alguns resultados básicos da teoria de corpos, que serão utilizados livremente ao longo de todo o texto. Para o conforto do leitor os listamos aqui, porém sem demonstração. As demonstrações desses resultados podem ser encontradas, por exemplo, em qualquer uma das seguintes referências [9], [11], [5], [7].

Sejam K e E corpos. Dizemos que E é uma *extensão* de K se existe um homomorfismo de corpos $\varphi : K \to E$. Claramente φ é um monomorfismo (pois $\varphi(1_K) = 1_E$) e é usual identificar K com sua imagem $\varphi(K) \subset E$. A dimensão de E sobre K, visto como espaço vetorial, chamamos de *grau* de E sobre K e denotemos por $[E : K](:= dim_K E)$. Dizemos que E é uma *extensão finita* de K se $[E : K]$ for finito.

Dados uma extensão E de K e $\alpha \in E$, dizemos que α é *algébrico* sobre K se α é raiz de algum polinômio não nulo com coeficientes em K e denotamos por $m_{\alpha,K}(X)$ o polinômio em $K[X]$ mônico de menor grau do qual α é raiz.

Dizemos que duas extensões E e F de um mesmo corpo K são *K-isomorfas* (e denotamos $E \simeq_K F$) se existe um K-isomorfismo $\varphi : E \to F$, isto é, φ é isomorfismo de corpos e $\varphi|_K = id_K$.

Proposição 1.1.
i) *Sejam F extensão de K e E extensão de F. Então E é extensão de K e* $[E : K] = [E : F][F : K]$.

ii) *Sejam E uma extensão de K e $\alpha \in E$ algébrico sobre K. Então $K(\alpha)$ é uma extensão finita de K, $[K(\alpha) : K] = gr(m_{\alpha,K}(X))$ e $K(\alpha) \simeq_K \frac{K[X]}{(m_{\alpha,K}(X))}$.*

Todo homomorfismo de corpos $\sigma : F \to F'$, induz um homomorfismo de anéis $\sigma^* : F[X] \to F'[X]$, dado por $\sigma^*(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \sigma(a_i) X^i$. Se em particular σ é um isomorfismo de corpos então, σ^* é um isomorfismo de anéis.

Proposição 1.2. *Sejam $\sigma : F \to F'$ isomorfismo de corpos, $\sigma^* : F[X] \to F'[X]$ o isomorfismo correspondente, $f(X) \in F[X]$ irredutível, $f^*(X) = \sigma^*(f(X)) \in F'[X]$, α raiz de f em alguma extensão de F e α^* raiz de f^* em alguma extensão de F'. Então, existe um único isomorfismo de corpos $\widetilde{\sigma} : F(\alpha) \to F'(\alpha^*)$ tal que, $\widetilde{\sigma}|_F = \sigma$ e $\widetilde{\sigma}(\alpha) = \alpha^*$.*

Sejam $\sigma_i : F \to F'$, $1 \leq i \leq n$, homomorfismos de corpos. Dizemos que $\sigma_1, ..., \sigma_n$ são linearmente independentes sobre F' se a expressão $\sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0$, para todo $x \in F$ e $\lambda_i \in F'$, implicar sempre $\lambda_i = 0$, para todo $1 \leq i \leq n$.

Lema 1.3. (*Dedekind*) *Sejam F e F' corpos. Então todo conjunto finito de homomorfismos distintos $\sigma_i : F \to F'$, $1 \leq i \leq n$, é linearmente independente sobre F'.*

Dado E uma extensão de K denotamos $Aut_K(E)$ o grupo dos K-automorfismos de E, isto é, o grupo dos automorfismos σ de E tais que $\sigma|_K = id_K$. Dado $S \subset Aut_K(E)$ um subconjunto não vazio, denotamos $E^S = \{x \in E \mid \sigma(x) = x, \sigma \in S\}$.

Teorema 1.4. *Sejam E uma extensão finita de K e $S \subset Aut_K(E)$ um subconjunto finito não vazio. Então E^S é subcorpo de E e $[E : E^S] \geq |S|$. Em particular se S é subgrupo então $[E : E^S] = |S|$.*

Um polinômio $f(X) \in K[X]$ é chamado *separável* se cada fator irredutível de $f(X)$ não possui raízes múltiplas. Dizemos que $\alpha \in E$ é *separável* sobre K, se α é algébrico e $m_{\alpha,K}(X)$ é separável. Um *corpo de raízes* de um polinômio

não nulo $f(X) \in K[X]$ é uma extensão finita E de K de menor grau tal que $f(X)$ se decompõe em fatores lineares em $E[X]$.

Teorema 1.5. *Sejam E uma extensão finita de K e $G \subset Aut_K(E)$, um subgrupo finito. As seguintes afirmações são equivalentes:*
i) $E^G = K$.
ii) $[E : K] = |G|$ e $G = Aut_K(E)$.
iii) *E é um corpo de raízes de algum polinômio separável $f(X) \in K[X]$.*

Seja E uma extensão finita de K. Dizemos que E é *extensão galoisiana* de K se E satisfaz uma das condições equivalentes do Teorema 1.5. Além disso, se $G = Aut_K(E)$ é cíclico dizemos que E é *extensão cíclica* de K.

Teorema 1.6. (***Teorema Fundamental da Teoria de Galois***)
Sejam E uma extensão galoisiana de K e $G = Aut_K(E)$. Então,
i) *existe uma correspondência bijetiva (que inverte inclusão) entre os subcorpos intermediários de E e os subgrupos de G, dada por $F \mapsto Aut_F(E)$ e $H \mapsto E^H$.*
ii) *para todo subgrupo H de G, E^H é extensão galoisiana de K se e somente se $H \lhd G$ e, neste caso, $Aut_K(E^H) \simeq \frac{G}{H}$.*

1.2 Extensões Cíclicas de grau p $\neq 2$
(com raiz primitiva da unidade)

Nesta seção K denotará um corpo de característica distinta de p, que contém uma raiz p-ésima primitiva da unidade, isto é, existe $\xi \in K$ tal que $\xi^p = 1$ e $\xi^i \neq 1$ para todo $1 \leq i \leq p-1$.

Teorema 1.7. *Seja E uma extensão de grau p de K. Então, E é extensão cíclica se e somente se existe $\alpha \in E$ tal que $E = K(\alpha) \simeq_K \frac{K[X]}{(X^p - a)}$, para algum $a \in K \backslash K^p$.*

Demonstração

($\Leftarrow$) Suponhamos $E = K(\alpha) \simeq_K \frac{K[X]}{(X^p-a)}$. Logo $m_{\alpha,K}(X) = X^p - a$ e $\alpha, \alpha\xi, ..., \alpha\xi^{p-1}$

são todas as raízes distintas de $X^p - a$ em E. Isto é,

$$m_{\alpha,K}(X) = X^p - a = \prod_{i=0}^{p-1}(X - \xi^i\alpha).$$

Então, E é o corpo de raízes de $X^p - a$ sobre K e $X^p - a$ é separável. Portanto E é uma extensão galoisiana de K, pelo Teorema 1.5.iii. Pela Proposição 1.2 existe $\sigma \in Aut_K(E)$ tal que $\sigma(\alpha) = \xi\alpha$. É imediato ver que σ tem ordem p. Por outro lado, pelo Teorema 1.5.ii $|Aut_K(E)| = [E : K] = p$. Logo $Aut_K(E) = \langle\sigma\rangle$, ou seja, E é extensão cíclica de K.

($\Rightarrow$) Por hipótese existe $\sigma \in Aut_K(E)$ tal que $Aut_K(E) = \langle\sigma\rangle$. Note que, a ordem de σ é p e pelo Lema 1.3,

$$\sigma^0 + \xi^{p-1}\sigma + \xi^{p-2}\sigma^2 + ... + \xi\sigma^{p-1} \neq 0.$$

Isto nos diz que existe $c \in E$ tal que

$$\alpha = c + \xi^{p-1}\sigma(c) + \xi^{p-2}\sigma^2(c) + ... + \xi\sigma^{p-1}(c) \neq 0$$

Logo,

$$\sigma(\alpha) = \sigma(c) + \xi^{p-1}\sigma^2(c) + \xi^{p-2}\sigma^3(c) + ... + \xi\sigma^p(c) = \xi\alpha,$$

o que implica $\sigma^i(\alpha) = \xi^i\alpha$, para todo $0 \leq i \leq p-1$. Por conseguinte $\sigma(\alpha^p) = \sigma(\alpha)^p = (\xi^i\alpha)^p = \alpha^p$, donde segue que $\alpha^p \in E^{\langle\sigma\rangle} = K$. Seja $a \in K$ tal que $\alpha^p = a$. Então, $m_{\alpha,K}(X)$ divide $X^p - a$. Mas note que,

$$X^p - a = \prod_{i=0}^{p-1}(X - \xi^i\alpha) = \prod_{i=0}^{p-1}(X - \sigma^i(\alpha))$$

e $m_{\alpha,K}(\sigma^i(\alpha)) = \sigma^i(m_{\alpha,K}(\alpha)) = \sigma^i(0) = 0$, para todo $0 \leq i \leq p-1$. Logo, $m_{\alpha,K}(X) = X^p - a$. Portanto, $a \notin K^p$ e pela Proposição 1.1.ii $[K(\alpha) : K] = p = [E : K]$ e, $E = K(\alpha) \simeq_K \frac{K[X]}{(X^p-a)}$. □

O teorema seguinte nos dá condições necessárias e suficientes para decidirmos quando duas extensões cíclicas de K de grau p são K-isomorfas.

Teorema 1.8. *Sejam* $a, b \in K \setminus K^p$, $L_a = \frac{K[X]}{(X^p-a)}$ *e* $L_b = \frac{K[X]}{(X^p-b)}$. *Então,* $L_a \simeq_K L_b$ *se e somente se existe* $\lambda \in K\backslash 0$ *e* $1 \leq l \leq p-1$ *tais que* $b = \lambda^p a^l$.

