Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Curso de Especialização em Matemática

Vinícius Lara Lima

Solubilidade por Radicais em Corpos de Característica p

Belo Horizonte
2013

Vinícius Lara Lima

Solubilidade por Radicais em Corpos de Característica p

Monografia apresentada ao Curso de Matemática da UFMG, como requisito para a obtenção parcial do grau de ESPECIALISTA em Matemática.

Orientador: André Gimenez Bueno

Doutor em Matemática - UFMG

Belo Horizonte

2013

Lima, Vinícius

Solubilidade por Radicais em

Corpos de Característica p / Vinícius Lima - 2013

42.p

1.Álgebra Abstrata 2. Teoria dos Números.. I.Título.

CDU 536.21

Vinícius Lara Lima

Solubilidade por Radicais em Corpos de Característica p

Monografia apresentada ao Curso de Matemática da UFMG, como requisito para a obtenção parcial do grau de ESPECIALISTA em Matemática.

Aprovado em

BANCA EXAMINADORA

André Gimenez Bueno

Doutor em Matemática - UFMG

Fábio Enrique Brochero Martinez

Doutor em Matemática - UFMG

Viktor Bekkert

Doutor em Matemática - UFMG

Resumo

A solubilidade por radicais é tema frequentemente discutido e estudado nas universidades, principalmente quando envolve polinômios com coeficientes no conjunto dos racionais, corpo de característica zero. Por outro lado, menos frequente é a discussão da solubilidade por radicais em corpos de característica p, com p primo. Este trabalho é produto de pesquisa cujo objetivo foi o de elucidar os principais resultados que envolvem o asunto.

Abstract

The solvabilty of polynomial equations by radicals is usually studied in undergraduate courses only for fields of zero characteristic, e.g. the rationals. The main result can be extended to characteristic p, provided one takes into account the Artin-Schreier extensions. This work proposes to determine which equations are solvable by radicals, over any field.

Keywords: Galois Theory, Artin-Schreier extensions, Norms and Traces, Hilbert's theorem 90.

Agradecimentos

Agradeço a Deus, esposa, familiares, professores e colegas da UFMG.

Sumário

1 Introdução

O presente trabalho aborda resultados importantes da Teoria de Galois, sobretudo aqueles que nos auxiliam no entendimento da solubilidade por radicais em corpos de característica p.

Bem conhecida é a história de Evarist Galois (1811-1832) e sua tentativa e acerto na prova da não solubilidade por radicais de equações com grau igual ou superior a 5. É certo também que Niels Abel (1802-1829) teve papel fundamental nesse trabalho e que ambos trabalhavam em equações com coeficientes em corpos de característica zero. De fato, muito relevante foi tal demonstração e a partir daí muito se desenvolveu a Álgebra Abstrata até chegar à Teoria de Galois como hoje a conhecemos, muito mais abrangente, incluindo resultados para corpos de característica p.

Com objetivo de facilitar a leitura e sem a pretenção de discorrer assuntos considerados como pré-requisitos para uma ideal interpretação, esta monografia ocultará algumas demonstrações que podem ser verificadas nos livros elencados nas referências bibliográficas. No momento, resalta-se o fato de ser usado como bibliografia principal o excelente livro Álgebra, de Serge Lang [1].

Previamente, serão apresentadas definições e resultados de parte da teoria que envolve extensões de corpos e corpos finitos. Após, tópicos aqui considerados essenciais da Teoria de Galois. Destaque para os Teoremas comummente denominados Fundamental da Teoria de Galois, 90 de Hilbert (formas multiplicativa e aditiva), Artin-Schreier, além é claro do Teorema central que trata solubilidade por radicais em corpos de característica $p \geq 0$.

Com intenção de trazer clareza ao texto é que o autor teve o cuidado de detalhar demonstrações e de inserir comentários, observações e exemplos que trazem originilidade a este trabalho e, de fato, o distingue do texto encontrado em qualquer das referências.

2 Conteúdo Preliminar

Neste capítulo são apresentados alguns resultados importantes para melhor entendimento do assunto que trata este trabalho. Entretanto, são conteúdos básicos da Teoria de Corpos, trabalhados em cursos de Álgebra para graduação. ç

2.1 Extensão de Corpos

Um corpo E é chamado de *extensão* de um corpo K sempre que $E \supseteq K$, isto é, se K for um subcorpo de E.

Observe que podemos enxergar E como um Espaço Vetorial sobre K e assim, se E tem dimensão finita - como espaço vetorial -, dizemos que E é uma extensão finita de K, respectivamente, se E tem dimensão infinita, dizemos que E é uma extensão infinita sobre K.

Denotamos por $[E : K]$ o *grau* da extensão E sobre K, que corresponde à dimensão do espaço vetorial E sobre K. O grau de uma extensão pode ser finito ou infinito.