Demonstração

Sejam $L_a = K(\alpha)$ e $L_b = K(\beta)$, com $\alpha = X + (X^p - a)$ e $\beta = X + (X^p - b)$. ($\Rightarrow$) Sejam $\varphi : L_a \to L_b$ um K-isomorfismo e $\varphi(\alpha) = \gamma \in L_b$. Temos que $\{1, \alpha, ..., \alpha^{p-1}\}$ é base de L_a sobre K então $\{1, \gamma, ..., \gamma^{p-1}\}$ é base de L_b sobre K, e portanto existem únicos $\lambda_i \in K$, $0 \leq i \leq p-1$, tais que

$$\beta = \lambda_0 + \lambda_1\gamma + ... + \lambda_{p-1}\gamma^{p-1} \in L_b.$$

Note que $Aut_K(L_b)$ é cíclico. Seja σ o gerador desse grupo dado por $\sigma(\beta) = \xi\beta$. Como α é raiz de $X^p - a$ temos,

$$a = \varphi(a) = \varphi(\alpha^p) = \varphi(\alpha)^p = \gamma^p.$$

Logo,

$$\gamma^p = a = \sigma(a) = \sigma(\gamma)^p$$

e, por conseguinte $\left(\frac{\sigma(\gamma)}{\gamma}\right)^p = 1$ de onde segue que $\sigma(\gamma) = \xi^i\gamma$, para algum $0 < i \leq p-1$.

Então,

$$\begin{aligned} \xi\beta &= \sigma(\beta) = \sigma(\lambda_0 + \lambda_1\gamma + \lambda_2\gamma^2 + ... + \lambda_{p-1}\gamma^{p-1}) \\ &= \lambda_0 + \lambda_1\sigma(\gamma) + \lambda_2\sigma(\gamma)^2 + ... + \lambda_{p-1}\sigma(\gamma)^{p-1} \\ &= \lambda_0 + \lambda_1\xi^i\gamma + \lambda_2\xi^{2i}\gamma^2 + ... + \lambda_{p-1}\xi^{(p-1)i}\gamma^{p-1}. \end{aligned} \tag{1.1}$$

Por outro lado,

$$\xi\beta = \xi\lambda_0 + \xi\lambda_1\gamma + \xi\lambda_2\gamma^2 + ... + \xi\lambda_{p-1}\gamma^{p-1}. \tag{1.2}$$

Igualando (1.1) e (1.2) obtemos $\lambda_l(\xi^{li} - \xi) = 0$ para todo $0 \leq l \leq p-1$. Disto decorre que $\lambda_l = 0$ para todo l tal que $li \not\equiv 1$ (mod p), ou seja, $\beta = \lambda\gamma^l$, com $\lambda \in K\backslash 0$ e $li \equiv 1(mod\ p)$. Portanto, $b = \beta^p = \lambda^p\gamma^{lp} = \lambda^p a^l$ com $1 \leq l \leq p-1$.

($\Leftarrow$) Por hipótese temos $b = \lambda^p a^l$, para algum $1 \leq l \leq p-1$ e $\lambda \in K\backslash 0$. Definamos,

$$\varphi : K[X] \xrightarrow{\sim} K[X] \xrightarrow{\pi} \frac{K[X]}{(X^p - b)}$$

$$h(X) \mapsto h(\lambda^{-1}X) \mapsto \overline{h(\lambda^{-1}X)}.$$

Naturalmente vê-se que φ está bem definida e é um homomorfismo de anéis sobrejetivo tal que $\varphi|_K = id_K$.

Decorre da Proposição 1.1.i que $K(\alpha) = K(\alpha^l)$. Além disso,

$$X^p - a^l = m_{\alpha^l,K}(X) \text{ e}$$

$$\varphi(X^p - a^l) = \overline{(\lambda^{-1}X)^p - a^l} = (\overline{\lambda^{-p}})(\overline{X^p - \lambda^p a^l}) = (\overline{\lambda^{-p}})(\overline{X^p - b}) = \overline{0}.$$

Consequentemente, $Ker(\varphi) = (X^p - a^l)$ e temos

$$L_a = K(\alpha) = K(\alpha^l) \simeq_K \frac{K[X]}{(X^p - a^l)} \simeq_K \frac{K[X]}{(X^p - b)} = L_b. \qquad \square$$

1.3 Extensões Cíclicas de grau p $\neq 2$

(sem raiz primitiva da unidade)

Nesta seção K denotará um corpo de característica distinta de p, que não contém raiz p-ésima primitiva da unidade. Em tudo que se seguirá $\widetilde{K}$ denotará um fecho algébrico de K, com $\xi \in \widetilde{K}$ uma raiz p-ésima primitiva da unidade, $K' = K(\xi)$ e $m = [K' : K] = gr(m_{\xi,K}(X))$. Claramente $m_{\xi,K}(X)$ é um fator do polinômio

$$\Phi_p(X) = X^{p-1} + X^{p-2} + ... + X + 1 = \prod_{i=1}^{p-1}(X - \xi^i),$$

donde segue que $m_{\xi,K}(X)$ é separável sobre K e K' é corpo de raízes de $m_{\xi,K}(X)$. Portanto K' é uma extensão galoisiana de K, pelo Teorema 1.5.iii. Além disso, para todo $\rho \in Aut_K(K')$ existe $1 \leq t(\rho) \leq p-1$ único tal que $\rho(\xi) = \xi^{t(\rho)}$. Isto define uma aplicação $\theta : Aut_K(K') \to \mathbb{Z}_p\backslash 0$, dada por $\rho \mapsto t(\rho)$, a qual é claramente um homomorfismo injetor de grupos. Desta forma temos que $Aut_K(K')$ é isomorfo a um subgrupo do grupo $\mathbb{Z}_p\backslash 0$. Considerando que $\mathbb{Z}_p\backslash 0$, como grupo multiplicativo do corpo finito $\mathbb{Z}_p$, é cíclico, segue que $Aut_K(K')$ é também cíclico. Além disso, $m = |Aut_K(K')|$ é um fator de $p-1$.

Teorema 1.9.

i) *Toda extensão F de K, cíclica de grau p, está contida em uma extensão F' de K, cíclica de grau mp, que contém K'.*

ii) *Toda extensão F' de K, cíclica de grau mp, que contém K', contém uma extensão (única) F de K, cíclica de grau p.*

Demonstração

i) Podemos assumir que $F \subset \tilde{K}$. Seja F' a menor extensão de K em $\tilde{K}$ que contém K' e F. Claramente $F' = F(\xi)$, desde que $m_{\xi,F}(X) = m_{\xi,K}(X)$ pois, $mdc([F : K], gr(m_{\xi,K}(X)) = 1$, e temos pela Proposição 1.1.i

$$[F' : K] = [F' : F][F : K] = mp.$$

Seja $G = Aut_K(F')$ então $K \subset F'^G$ e segue do Teorema 1.4 e Proposição 1.1.i que $[F' : K] = [F' : F'^G][F'^G : K] = |G|[F'^G : K] \geq |G|$.

Mostraremos a seguir que $[F' : K]$ é exatamente igual a $|G|$ e que G é cíclico. Para tanto é suficiente mostrar que G possui um elemento cuja ordem é mp. Sejam $\sigma \in Aut_K(F)$ e $\tau \in Aut_K(K')$ geradores desses respectivos grupos. Pela Proposição 1.2 existe $\rho \in Aut_K(F')$ tal que $\rho|_F = \sigma$ e $\rho(\xi) = \tau(\xi)$. Então $\rho^p|_F = id_F$ e, se $\tau(\xi) = \xi^t$ para algum $1 < t \leq p-1$, $\rho^p(\xi) = \tau^p(\xi) = \xi^{t^p} = \xi^t = \tau(\xi)$ (pois $t^p \equiv t$ (mod p)), ou seja, $\rho^p|_{K'} = \tau$. Consequentemente $\rho^{mp}|_{K'} = \tau^m = id_{K'}$ e $\rho^{mp}|_F = \sigma^{mp} = id_F$. Logo, $\rho^{mp} = id_K$ e portanto $n = o(\rho)$ divide mp.

Por outro lado, $\rho^n = id_K$ implica $\sigma^n = id_F$ e $\tau^n = id_{K'}$, donde segue que $m = o(\tau)$ e $p = o(\sigma)$ dividem n. Desde que m e p são co-primos (pois $1 < m \leq p-1$) então mp também divide n e portanto $o(\rho) = n = mp$, o que conclui a demonstração de i).

ii) Por hipótese $G = Aut_K(F')$ é cíclico de ordem mp e portanto possui um único subgrupo H de ordem m. Pelo Teorema 1.6.ii F'^H é extensão galoisiana de K e $[F'^H : K] = \left|\frac{G}{H}\right| = p$. Logo, basta tomar $F = F'^H$. □

O teorema que segue caracteriza todas as extensões cíclicas de K de grau mp que contêm K'. Para tanto faremos uso da aplicação multiplicativa $\eta : K' \to K'$ dada por $\eta(x) = \prod_{l=0}^{m-1} \tau^l(x^{t^{m-l}})$, $x \in K'$, com $1 \leq t \leq p-1$ tal que $\tau(\xi) = \xi^t$. Essa aplicação é conhecida na literatura como *norma de Stickelberger.*

Teorema 1.10. *Sejam F' uma extensão de K contendo K' de grau mp e τ um gerador de $Aut_K(K')$ com $\tau(\xi) = \xi^t$. Então, as seguintes afirmações são equivalentes:*

i) *F' é extensão cíclica de K.*

ii) *Existem $\alpha \in F'$, $a \in K' \setminus (K')^p$ e $\lambda \in K'^*$ tais que $\alpha^p = a$ e $\tau(a) = \lambda^p a^t$.*

iii) *Existem $\beta \in F'$ e $b, c \in K' \setminus (K')^p$ tais que $F' = K'(\beta)$, $\beta^p = b$ e $b = \eta(c)$.*

Demonstração

i)⇒ii) Por hipótese $G = Aut_K F'$ é cíclico de ordem mp. Em particular existem $\sigma, \rho \in G$ tais que $o(\sigma) = p$, $o(\rho) = m$ e $G = \langle \sigma\rho \rangle$. Pelos Teoremas 1.4, 1.5 e 1.6 temos $|Aut_{K'}(F')| = [F' : K'] = p = |\langle \sigma \rangle|$. Consequentemente, $Aut_{K'}(F') = \langle \sigma \rangle$ pois G, sendo cíclico, possui um único subgrupo de ordem p. Logo, F' é uma extensão cíclica de $K' = F'^{\langle \sigma \rangle}$ e pelo Teorema 1.7 existem $\alpha \in F'$ e $a \in K' \setminus K'^p$ tais que $F' = K'(\alpha)$, $\alpha^p = a$ e $\sigma(\alpha) = \xi\alpha$.

Por outro lado, $\{\rho^i \mid 0 \leq i \leq m-1\}$ é um sistema de representantes das classes laterais de $\langle \sigma \rangle$ em G. Então, também pelo Teorema 1.6.ii segue que $Aut_K(K') = \langle \rho|_{K'} \rangle$ e portanto existe $1 \leq l \leq m-1$ tal que $\rho^l|_{K'} = \tau$. Como $o(\tau) = m$ necessariamente também temos $o(\rho^l) = m$. Substituindo ρ por ρ^l se necessário, podemos assumir que $\rho|_{K'} = \tau$.

Finalmente se $\rho(\alpha) = \sum_{i=0}^{p-1} \lambda_i \alpha^i$, com $\lambda_i \in K'$ então,

$$\sigma\rho(\alpha) = \sum_{i=0}^{p-1} \lambda_i \sigma(\alpha)^i = \sum_{i=0}^{p-1} \lambda_i \xi^i \alpha^i$$

e, desde que $\sigma\rho = \rho\sigma$,

$$\sigma\rho(\alpha) = \rho(\sigma(\alpha)) = \rho(\xi\alpha) = \tau(\xi)\rho(\alpha) = \xi^t \rho(\alpha) = \sum_{i=0}^{p-1} \lambda_i \xi^t \alpha^i.$$

Decorre que $\lambda_i = 0$ para todo $i \neq t$ e $\rho(\alpha) = \lambda_t \alpha^t$. Portanto $\tau(a) = \rho(a) = \rho(\alpha)^p = (\lambda_t \alpha^t)^p = \lambda_t^p a^t$.

ii)⇒ iii) Por hipótese $\tau(a) = \lambda^p a^t$. Recursivamente obtemos $\tau^l(a) = \lambda_l^p a^{t^l}$, com $\lambda_l = \prod_{i=0}^{l-1} \tau^i \left(\lambda^{t^{l-(i+1)}} \right)$, para todo $1 \leq l \leq m-1$.

Recordemos que m é um fator de $p-1$ e seja $r=\frac{p-1}{m}$. Também observemos que $\xi^{t^m}=\tau^m(\xi)=\xi$ e portanto existe $k\in\mathbb{Z}$ tal que $t^m=1+kp$.

Então,

$$\begin{aligned}\eta(a^r) &= \prod_{l=0}^{m-1}\tau^l\left(a^{t^{m-l}}\right)^r = a^{rt^m}\prod_{l=1}^{m-1}\tau^l\left(a^{t^{m-l}}\right)^r \\ &= a^{rt^m}\left(\prod_{l=1}^{m-1}\lambda_l^{pt^{m-l}}a^{t^m}\right)^r = a^{rt^m}\left(\prod_{l=1}^{m-1}\lambda_l^{rpt^{m-l}}\right)a^{r(m-1)t^m} \\ &= \left(\prod_{l=1}^{m-1}\lambda_l^{rt^{m-l}}\right)^p a^{rmt^m} = \left(a^{k(p-1)}\prod_{l=1}^{m-1}\lambda_l^{rt^{m-l}}\right)^p a^{p-1} = c_0^p a^{p-1},\end{aligned}$$

com $c_0 = a^{k(p-1)}\prod_{l=1}^{m-1}\lambda_l^{rt^{m-l}}$.

Portanto, para $\beta=\frac{\alpha}{ac_0}$ temos $F'=K'(\beta)$ e

$$\beta^p=(ac_0)^{-p}a=(c_0^pa^{p-1})^{-1}=\eta(a^r)^{-1}=\eta(a^{-r}).$$

Logo basta tomar $c=a^{-r}$ e $b=\eta(c)$ para obtermos o resultado desejado.

iii)⇒i) Segue do Teorema 1.7 que $Aut_{K'}(F')$ é cíclico de ordem p gerado por σ tal que $\sigma(\beta)=\xi\beta$. Em particular $\sigma\in Aut_K(F')$. Logo, para obtermos o nosso resultado, é suficiente determinar $\rho\in Aut_K(F')$ tal que $o(\rho)=[K':K]=m$ e $\sigma\rho=\rho\sigma$. Iremos obter ρ como uma extensão de τ a F'. Para tanto necessitamos de alguma preparação. Notemos que

$$\begin{aligned}\tau(b) &= \tau(\eta(c))=\tau\left(\prod_{l=0}^{m-1}\tau^l(c^{t^{m-l}})\right) \\ &= \tau\left(c^{t^m}\tau(c^{t^{m-1}})\ldots\tau^{m-2}(c^{t^2})\tau^{m-1}(c^t)\right) \\ &= \tau(c^{t^m})\tau^2(c^{t^{m-1}})\ldots\tau^{m-1}(c^{t^2})c^t \\ &= \frac{\tau(c^{t^m})\tau^2(c^{t^{m-1}})\ldots\tau^{m-1}(c^{t^2})c^{t^{m+1}}}{c^{t(t^m-1)}} \\ &= c^{t(1-t^m)}\left(c^{t^m}\tau(c^{t^{m-1}})\tau^2(c^{t^{m-2}})\ldots\tau^{m-1}(c^t)\right)^t \\ &= c^{-tkp}b^t=d^pb^t\end{aligned}$$

com $d = c^{-tk}$.

Seja $\beta_1 = d\beta^t$. Segue da Proposição 1.1.i que $F' = K'(\beta_1)$ e de

$$\beta_1^p = d^p \beta^{pt} = d^p b^t = \tau(b)$$

segue que, $m_{\beta_1,K'}(X) = X^p - \tau(b) = \tau^*(m_{\beta,K'}(X))$.

Logo, pela Proposição 1.2 existe um único isomorfismo $\rho : F' \to F'$ tal que $\rho|_{K'} = \tau$ e $\rho(\beta) = \beta_1$. Disto decorre que $\rho \in Aut_K(F')$ e $o(\rho) \geq o(\tau) = m$. Por um cálculo recursivo obtemos

$$\begin{aligned} \rho^m(\beta) &= \tau^{m-1}(d)\tau^{m-2}(d^t)\tau^{m-3}(d^{t^2})...\tau(d^{t^{m-2}})d^{t^{m-1}}\beta^{t^m} \\ &= \tau^{m-1}(c^{-tk})\tau^{m-2}(c^{-t^2k})\tau^{m-3}(c^{-t^3k})...\tau(c^{-t^{m-1}k})c^{-t^mk}\beta^{t^m} \\ &= \eta(c)^{-k}\beta^{1+kp} = b^{-k}b^k\beta = \beta. \end{aligned}$$

como $\rho^m(x) = \tau^m(x) = x$, para todo $x \in K'$, segue que $o(\rho) = m$.

Finalmente, $\rho\sigma|_{K'} = \rho|_{K'} = \tau = \sigma\rho|_{K'}$ e

$$\rho\sigma(\beta) = \rho(\xi\beta) = \tau(\xi)\rho(\beta) = \tau(\xi)d\beta^t = d(\xi\beta)^t = \sigma(d\beta^t) = \sigma\rho(\beta)$$

Portanto $\sigma\rho = \rho\sigma$, o que conclui a demonstração. □

Capítulo 2

Extensões Cúbicas Cíclicas

Neste capítulo K denotará um corpo de característica distinta de 3, que não possui raiz cúbica primitiva da unidade.

No que se seguirá $K' = K(\xi)$, onde ξ é uma raiz cúbica primitiva da unidade em algum fecho algébrico de K. Claramente $m_{\xi,K}(X) = X^2 + X + 1$ e $Aut_K(K')$ é um grupo cíclico de ordem 2, com gerador τ dado por $\tau(\xi) = \xi^2$.

2.1 Caracterização 1

Nesta seção apresentamos uma caracterização de extensão cúbica cíclica de K como subextensão (única) de uma determinada extensão cíclica de grau 6 de K. Isto está descrito no teorema seguinte, o qual nada mais é do que uma versão dos teoremas 1.9 e 1.10 (ver capítulo anterior) aplicada ao caso $p = 3$.

Teorema 2.1.

i) *Toda extensão cúbica cíclica de K é univocamente determinada como subextensão de uma extensão cíclica de grau 6 de K, que contém K'.*

ii) *Seja $F' \supset K'$ uma extensão de K de grau 6. Então, F' é cíclica se e somente se existem $\delta \in K'$ e $\beta \in F'$ tais que $F' = K'(\beta)$ e $\beta^3 = \delta^2\tau(\delta) \notin K'^3$.*

Demonstração

i) Decorre imediatamente do Teorema 1.9.

ii) Pelo Teorema 1.10, F' é cíclica se e somente se existem $\delta \in K'$ e $\beta \in F'$ tais que $F' = K'(\beta)$ e $\beta^3 = \delta^4\tau(\delta^2) \notin K'^3$. Mas note que se $\beta_1 = (\delta^2\tau(\delta))^{-1}\beta^2$ então $F' = K'(\beta_1)$, $\beta_1^3 \notin K'^3$ e $\beta_1^3 = (\delta^2\tau(\delta))^{-3}\beta^6 = (\delta^2\tau(\delta))^{-3}(\delta^4\tau(\delta^2))^2 = \delta^2\tau(\delta)$. Reciprocamente, se $F' = K'(\beta)$, com $\beta^3 = \delta^2\tau(\delta) \notin K'^3$ então para $\beta_1 = \beta^2$ temos $F' = K'(\beta_1)$, $\beta_1^3 \notin K'^3$ e $\beta_1^3 = \delta^4\tau(\delta^2)$. □

O método para determinar a única extensão cúbica cíclica de K contida em F' está totalmente descrito nas demonstrações dos teoremas 1.9 e 1.10.

E, para completar, o lema seguinte nos dá uma forma de obter $\delta \in K'$ tal que $\delta^2\tau(\delta) \notin K'^3$.

Por conveniência de notação assumiremos doravante em todo este capítulo que $E^* = E\backslash 0$, para qualquer extensão E de K.