Uma extensão E sobre K pode ser algébrica ou transcendente. Dizemos que E é uma *extensão algébrica* se $\forall\ \alpha \in E,\ f(\alpha) = 0$ para algum $f(x) \in K[x]$ (anel de polinômios), não nulo, nesse caso α é algébrico sobre K. Se, para algum $\alpha \in E,\ \nexists\ f(x) \in K[x]$, não nulo, tal que $f(\alpha) = 0$ então α é transcendente e a extensão E é *transcendente* .

Denotamos por $K(\alpha)$ o menor corpo que contém o corpo K e o elemento α. Então $K(\alpha)$ é uma extensão de K.

Dizemos também que uma extensão E sobre K é *simples* se $\exists\ \alpha \in E$ tal que $E = K(\alpha)$.

Exemplo 2.1.1. Temos que $\mathbb{R} \subset \mathbb{C},\ \mathbb{C}$ é extensão de $\mathbb{R}$. Como $\mathbb{C} = \mathbb{R}[i]$ e i é algébrico sobre $\mathbb{R}$, pois $f(x) = x^2 + 1 \ \in \ \mathbb{R}[x]$ e $f(i) = 0$, então $\mathbb{C}$ é uma extensão algébrica e simples.

O corpo $\mathbb{C}$ tem grau 2 sobre $\mathbb{R}$, logo $[\mathbb{C} : \mathbb{R}] = 2$. Isso segue do fato de $\{1, i\}$ ser uma base para $\mathbb{C}$ sobre $\mathbb{R}$. De fato, todo numero complexo é da forma $a + bi$, ou seja, $\{1, i\}$ gera $\mathbb{C}$. Além disso, $a + bi = 0$, então $a = b = 0$, que mostra que $\{1, i\}$ é L.I..

Observação 2.1.2. Observe que $\forall\ a+bi \in \mathbb{C},\ f(x) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$ é o polinômio tal que $f(a+bi) = 0$.

Exemplo 2.1.3. $\mathbb{R}$ é extensão transcendente sobre $\mathbb{Q}$, pois $\pi \in \mathbb{R}$ é transcendente (ver [10]).

Sendo α um número transcedente sobre o corpo K indica que a extensão $K(\alpha)$ será infinita. De fato, a base de $K(\alpha)$ deve conter α e todas as suas potências, logo $K(\alpha)$ é extensão infinita sobre K. Veremos, ainda nneste capítulo, teorema que destaca o fato de $K(\alpha)$ ser isomorfo a $K(x)$ (corpo quociente do anel de polinômios), toda vez que α é transcendente.

Definição 2.1.4. O *polinômio minimal* de um elemento α, $\alpha \in E$ extensão sobre K é o polinômio mônico irredutível $f(x) \in K[x]$ de menor grau tal que $f(\alpha) = 0$.

Devemos resaltar que o polinômio minimal é único (ver [4]).

Teorema 2.1.5. *Sejam E, F e K três corpos tais que $K \subset F \subset E$, F extensão finita sobre K e E extensão finita sobre F, então*

$$[E : K] = [E : F][F : K].$$

Demonstraremos mais adiante que o grau de uma extensão algébrica finita sobre um corpo K é igual ao grau do polinômio minimal dos elementos algébricos adjuntados.

Teorema 2.1.6. *Seja $\varphi : K[x] \to E$ tal que $\alpha \in E \supset K$, E extensão sobre o corpo K e $\varphi(f(x)) = f(\alpha)$, então φ é um homomorfismo e:*

i) Im $\varphi = K[\alpha]$

ii) *Se α é transcendente sobre K, então* ker $\varphi = \{0\}$.

iii) *Se α é algébrico sobre K e $f(x)$ é o polinômio minimal de α, então* ker $\varphi = K[x]\cdot f(x)$ *é um ideal maximal de $K[x]$.*

iv) $K[x]/\ker\ \varphi$ *(anel quociente)* $\approx K[\alpha]$.

Assim, o corpo quociente $K(\alpha) \approx K[\alpha]$ para α algébrico e, para α transcendente, $K[x] \approx K[\alpha]$, isto é, $K(x) \approx K(\alpha)$. O teorema acima pode ser demonstrado a partir do 1° teorema de homomorfismo entre anéis.

Como consequência do Teorema 2.1.6 podemos verificar o seguinte corolário:

Corolário 2.1.7. *Sejam α e $\beta \in L \supset K$ dois elementos algébricos sobre K e $f(x)$ o polinômio minimal de α e β. Então $K(\alpha)$ e $K(\beta)$ são isomorfos.*

Proposição 2.1.8. *Seja n o grau do polinômio minimal de $\alpha \in E \supset K$, com E extensão de corpos sobre K, então tomando $f(x) \in K[x]$, $f(\alpha)$ é expresso de modo único na forma*

$$f(\alpha) = a_0 + a_1\alpha^1 + \ldots + a_{n-1}\alpha^{n-1}$$

com $a_i \in K \ \forall i \in \{0, 1, 2, ..., n-1\}$. A partir da proposição acima, observemos que $\forall\ f \in K(\alpha),\ f = a_0 + a_1\alpha^1 + \ldots + a_{n-1}\alpha^{n-1}$ desde que n seja o grau do polinômio minimal de α, assim $n = [K(\alpha) : K]$, pois podemos considerar o conjunto $\{1, \alpha^1, \ldots, \alpha^{n-1}\}$ linearmente independente como base de $K(\alpha)$, onde 1 é a unidade de K.