Observemos também que para todo $x \in K'$ temos $x+\tau(x) \in K$ e $x\tau(x) \in K$. Isto define duas aplicações $T : K' \to K$ e $N : K' \to K$ dadas por $T(x) = x+\tau(x)$ e $N(x) = x\tau(x)$, para todo $x \in K'$ chamadas respectivamente *traço* e *norma* de K' sobre K. É imediato verificar que T é K-linear e N é multiplicativa.

Lema 2.2. *Seja $\delta \in K'$. Então $\delta^2\tau(\delta) \in (K'^*)^3 \Leftrightarrow \delta \in K^*(K'^*)^3$.*

Demonstração

Note que $\delta^2\tau(\delta) = \delta N(\delta)$. Logo, se $\delta^2\tau(\delta) = u^3$ para algum $u \in K'^*$ então $\delta = N(\delta)^{-1}u^3 \in K^*(K'^*)^3$.

Reciprocamente se $\delta = vu^3$, com $v \in K^*$ e $u \in K'^*$ então

$$\begin{aligned}\delta^2\tau(\delta) &= (vu^3)^2\tau(vu^3)\\ &= (v^2u^6)v\tau(u)^3\\ &= v^3(u^2\tau(u))^3 \in (K'^*)^3.\end{aligned}$$

□

2.2 Polinômio Gerador

Dado $\delta \in K'$ tal que $\delta^2\tau(\delta) \notin K'^3$ denotemos $F'_\delta = K'(\beta)$, com $\beta^3 = \delta^2\tau(\delta)$ e F_δ a única extensão cúbica cíclica de K contida em F'_δ. Naturalmente pela Proposição 1.1.i temos $F_\delta = K(x)$ para qualquer $x \in F_\delta \backslash K$. Nesta seção vamos escolher um específico x, construído a partir de β e determinar $m_{x,K}(X)$, bem como o gerador σ do grupo cíclico $Aut_K(F_\delta)$. Veremos isso no próximo teorema.

Teorema 2.3. *Seja $\delta = a + b\xi^2 \in K'$ tal que $\delta^2\tau(\delta) \notin K'^3$. Então,*
i) *existe $x \in F_\delta$ tal que $F_\delta = K(x)$ e $m_{x,K}(X) = X^3 - 3N(\delta)X - N(\delta)T(\delta)$;*
ii) *$Aut_K(F_\delta) = \{id_{F_\delta}, \sigma, \sigma^2\}$ com*

$$\sigma(x) = \frac{1}{b}\left(x^2 - ax - 2N(\delta)\right) \quad e \quad \sigma^2(x) = -\frac{1}{b}\left(x^2 + (b-a)x - 2N(\delta)\right).$$

Demonstração

i) Segue da demonstração do Teorema 1.10 (iii $\Rightarrow$ i) e da demonstração do Teorema 2.1.ii que $Aut_K(F'_\delta)$ é gerado pelos K-automorfismos σ e ρ dados por $\sigma(\beta) = \xi\beta$, $\rho(\beta) = \delta^{-1}\beta^2$, $\sigma|_{K'} = id_{K'}$ e $\rho|_{K'} = \tau$. Além disso, conforme vimos na demonstração do Teorema 1.9.ii $F_\delta = F_\delta'^{\langle\rho\rangle}$. Notemos que $o(\rho) = o(\tau) = 2$. Portanto $x = T_\rho(\beta) = \beta + \rho(\beta) \in F_\delta$. Obviamente $x \notin K$ pois $\{1, \beta, \beta^2\}$ é um conjunto linearmente independente sobre $K' \supset K$. Portanto $F_\delta = K(x)$, pela Proposição 1.1.i. De

$$\begin{aligned}
x^3 &= (\beta + \rho(\beta))^3 \\
&= \beta^3 + \rho(\beta)^3 + 3\beta^2\rho(\beta) + 3\beta\rho(\beta)^2 \\
&= \beta^3 + \rho(\beta)^3 + 3\beta\rho(\beta)(\beta + \rho(\beta)) \\
&= (\beta^3 + \rho(\beta)^3) + 3\delta^{-1}\beta^3 x \\
&= 3\delta^{-1}\delta^2\tau(\delta)x + \delta^2\tau(\delta) + \tau(\delta^2)\delta \\
&= 3N(\delta)x + N(\delta)T(\delta)
\end{aligned}$$

vemos que $m_{x,K}(X) = X^3 - 3N(\delta)X - N(\delta)T(\delta)$.

ii) Decorre também do Teorema 1.6.ii que $Aut_K(F_\delta)$ é cíclico gerado por $\sigma|_{F_\delta}$.

Agora, notemos que

$$\begin{aligned}\sigma(x) &= \sigma(\beta+\rho(\beta)) = \sigma(\beta)+\sigma\rho(\beta) = \sigma(\beta)+\rho\sigma(\beta)\\ &= \xi\beta+\rho(\xi\beta) = \xi\beta+\xi^2\rho(\beta)\end{aligned}$$

e

$$\begin{aligned}x^2 &= (\beta+\rho(\beta))^2 = \beta^2+\rho(\beta)^2+2\beta\rho(\beta)\\ &= \delta\rho(\beta)+\tau(\delta)\beta+2\delta^{-1}\beta^3\\ &= \delta\rho(\beta)+\tau(\delta)\beta+2N(\delta)\\ &= (a+b\xi^2)\rho(\beta)+(a+b\xi)\beta+2N(\delta)\\ &= ax+b\sigma(x)+2N(\delta).\end{aligned}$$

Logo,

$$\sigma(x) = \frac{1}{b}\left(x^2-ax-2N(\delta)\right).$$

Desde que o termo em X^2 de $m_{x,K}(X)$ é nulo, segue que $x+\sigma(x)+\sigma^2(x)=0$ e portanto

$$\sigma^2(x) = -\frac{1}{b}\left(x^2+(b-a)x-2N(\delta)\right). \qquad \square$$

Conforme vimos, o Teorema 2.3 expressa $m_{x,K}(X)$ e $\sigma(x)$ em termos do traço e da norma do elemento $\delta = a+b\xi^2 \in K'$, satisfazendo $\delta^2\tau(\delta) \notin K'^3$. Aparentemente fica a impressão de que toda extensão cúbica cíclica de K depende dos dois parâmetros $a, b \in K$ escolhidos. Veremos na seqüência que podemos sempre escolher um novo $\delta_1 \in K'$, dependendo de um único parâmetro $c \in K$ e que determina a mesma extensão F_δ.

Notemos primeiramente que se $\delta_1 = \tau(\delta)$ e $\beta_1 = \rho(\beta)$ então $F'_\delta = K'(\beta_1)$ e $\beta_1^3 = \rho(\beta^3) = \rho(\delta^2\tau(\delta)) = \tau(\delta)^2\delta = \delta_1^2\tau(\delta_1)$. Isto nos diz então que é indiferente escolher $\delta = a+b\xi$ ou $a+b\xi^2$.

Seja então $\delta = a+b\xi$, com $a, b \in K$. A condição $\delta^2\tau(\delta) \notin K'^3$ exige necessariamente $b \neq 0$. Assim, $\delta = b(c+\xi)$, com $c = \frac{a}{b}$. Sejam $\delta_1 = c+\xi$ e $\beta_1 = b^{-1}\beta$. Então, $F'_\delta = K'(\beta_1)$ e $\beta_1^3 = b^{-3}\delta^2\tau(\delta) = b^{-3}(b\delta_1)^2\tau(b\delta_1) = \delta_1^2\tau(\delta_1)$, ou seja, $F'_\delta = F'_{\delta_1}$.

Corolário 2.4. *Seja $\delta = c + \xi \in K'$, com $c \in K$ tal que $c \neq \frac{s^3-3s+1}{3(s^2-s)}$, para todo $s \in K \setminus \{0,1\}$. Então,*

i) *existe $x \in F_\delta$ tal que $F_\delta = K(x)$ e*

$$m_{x,K}(X) = X^3 - 3(c^2 - c + 1)X - (2c - 1)(c^2 - c + 1).$$

ii) *$Aut_K(F_\delta) = \{id_{F_\delta}, \sigma, \sigma^2\}$ com $\sigma(x) = x^2 - cx - 2(c^2 - c + 1)$ e*

$$\sigma^2(x) = -x^2 + (c - 1)x - 2(c^2 - c + 1).$$

Demonstração

Começamos por observar que pelo Lema 2.2,

$$\delta^2\tau(\delta) \in (K'^*)^3 \Leftrightarrow \delta \in K^*(K'^*)^3 \Leftrightarrow \delta = ru^3,$$

com $r \in K^*$ e $u \in K'^*$. Logo $u \notin K$ (pois $\delta \notin K$) e podemos tomar $u = s + \xi$. Assim, de $\delta = ru^3$ segue que $c + \xi = r(s^3 - 3s + 1) + 3r(s^2 - s)\xi$, novamente porque $\delta \notin K$ temos também $s \neq 0, 1$. Por conseguinte resulta que $r = \frac{1}{3(s^2-s)}$ e $c = \frac{s^3-3s+1}{3(s^2-s)}$. Portanto,

$$\delta^2\tau(\delta) \notin K'^3 \Leftrightarrow c \neq \frac{s^3 - 3s + 1}{3(s^2 - s)},$$

para todo $s \in K \setminus \{0,1\}$. Finalmente, para obter i) e ii) basta observar que $T(\delta) = 2c - 1$ e $N(\delta) = c^2 - c + 1$. □

2.3 Caracterização 2

O teorema a seguir é uma conseqüência imediata do que vimos nas Seções 2.1 e 2.2.

Teorema 2.5. *Seja F uma extensão de K. Então F é extensão cúbica cíclica se e somente se $F \simeq_K \frac{K[X]}{(f_c(X))}$, com $f_c(X) = X^3 - 3(c^2 - c + 1)X - (2c - 1)(c^2 - c + 1)$ e $c \neq \frac{s^3-3s+1}{3(s^2-s)}$ para todo $s \in K \setminus \{0,1\}$.*

Demonstração

($\Rightarrow$) Segue do Corolário 2.4.i.

($\Leftarrow$) Começamos por afirmar que $F_c = \frac{K[X]}{(f_c(X))}$ é uma extensão de grau 3 de K, ou seja, que $f_c(X) = X^3 - 3(c^2-c+1)X - (2c-1)(c^2-c+1)$ é irredutível sobre K. De fato, se $f_c(X)$ é redutível sobre K então $f_c(t) = 0$ para algum $t \in K$. Logo, para $s = t + c$ temos $s^3 - 3cs^2 + 3(c-1)s + 1 = 0$ e disto segue que $3c(s^2 - s) = s^3 - 3s + 1$. Observemos que $s \neq 0, 1$, pois $-c$ e $1 - c$ não são raízes de $f_c(X)$. Portanto $c = \frac{s^3-3s+1}{3(s^2-s)}$, o que é absurdo.

Agora, dados $x_0 = x = X + (f_c(X))$, $x_1 = x^2 - cx - 2(c^2 - c + 1)$ e $x_2 = -x^2 + (c-1)x - 2(c^2 - c+1)$, é fácil ver que $f_c(X) = (X - x_0)(X - x_1)(X - x_2)$ e portanto $F_c = \frac{K[X]}{(f_c(X))} = K(x)$ é corpo de raízes de $f_c(X)$. Além disso as raízes x_0, x_1 e x_2 são distintas pois $\{1, x, x^2\}$ é uma base de F_c sobre K.

Portanto $f_c(X)$ é separável sobre K e F_c é extensão cúbica cíclica de K, pelo Teorema 1.5. □

O próximo teorema nos dá outra caracterização de uma extensão cúbica cíclica de K via um novo polinômio gerador, o qual é, a nosso ver, bem mais interessante que o dado no Teorema 2.5.

Teorema 2.6. *Seja F uma extensão de K. Então F é cúbica cíclica se e somente se $F \simeq_K \frac{K[X]}{(f_k(x))}$, com $f_k(X) = X^3 + kX^2 - (k+3)X + 1$ e $k \neq \frac{s^3-3s+1}{s-s^2}$, para todo $s \in K \setminus \{0, 1\}$.*

Demonstração

($\Rightarrow$) Pelo Corolário 2.4.i, existe $x \in F$ tal que $F = K(x)$ e $m_{x,K}(X) = X^3 - 3(c^2 - c + 1)X - (2c-1)(c^2 - c + 1)$. Seja $y = x + c$. Então, $F = K(y)$ e temos

$$\begin{aligned} 0 &= (y-c)^3 - 3(c^2 - c + 1)(y - c) - (2c - 1)(c^2 - c + 1) \\ &= y^3 - 3cy^2 + 3(c-1)y + 1. \end{aligned}$$

Portanto, $m_{y,K}(X) = X^3 + kX^2 - (k+3)X + 1 := f_k(X)$, com $k = -3c$ e o isomorfismo requerido segue pela Proposição 1.1.ii. Também pelo Corolário 2.4 temos $c \neq \frac{s^3-3s+1}{3(s^2-s)}$ ou $k \neq \frac{s^3-3s+1}{s-s^2}$, para todo $s \in K \setminus \{0, 1\}$.

($\Leftarrow$) Afirmamos que $f_k(X) = X^3 + kX^2 - (k+3)X + 1$ é irredutível sobre K pois, caso contrário, teríamos $f_k(s) = 0$ para algum $s \in K$ e por conseqüência

$k(s-s^2) = s^3 - 3s + 1$. Observando que 0 e 1 não são raízes de $f_k(X)$, teríamos então $k = \frac{s^3-3s+1}{s-s^2}$, o que é absurdo.

Sejam $F_k = \frac{K[X]}{(f_k(X))} = K(x)$, com $x = X + (f(X))$, $x_0 = x$, $x_1 = \frac{1}{1-x}$ e $x_2 = \frac{x-1}{x}$. Claramente x_0, x_1 e x_2 são distintos, pois $\{1, x, x^2\}$ é uma base de F_k sobre K. Além disso, de $x_0 + x_1 + x_2 = -k$, $x_0x_1 + x_0x_2 + x_1x_2 = -(k+3)$ e $x_0x_1x_2 = -1$ vemos que $f_k(X) = (X - x_0)(X - x_1)(X - x_2)$.

Portanto $f_k(X)$ é separável sobre K e F_k é corpo de raízes de $f_k(X)$. Logo F_k é extensão cúbica cíclica de K, pelo Teorema 1.5. □

2.4 A Classificação

Nesta seção nos dedicaremos a encontrar condições necessárias e suficientes para que duas extensões cúbicas cíclicas de K sejam K-isomorfas. Começamos com o seguinte lema

Lema 2.7. *Sejam $\delta_1, \delta_2 \in K'$ tais que $\delta_1^2\tau(\delta_1), \delta_2^2\tau(\delta_2) \notin K'^3$. Então,*

$$F_{\delta_1} \simeq_K F_{\delta_2} \Leftrightarrow \delta_2\delta_1^{-1} \in K^*(K'^*)^3 \text{ ou } \delta_2\tau(\delta_1^{-1}) \in K^*(K'^*)^3.$$

Demonstração

É imediato verificar que $F_{\delta_1} \simeq_K F_{\delta_2}$ se e somente se $F'_{\delta_1} \simeq_{K'} F'_{\delta_2}$. Pelo Teorema 1.8 este último isomorfismo ocorre se e somente se

$$(\delta_2\delta_1^{-1})^2\tau(\delta_2\delta_1^{-1}) \in (K'^*)^3 \text{ ou } (\delta_2\delta_1)^2\tau(\delta_2\delta_1) \in (\mathrm{K}'^*)^3,$$

o que é equivalente, pelo Lema 2.2, a $\delta_2\delta_1^{-1} \in K^*(K'^*)^3$ ou $\delta_2\delta_1 \in K^*(K'^*)^3$. Observando que $\delta_2\tau(\delta_1^{-1}) = N(\delta_1)^{-1}\delta_2\delta_1$ segue o resultado. □

Observação 2.8. Vimos na seção 2.1 que um elemento $\delta \in K'$ determina (univocamente) uma extensão cúbica cíclica F_δ de K se e somente se $\delta^2\tau(\delta) \notin K'^3$. Vimos também na demonstração do Corolário 2.4 que, para $\delta = c+\xi$, $\delta^2\tau(\delta) \notin K'^3$ se e somente se $c \neq \frac{s^3-3s+1}{3(s^2-s)}$, para todo $s \in K \setminus \{0, 1\}$. Claramente $\delta^2\tau(\delta) \notin K'^3$ se e somente se $\tau(\delta)^2\delta \notin K'^3$ e isto, conforme pode ser visto facilmente, usando o mesmo raciocínio acima mencionado, é equivalente a $c \neq \frac{s^3-3s^2+1}{3(s-s^2)}$, para todo

$s \in K \setminus \{0,1\}$. Portanto, para $\delta = c + \xi$ temos

$$c \neq \frac{s^3 - 3s + 1}{3(s^2 - s)} \Leftrightarrow \delta^2 \tau(\delta) \notin K'^3 \Leftrightarrow \tau(\delta)^2 \delta \notin K'^3 \Leftrightarrow c \neq \frac{s^3 - 3s^2 + 1}{3(s - s^2)},$$

para todo $s \in K \setminus \{0,1\}$.

Corolário 2.9. *Sejam $\delta_1 = c + \xi$ e $\delta_2 = d + \xi$ com $c, d \in K$ distintos e tais que $c, d \neq \frac{s^3-3s+1}{3(s^2-s)}$, para todo $s \in K \setminus \{0,1\}$. Então, $F_{\delta_1} \simeq_K F_{\delta_2}$ se e somente se existe $t \in K$ tal que*

$$d = \frac{(t^3 - 3t + 1)c - 3(t^2 - t)}{3(t^2 - t)c + (t^3 - 3t^2 + 1)}$$

ou

$$d = \frac{(t^3 - 3t + 1)c - (t^3 - 3t^2 + 1)}{3(t^2 - t)c - (t^3 - 3t + 1)}.$$

Demonstração

Por Lema 2.7 $F_{\delta_1} \simeq_K F_{\delta_2}$ se e somente se $\delta_2 \delta_1^{-1} \in K^*(K'^*)^3$ ou $\delta_2 \tau(\delta_1^{-1}) \in K^*(K'^*)^3$. Vejamos a primeira alternativa. Para a segunda procede-se de modo análogo.

Sejam $r \in K^*$ e $u \in K^*$ tais que $\delta_2 = ru^3\delta_1$. Notemos que $d \neq c$ e portanto necessariamente $u = t_0 + t_1\xi$, com $t_1 \neq 0$. Substituindo u por ut_1^{-1}, se necessário, podemos supor $u = t + \xi$, para algum $t \in K$. Agora, um simples cálculo nos dá o resultado desejado. □

Corolário 2.10. *Sejam $\delta_1 = c+\xi$ e $\delta_2 = d+\xi$, com $c, d \in K$ tais que $d \neq c$, $1-c$ e c, $d \neq \frac{s^3-3s+1}{3(s^2-s)}$, para todo $s \in K\setminus\{0,1\}$. Então, $F_{\delta_1} \simeq_K F_{\delta_2}$ se e somente se para $k = 3\left(\frac{cd-d+1}{d-c}\right)$ ou $k = 3\left(\frac{cd-1}{1-c-d}\right)$, o polinômio $f_k(X) = X^3 + kX^2 - (k+3)X + 1$ é redutível sobre K.*

Demonstração

Segue do Corolário 2.9 que $F_{\delta_1} \simeq_K F_{\delta_2}$ se, e somente se, existe $t \in K$ tal que

$$d = \frac{(t^3 - 3t + 1)c - 3(t^2 - t)}{3(t^2 - t)c + (t^3 - 3t^2 + 1)}$$

ou

$$d = \frac{(t^3 - 3t + 1)c - (t^3 - 3t^2 + 1)}{3(t^2 - t)c - (t^3 - 3t + 1)}.$$

Desenvolvendo a primeira igualdade (resp. a segunda) como uma polinomial em t obtemos $t^3 + kt^2 - (k+3)t + 1 = 0$ com $k = 3\left(\frac{cd-d+1}{d-c}\right)$ (resp. $k = 3\left(\frac{cd-1}{1-c-d}\right)$). □

Observação 2.11. A hipótese $d \neq c$, $1-c$ no Corolário 2.10 não é uma restrição pois para $d = c$ temos $\delta_1 = \delta_2$, para $d = 1 - c$ temos $\delta_2 = -\tau(\delta_1)$ e pode-se verificar facilmente que $F_{\delta_1} = F_{-\tau(\delta_1)}$.

Corolário 2.12. *Sejam* $k_i \in K$, $f_{k_i}(X) = X^3 + k_iX^2 - (k_i+3)X + 1$ *e* $F_{k_i} = \frac{K[X]}{(f_{k_i}(X))}$, $i = 1, 2$. *Assuma que* $k_2 \neq k_1$, $-(\frac{1}{3} + k_1)$ *e* $k_1, k_2 \neq \frac{s^3-3s+1}{s-s^2}$, *para todo* $s \in K \setminus \{0, 1\}$. *Então* $F_{k_1} \simeq_K F_{k_2}$ *se e somente se para* $k = \frac{9k_1k_2+3k_2+1}{k_1-k_2}$ *ou* $k = \frac{27k_1k_2-3}{1+3k_1+3k_2}$, *o polinômio* $f_k(X) = X^3 + kX^2 - (k+3)X + 1$ *é redutível sobre* K.

Demonstração

É suficiente observar que se $c_i = -3k_i$, $i = 1, 2$, então $c_2 \neq c_1$, $1 - c_1$ e $c_1, c_2 \neq \frac{s^3-3s+1}{3(s^2-s)}$ para todo $s \in K \setminus \{0, 1\}$,

$$3\frac{c_1c_2 - c_2 + 1}{c_2 - c_1} = \frac{9k_1k_2 + 3k_2 + 1}{k_1 - k_2}$$

e

$$3\frac{c_1c_2 - 1}{1 - c_1 - c_2} = \frac{27k_1k_2 - 3}{1 + 3k_1 + 3k_2}.$$

O resultado decorre então do Corolário 2.10. □

Observação 2.13. Na demonstração do Teorema 2.6 vimos que, para cada $k \in K$, o polinômio $f_k(X) = X^3 + kX^2 - (k+3)X + 1$ é irredutível sobre K se e somente se $k \neq \frac{s^3-3s+1}{s-s^2}$, para todo $s \in K \setminus \{0, 1\}$. Vimos também, no caso em que $f_k(X)$ é irredutível, $F_k = \frac{K[X]}{(f_k(X))}$ é uma extensão cúbica cíclica de K. Em toda esta parte da demonstração do Teorema 2.6 não foi utilizada a hipótese de a característica de K ser diferente de 3. De fato, é possível mostrar que toda extensão cúbica cíclica de K é do tipo F_k, independentemente de qualquer hipótese sobre a característica de K. Para a demonstração de tal fato utiliza-se de outras técnicas e procedimentos distintos daqueles utilizados aqui. Tais técnicas e procedimentos são oriundos do que hoje é conhecida na literatura

como a *teoria de Kummer sem raízes da unidade.* (ver, por exemplo, [4], [8] e [3]).

2.5 Exemplos

Para os exemplos utilizaremos as caracterizações de extensões cúbicas cíclicas dadas nos Teoremas 2.5, 2.6 e consideraremos K como sendo o corpo $\mathbb{Q}$ dos números racionais.

c	$f_c(X)$
-3	$X^3 - 39X + 91$
-2	$X^3 - 21X + 35$
-1	$X^3 - 9X + 9$
0	$X^3 - 3X + 1$
1	$X^3 - 3X - 1$
2	$X^3 - 9X - 9$
3	$X^3 - 21X - 35$

Pelo Lema 2.5 é suficiente afirmar que $c \neq \frac{s^3-3s+1}{3(s^2-s)}$, ou equivalentemente $s^3 - 3cs^2 + 3(c-1)s + 1 \neq 0$, para todo $s \in \mathbb{Q} \setminus \{0, 1\}$.

Mas isto é imediato pois o polinômio $f_c(X) = X^3 - 3cX^2 + 3(c-1)X + 1 \in \mathbb{Q}(X)$ é irredutível, para todo c listado na tabela acima.

k	$f_k(X)$
-3	$X^3 - 3X^2 + 1$
-2	$X^3 - 2X^2 - X + 1$
-1	$X^3 - X^2 - 2X + 1$
0	$X^3 - 3X + 1$
1	$X^3 + X^2 - 4X + 1$
2	$X^3 + 2X^2 - 5X + 1$
3	$X^3 + 3X^2 - 6X + 1$

Pelo Lema 2.6 é suficiente afirmar que $c \neq \frac{s^3-3s+1}{s-s^2}$, ou equivalentemente $s^3 + ks^2 - (k+3)s + 1 \neq 0$, para todo $s \in \mathbb{Q} \setminus \{0, 1\}$.

Mas isto é imediato pois o polinômio $f_k(X) = X^3+kX^2-(k+3)X+1 \in \mathbb{Q}(X)$ é irredutível, para todo k listado na tabela acima.

Capítulo 3

Extensões Quínticas Cíclicas

Neste capítulo K denotará um corpo de característica distinta de 5, que não possui raiz quíntica primitiva da unidade.

Também neste capítulo $K' = K(\xi)$, onde ξ é uma raiz quíntica primitiva da unidade em algum fecho algébrico de K. Conforme observado na seção 1.3, $m_{\xi,K}(X)$ é um fator do polinômio $\Phi_5(X) = X^4+X^3+X^2+X+1 = \prod_{i=1}^{4}(X-\xi^i)$, ou seja, $m_{\xi,K}(X) = (X-\xi)(X-\xi^4)$ ou $\Phi_5(X)$. No primeiro caso $\xi+\xi^4$, $\xi^2+\xi^3 \in K$ e $Aut_K(K')$ é um grupo cíclico de ordem 2, com gerador τ dado por $\tau(\xi) = \xi^4 = \xi^{-1}$. No segundo caso $Aut_K(K')$ é um grupo cíclico de ordem 4, com gerador τ dado por $\tau(\xi) = \xi^2$ ou ξ^3.

3.1 Caracterização 1

Analogamente ao que vimos na Seção 2.1, aqui também apresentamos uma caracterização de extensão quíntica cíclica como subextensão (única) de uma determinada extensão cíclica de grau 10 ou 20 de K, conforme $\xi+\xi^4 \in K$ ou $\xi+\xi^4 \notin K$. Esse resultado, descrito no próximo teorema é a versão dos Teoremas 1.9 e 1.10 no caso $p = 5$.

Teorema 3.1.

i) *Toda extensão quíntica cíclica de K é univocamente determinada como subextensão de uma extensão cíclica de K contendo K', de grau 10* (resp. 20) se $\xi + \xi^4 \in K$ (resp. $\xi + \xi^4 \notin K$).

ii) *Assuma que $\xi+\xi^4 \in K$ (resp. $\xi+\xi^4 \notin K$) e seja $F' \supset K'$ uma extensão de K de grau 10 (resp. 20). Então F' é cíclica se e somente se existem $\delta \in K'$ e $\beta \in F'$ tais que $F' = K'(\beta)$ e $\beta^5 = \delta^{-1}\tau(\delta) \notin K'^5$ (resp. $\beta^5 = (\delta\tau(\delta^3))^{-1}\tau^2(\delta\tau(\delta^3)) \notin K'^5$).*

Demonstração

i) Decorre imediatamente do Teorema 1.9.

ii) Pelo Teorema 1.10. F' é cíclica se e somente se existem $\delta \in K'$ e $\beta \in F'$ tais que $F' = K'(\beta)$ e $\beta^5 = \delta^{16}\tau(\delta^4)$ se $\xi + \xi^4 \in K$ ou $\beta^5 = \delta^{16}\tau(\delta^8)\tau^2(\delta^4)\tau^3(\delta^2)$ se $\xi + \xi^4 \notin K$.

Tomando $\beta_1 = \delta^3\tau(\delta)\beta^{-1}$ se $\xi + \xi^4 \in K$ ou $\beta_1 = \delta^3\tau(\delta)\tau^2(\delta)\tau^3(\delta)\beta^{-1}$ se $\xi + \xi^4 \notin K$ obtemos no primeiro caso $F' = K'(\beta_1)$ com $\beta_1^5 = \delta^{-1}\tau(\delta) \notin K'^5$ e no segundo caso $F' = K'(\beta_1)$ com $\beta_1^5 = \delta_1^{-1}\tau^2(\delta_1) \notin K'^5$, onde $\delta_1 = \delta\tau(\delta^3)$. A recíproca é imediata. □

A maneira de se obter a única extensão quíntica cíclica de K contida em F' está totalmente descrita nas demonstrações dos Teoremas 1.9 e 1.10.

O lema seguinte nos propicia uma forma de se obter $\delta \in K'$ que satisfaça as condições descritas no Teorema 3.1.ii.

Também em todo este capítulo $E^* := E \setminus 0$, para qualquer extensão E de K.

Com relação às aplicações traço e norma há dois casos a considerar:

i) $\xi+\xi^4 \in K$. Neste caso $Aut_K(K')$ é gerado por um automorfismo τ de ordem 2 e as aplicações traço e norma são dadas, respectivamente, por $T_\tau(x) = x + \tau(x)$ e $N_\tau(x) = x\tau(x)$ para todo $x \in K'$.

ii) $\xi+\xi^4 \notin K$. Neste caso $Aut_K(K')$ é gerado por um automorfismo τ de ordem 4 e há dois tipos de traço e norma a considerar:

$$T_\tau : K' \to K,\ x \mapsto \sum_{i=0}^{3}\tau^i(x); \qquad N_\tau : K' \to K,\ x \mapsto \prod_{i=0}^{3}\tau^i(x)$$

e

$$T_{\tau^2} : K' \to K_1,\ x \mapsto x + \tau^2(x);\ N_{\tau^2} : K' \to K_1,\ x \mapsto x\tau^2(x),$$

para todo $x \in K'$ onde $K_1 := K'^{\langle\tau^2\rangle}$.

Lema 3.2. *Seja $\delta \in K'$.*
i) *Assuma que $\xi + \xi^4 \in K$. Então, $\delta^{-1}\tau(\delta) \in (K'^*)^5 \Leftrightarrow \delta \in K^*(K'^*)^5$.*
ii) *Assuma que $\xi + \xi^4 \notin K$. Então,*

$$(\delta\tau(\delta^3))^{-1}\tau^2(\delta\tau(\delta^3)) \in (K'^*)^5 \Leftrightarrow \delta\tau(\delta^3) \in K_1^*(K'^*)^5 \Leftrightarrow$$

existe $v \in K_1^*(K'^*)^5$ tal que $\tau(\delta) = v\delta^3$.

Demonstração

i) Se $\delta^{-1}\tau(\delta) \in (K'^*)^5$ então $N_\tau(\delta)\delta^3 \in (K'^*)^5$, ou seja, $\delta^3 \in K^*(K'^*)^5$. Disto segue que $\delta \cdot \delta^5 = (\delta^3)^2 \in K^*(K'^*)^5$ e portanto $\delta \in K^*(K'^*)^5$.

Reciprocamente, se $\delta = uv^5$, com $u \in K^*$ e $v \in K'^*$, então

$$\delta^{-1}\tau(\delta) = (v^{-1}\tau(v))^5 \in (K'^*)^5.$$

ii) Tomando $\delta_1 = \delta\tau(\delta^3)$ e fazendo uso de N_{τ^2} em lugar de N_τ e de K_1 em lugar de K, procedemos de modo idêntico ao caso i) para obter

$$\delta_1^{-1}\tau^2(\delta_1) \in (K'^*)^5 \Leftrightarrow \delta_1 \in K_1^*(K'^*)^5.$$

Agora, se $\delta_1 = \delta\tau(\delta^3) \in K_1^*(K'^*)^5$ então $\delta^2\tau(\delta^6) \in K_1^*(K'^*)^5$ e portanto $\tau(\delta) \in K_1^*(K'^*)^5\delta^3$, ou seja, existe $v \in K_1^*(K'^*)^5$ tal que $\tau(\delta) = v\delta^3$.

Reciprocamente, se $\tau(\delta) = u\lambda^5\delta^3$, com $u \in K_1^*$ e $\lambda \in K'^*$, então
$\delta\tau(\delta^3) = \delta(u\lambda^5\delta^3)^3 = u^3(\lambda^3\delta^2)^5 \in K_1^*(K'^*)^5$. □

3.2 Polinômio Gerador

Dado $\delta \in K'$ satisfazendo as condições do Teorema 3.1.ii, denotemos $F'_\delta = K'(\beta)$, com $\beta^5 = \delta^{-1}\tau(\delta)$ se $\xi+\xi^4 \in K$ e $\beta^5 = (\delta\tau(\delta^3))^{-1}\tau^2(\delta\tau(\delta^3))$ se $\xi+\xi^4 \notin K$.

Denotemos também por F_δ a única extensão quíntica de K contida em F'_δ. Pela Proposição 1.1.i temos $F_\delta = K(x)$, para qualquer $x \in F_\delta \setminus K$. Tal como no caso cúbico (ver Seção 2.2) aqui também vamos escolher um específico x, construído a partir de β, e determinar $m_{x,K}(X)$.

Teorema 3.3.

i) *Assuma que* $\xi + \xi^4 \in K$ *e seja* $\delta \in K'$ *tal que* $\delta^{-1}\tau(\delta) \notin K'^5$. *Então existe* $x \in F_\delta$ *tal que* $F_\delta = K(x)$ *e*

$$m_{x,K}(X) = X^5 - 5X^3 + 5X - T_\tau(\delta^{-1}\tau(\delta)).$$

ii) *Assuma que* $\xi + \xi^4 \notin K$ *e seja* $\delta \in K'$ *tal que* $(\delta\tau(\delta^3))^{-1}\tau^2(\delta\tau(\delta^3)) \notin K'^5$. *Então existe* $x \in F_\delta$ *tal que* $F_\delta = K(x)$ *e*

$m_{x,K}(X) = X^5 - 10X^3 - 5T_\tau\left(\frac{\tau^2(\delta\tau(\delta^3))}{\delta\tau(\delta^3)}\right)X^2 + 5\left(1 - T_\tau\left(\frac{\delta^4\tau(\delta^2)}{\tau^2(\delta^4\tau(\delta^2))}\right)\right)X - T_\tau\left(\frac{\delta^7\tau(\delta))}{\tau^2(\delta^7\tau(\delta))}\right)$.

Demonstração

Segue da demonstração do Teorema 1.10.iii $\Rightarrow$ i e da demonstração do Teorema 3.1.ii que $Aut_K(F'_\delta)$ é gerado pelos K-automorfismos σ e ρ dados por

i) $\sigma(\beta) = \xi\beta$, $\rho(\beta) = \beta^{-1}$, $\sigma|_{K'} = id_{K'}$ e $\rho|_{K'} = \tau$, se $\xi + \xi^4 \in K$,
ou
ii) $\sigma(\beta) = \xi\beta$, $\rho(\beta) = c\beta^2$, $\sigma|_{K'} = id_{K'}$ e $\rho|_{K'} = \tau$, com $c = (\delta\tau(\delta^3))\tau^2(\delta\tau(\delta^3))^{-1}$, se $\xi + \xi^4 \notin K$.

Além disso, conforme a demonstração do Teorema 1.9.ii, temos $F_\delta = F_\delta'^{\langle\rho\rangle}$ e, pelo Teorema 1.6.ii, $Aut_K(F_\delta) = \langle\sigma\rangle$.

Tomamos $x \in F_\delta$ dado por: $x = \beta + \rho(\beta) = \beta + \beta^{-1}$ no caso i) e $x = \beta + \rho(\beta) + \rho^2(\beta) + \rho^3(\beta) = \beta + c\beta^2 + \beta^{-1} + (c\beta^2)^{-1}$ no caso ii). Obviamente $x \notin K$ (pois $\sigma(x) \neq x$) e portanto $F_\delta = K(x)$, pela Proposição 1.1.i. Resta então determinar $m_{x,K}(X)$. Observemos que

$$m_{x,K}(X) = \prod_{i=0}^{4}(X - \sigma^i(x)) = X^5 - t_1X^4 + t_2X^3 - t_3X^2 + t_4X - t_5,$$

com $t_1 = T_\sigma(x)$, $t_2 = T_\sigma(x\sigma(x) + x\sigma^2(x))$, $t_3 = T_\sigma(x\sigma(x)\sigma^2(x) + x\sigma(x)\sigma^3(x))$, $t_4 = T_\sigma(x\sigma(x)\sigma^2(x)\sigma^3(x))$ e $t_5 = N_\sigma(x)$, onde T_σ e N_σ denotam, respectivamente,

as aplicações traço e norma relativas a σ, isto é, $T_\sigma(z) = \sum_{i=0}^{4}\sigma^i(z)$ e $N_\sigma(z) = \prod_{i=0}^{4}\sigma^i(z)$, para todo $z \in F'_\delta$.

Fazendo uso do fato que $T_\sigma(\beta^i) = 0$, $1 \leq i \leq 4$ e que $\sigma\rho = \rho\sigma$, iremos obter, após um cálculo direto e pacientemente efetuado: $t_1 = 0$, $t_2 = -5$, $t_3 = 0$, $t_4 = 5$ e $t_5 = T_\tau(\delta^{-1}\tau(\delta))$ no caso i), e $t_1 = 0$, $t_2 = -10$, $t_3 = 5T_\tau\left(\frac{\tau^2(\delta\tau(\delta^3))}{\delta\tau(\delta^3)}\right)$, $t_4 = 5\left(1 - T_\tau\left(\frac{\delta^4\tau(\delta^2)}{\tau^2(\delta^4\tau(\delta^2))}\right)\right)$ e $t_5 = T_\tau\left(\frac{\delta^7\tau(\delta))}{\tau^2(\delta^7\tau(\delta))}\right)$ no caso ii). □

3.3 Caracterização 2

O teorema a seguir é uma conseqüência imediata do que vimos nas Seções 3.1 e 3.2.

Teorema 3.4. *Seja F uma extensão de K.*

i) *Assuma que $\xi + \xi^4 \in K$. Então F é extensão quíntica cíclica de K se e somente se $F \simeq_K \frac{K[X]}{(f_c(X))}$, com $f_c(X) = X^5 - 5X^3 + 5X - T_\tau(c)$ e $c = u\tau(u)^{-1}$, para algum $u \in K'^* \setminus K^*(K'^*)^5$.*

ii) *Assuma que $\xi + \xi^4 \notin K$. Então F é extensão quíntica cíclica de K se somente se $F \simeq_K \frac{K[X]}{(f_c(X))}$, com*

$$f_c(X) = X^5 - 10X^3 - 5T_\tau(c)X^2 + 5(1 - T_\tau(c\tau(c)))X - T_\tau(c^2\tau(c))$$

e $c = u\tau^2(u)^{-1}$, para algum $u \in K'^* \setminus K_1^*(K'^*)^5$.

Demonstração

($\Rightarrow$) Decorre imediatamente dos Teoremas 3.1, 3.3 e do Lema 3.2. No caso i) basta tomar $u = \delta$. No caso ii), basta tomar $u = \delta\tau(\delta^3)$.

($\Leftarrow$) Se $u \notin K^*(K'^*)^5$ (resp. $u \notin K_1^*(K'^*)^5$) então $c = u\tau(u)^{-1} \notin K'^5$ (resp. $c = u\tau^2(u)^{-1} \notin K'^5$) pelo Lema 3.2. Logo tomando β em algum fêcho algébrico de K' tal que $\beta^5 = c^{-1}$ (resp. $\beta^5 = c^{-1}$), temos $F' = K'(\beta)$ uma extensão cíclica de K de grau 10 (resp. 20), pelo Teorema 3.1. Tomando F a única extensão quíntica cíclica de K contida F' e procedendo exatamente como na

demonstração do Teorema 3.3, vamos obter (em ambos os casos i) e ii)) $x \in F$ tal que $F = K(x)$ e $m_{x,K}(X) = f_c(X)$. Portanto $\frac{K[X]}{(f_c(X))}$ é uma extensão quíntica cíclica de K. □

Vejamos agora que:

a) no caso em que $\xi + \xi^4 \in K$ temos

$$T_\tau(c) = T_\tau\left(\frac{u}{\tau(u)}\right) = \frac{u}{\tau(u)} + \frac{\tau(u)}{u} = \frac{T_\tau(u^2)}{N_\tau(u)}.$$

b) no caso em que $\xi + \xi^4 \notin K$ temos

$$T_\tau(c) = T_\tau\left(\frac{u}{\tau^2(u)}\right) = \frac{u}{\tau^2(u)} + \frac{\tau(u)}{\tau^3(u)} + \frac{\tau^2(u)}{u} + \frac{\tau^3(u)}{\tau(u)} = \frac{T_\tau(u^2\tau(u)\tau^3(u))}{N_\tau(u)},$$

$$T_\tau(c\tau(c)) = T_\tau\left(\tfrac{u_1}{\tau^2(u_1)}\right) = \tfrac{T_\tau(u_1^2\tau(u_1)\tau^3(u_1))}{N_\tau(u_1)}, \text{ com } u_1 = u\tau(u),$$

$$T_\tau(c^2\tau(c)) = T_\tau\left(\tfrac{u_2}{\tau^2(u_2)}\right) = \tfrac{T_\tau(u_2^2\tau(u_2)\tau^3(u_2))}{N_\tau(u_2)}, \text{ com } u_2 = u^2\tau(u).$$

Vejamos também que no caso $\xi + \xi^4 \notin K$, temos $K' = K_1(\xi)$ com $K_1 = K(\xi + \xi^4) = K'^{\langle\tau^2\rangle}$. Logo, todo $u \in K'^*$ pode ser escrito na forma $u = v_0 + v_1\xi$ com $v_0, v_1 \in K_1$. Ainda se $v_1 \neq 0$ então $u' = \frac{u}{v_1} = \frac{v_0}{v_1} + \xi$ e $\frac{u'}{\tau^2(u')} = \frac{u}{\tau^2(u)}$, ou seja, para efeito do cálculo de $T_\tau\left(\frac{u}{\tau^2(u)}\right)$, podemos trocar u por u', se necessário.

Portanto podemos considerar apenas os elementos $u \in K'^*$ da forma $u = v+\xi$, com $v \in K_1$, ou seja, da forma $u = s+t(\xi+\xi^4)+\xi = s+(t+1)\xi+t\xi^4$, com $s, t \in K$.

Então para $c = \frac{u}{\tau^2(u)}$ temos $T_\tau(c) = \frac{T_\tau(u^2\tau(u)\tau^3(u))}{N_\tau(u)}$ e um cálculo direto nos dá $T_\tau(u^2\tau(u)\tau^3(u)) = \varepsilon(u)^4$, com $\varepsilon(u) = 1 + s + 2t$. Assim,

$$T_\tau(c\tau(c)) = T_\tau\left(\frac{u_1}{\tau^2(u_1)}\right) = \frac{\varepsilon(u_1)^4}{N_\tau(u_1)} = \frac{\varepsilon(u_1)^4}{N_\tau(u)^2},$$

$$T_\tau(c^2\tau(c)) = T_\tau\left(\frac{u_2}{\tau^2(u_2)}\right) = \frac{\varepsilon(u_2)^4}{N_\tau(u_2)} = \frac{\varepsilon(u_2)^4}{N_\tau(u)^3},$$

com $u_1 = u\tau(u) = s_1 + (t_1 + 1)\xi + t_1\xi^4$, $u_2 = u^2\tau(u) = s_2 + (t_2 + 1)\xi + t_2\xi^4$, $\varepsilon(u_1) = 1 + s_1 + 2t_1$ e $\varepsilon(u_2) = 1 + s_2 + 2t_2$.

Naturalmente s_i e t_i (i=1,2) são funções dos parâmetros s e t que determinam u e podem ser determinadas através de um cálculo paciente e efetivo. A norma $N_\tau(u)$, também função de s e t, é dada pela expressão:

$$N_\tau(u) = s^4 - s^3(1+2t) + s^2(1-t-t^2) - s(1+t-3t^2-2t^3) + (1-t+t^2+t^3+t^4).$$

Diante dessas considerações temos então a seguinte reformulação do Teorema 3.4.

Teorema 3.5. *Seja F uma extensão de K.*
i) *Assuma que $\xi + \xi^4 \in K$. Então F é uma extensão quíntica cíclica de K se e somente se $F \simeq_K \frac{K[X]}{(f_u(X))}$ com $f_u(X) = X^5 - 5X^3 + 5X - \frac{T_\tau(u^2)}{N_\tau(u)}$, para algum $u \in K'^* \setminus K^*(K'^*)^5$.*

ii) *Assuma que $\xi + \xi^4 \notin K$. Então F é extensão quíntica cíclica de K se e somente se $F \simeq_K \frac{K[X]}{(f_u(X))}$ com*

$$f_u(X) = X^5 - 10X^3 - 5\frac{\varepsilon(u)^4}{N_\tau(u)}X^2 + 5\left(1 - \frac{\varepsilon(u\tau(u))^4}{N_\tau(u)^2}\right)X - \frac{\varepsilon(u^2\tau(u))^4}{N_\tau(u)^3},$$

para algum $u \in K'^* \setminus K_1^*(K'^*)^5$. □

3.4 A Classificação

Nesta seção apresentaremos as condições necessárias e suficientes para que duas extensões quínticas cíclicas de K sejam K-isomorfas. Isto é descrito no teorema a seguir, o qual é conseqüência dos resultados discutidos nas seções anteriores. Para tanto utilizaremos a caracterização de extensões quínticas cíclicas de K dada pelo Teorema 3.5.

Teorema 3.6.

i) Assuma que $\xi + \xi^4 \in K$. Sejam $u_i \in K'^* \setminus K^*(K'^*)^5$ e $F_{u_i} = \frac{K[X]}{(f_{u_i}(X))}$, com $f_{u_i}(X) = X^5 - 5X^3 + 5X - \frac{T_\tau(u_i^2)}{N_\tau(u_i)}$, i=1,2. Então, $F_{u_1} \simeq_K F_{u_2}$ se e somente se $u_1 u_2^l \in K^*(K'^*)^5$, para algum $1 \leq l \leq 4$.

ii) Assuma que $\xi + \xi^4 \notin K$. Sejam $u_i \in K'^* \setminus K_1^*(K'^*)^5$ e $F_{u_i} = \frac{K[X]}{(f_{u_i}(X))}$, com

$$f_{u_i}(X) = X^5 - 10X^3 - 5\frac{\varepsilon(u_i)^4}{N_\tau(u_i)}X^2 + 5\left(1 - \frac{\varepsilon(u_i\tau(u_i))^4}{N_\tau(u_i)^2}\right)X - \frac{\varepsilon(u_i^2\tau(u_i))^4}{N_\tau(u_i)^3},$$

i=1,2.

Então $F_{u_1} \simeq_K F_{u_2}$ se e somente se $u_1u_2^l \in K_1^*(K'^*)^5$, para algum $1 \leq l \leq 4$.

Demonstração

Demonstraremos apenas o caso i). O caso ii) se demonstra de maneira similar.

Sejam $c_i = u_i\tau(u_i)^{-1}$ e $F'_{u_i} = F_{u_i}(\xi) = \frac{K'[X]}{(f_{u_i}(X))} \simeq \frac{K[X]}{(X^5 - c_i)}$, i=1,2.

É imediato verificar pelo Teorema 1.8 que $F_{u_1} \simeq_K F_{u_2}$ se e somente se, para algum $1 \leq l \leq 4$, $(u_1u_2^l)\tau(u_1u_2^l)^{-1} \in (K'^*)^5$, o que é equivalente a $u_1u_2^l \in K^*(K'^*)^5$, pelo Lema 3.2. □

Observemos que a relação de K-isomorfismo entre as extensões quínticas cíclicas de K é uma relação de equivalência.

Corolário 3.7. *Existe uma correspondência 1 a 1 entre o conjunto das classes de isomorfismo de extensões quínticas cíclicas de K e o conjunto dos elementos $\overline{u} \in \frac{K'^*}{K^*(K'^*)^5}$ $\left(resp.\ \frac{K'^*}{K_1^*(K'^*)^5}\right)$ tais que $\overline{u} \neq \overline{1}$ se $\xi + \xi^4 \in K$ (resp. $\xi + \xi^4 \notin K$).*

Demonstração

É uma conseqüência imediata do Teorema 3.6. □

3.5 Exemplos

Para o exemplo utilizaremos a caracterização de extensão quíntica cíclica dada no Teorema 3.5.

Vejamos o caso $K = \mathbb{Q}$. Tomemos $u = \xi$, por conseguinte temos $f_\xi(X) = X^5 - 10X^3 + 5X^2 + 10X + 1$.

O polinômio $f_\xi(X) = X^5 - 10X^3 + 5X^2 + 10X + 1$ é claramente irredutível em $\mathbb{Q}[X]$ ou equivalentemente em $\mathbb{Z}[X]$ (conforme Lema de Gauss). Caso contrário teríamos a imagem (módulo p) $\overline{f}_\xi(X)$ redutível em $\mathbb{Z}_p[X]$ para qualquer primo p. Em particular teríamos $\overline{f}_\xi(X) = X^5 + X^2 + 1$ redutível em $\mathbb{Z}_2[X]$ o que seria absurdo pois $\overline{f}_\xi(X)$ não tem raízes em $\mathbb{Z}_2$ e o único polinômio de grau 2 irredutível em $\mathbb{Z}_2[X]$ é $g(X) = X^2 + X + 1$ e $g(X)$ não divide $\overline{f}_\xi(X)$.

Portanto $f_\xi(X)$ é irredutível sobre $\mathbb{Q}$.

Referências Bibliográficas

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

[2] Childs, L.N.- *Cyclic Stickelberger cohomology and descent of Kummer extensions*, Proc. AMS **90**, 505-510

[3] Jensen, Ch.L. e Lodet, A. and Yui, N. - *Generic polynomials, Construtive Aspect of the Inverse galois Problem*, Cambridge university Press, 2002.

[4] Kersten, I. and Michalicck, J. - A characterization of Galois field extension of degree 3, *Comm. in Algebra*, **15** (1987), pp. 927-933.

[5] McCarthy, P.J. - *Algebraic Extensions of Fields*, Dover Pub, Inc New York, 1991.

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

[7] Nagata, M. - *Field Theory*, Marcel Dekker, New York, 1977.

[8] Paques, A. - A note on cubic Galois extensions, *Comm. in Algebra*, **29** (2001), pp. 5279-5289.

[9] Rotman, J. - *Galois Theory*, Springer Verlag, New York, 1990.

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

[11] Stewart, I. - *Galois Theory*, Chapman and Hall, New York, 1973.