Exemplo 2.1.9. Sejam $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ e $\mathbb{Q}[\sqrt[4]{2}] \supset \mathbb{Q}$ $f(x) = x^2 - 2$ e $g(x) = x^4 - 2$ são polinômios minimais de $\sqrt{2}$ e $\sqrt[4]{2}$ respectivamente. Temos que:

- $\forall\ k_1 \in \mathbb{Q}[\sqrt{2}],\ k_1 = a_0 + a_1(\sqrt{2})$ com $a_i \in \mathbb{Q},\ i \in \{0, 1\}$.
- $\forall\ k_2 \in \mathbb{Q}[\sqrt[4]{2}],\ k_2 = b_0 + b_1(\sqrt[4]{2}) + b_2(\sqrt[4]{2})^2 + b_3(\sqrt[4]{2})^3$ com $b_j \in \mathbb{Q},\ j \in \{0, 1, 2, 3\}$.

Isto é $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}]$. Note que $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, $[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}] = 4$ e $[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}[\sqrt{2}]] = 2$. Então $[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$

Exemplo 2.1.10. O elemento $\alpha = \sqrt[3]{2}$ é algébrico sobre $\mathbb{Q}$.

$\mathbb{Q}[\sqrt[3]{2}]$ é corpo e $f(x) = x^3 - 2$ é o polinômio minimal de $\sqrt[3]{2}$. Mas $\beta = \sqrt[3]{2} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}i}{2}\right) \in \mathbb{C}$ também tem $f(x)$ como polinômio minimal, $\mathbb{Q}[\beta]$ é corpo. Temos então $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$, $[\mathbb{Q}[\beta] : \mathbb{Q}] = 3$ e $\mathbb{Q}[\alpha] \approx \mathbb{Q}[\beta]$.

Exemplo 2.1.11. Seja p primo e $\alpha_j = \sqrt[2^j]{p} \in \mathbb{R}$. Então $f(x) = x^{2^j} - p \in \mathbb{Q}[x]$ é o polinômio minimal de α_j, $\forall\ j \in \mathbb{N}$.

Como α_j é algébrico, $\mathbb{Q}[\alpha_j]$ é corpo, $[\mathbb{Q}[\alpha_j] : \mathbb{Q}] = 2^j,\ \mathbb{Q} \subset \mathbb{Q}[\alpha_j] \subset \mathbb{R}$ e ainda

$$\mathbb{Q} \subset \mathbb{Q}[\alpha_1] \subset \mathbb{Q}[\alpha_2] \subset \mathbb{Q}[\alpha_3] \subset \ldots \subset \mathbb{R}$$

Verificamos que $\mathbb{R}$ é uma extensão infinita sobre $\mathbb{Q}$.

Definição 2.1.12. Dado um corpo K, se $\forall\ f(x) \in K[x]$ de grau ≥ 1 possui raiz em K, então dizemos que K é *algebricamente fechado*.

Vamos lembrar aqui da definição de Característica de um corpo.

Definição 2.1.13. A *característica* de um corpo K é o menor número inteiro positivo p tal que $p.a = 0\ \forall a \in K$. Se tal número não existe, dizemos que K tem característica zero.

Observe que a característica de um corpo K ou é zero ou é p primo. De fato, suponha que a característica seja n composto. Então $n = s.t$, com s e t inteiros positivos menores que n, e $n.1 = 0$. Isso implica que $s.t.1 = (s.1).(t.1) = 0$, e portanto $s.1 = 0$ ou $t.1 = 0$, ou seja, $s.a = 0$ ou $t.a = 0\ \forall a \in K$. Contrariando o fato de n ser característica.

Proposição 2.1.14. *Seja K um corpo de característica zero. Então as afirmações seguintes são equivalentes:*

i) *K é um corpo algebricamente fechado.*

ii) *Todo polinômio $f(x) \in K[x]$ se decompõe num produto de fatores lineares.*

iii) *Se $f(x) \in K[x]$ é irredutível, então $f(x)$ tem grau 1.*

iv) *Não existem extensões algébricas próprias de K.*

Essa proprosição pode ser facilmente verificada.

Para todo $f(x) \in K[x]$, $f(x) = c(x-\alpha_1)^{m_1} \cdot \ldots \cdot (x-\alpha_r)^{m_r}$, $r, m_1, \ldots, m_r \in \mathbb{N}$, $c \in K$. Chamamos de m_i a *multiplicidade da raiz* α_i e, se $m_i = 1$, α_i é chamada de *raiz simples* de $f(x)$.

No Capítulo 3.1 veremos mais detalhes e resultados que envolvem polinômios que se decompõe em fatores lineares bem como os corpos onde esses polinômios se decompõe.

Proposição 2.1.15. *Seja K corpo de característica zero. Se $f(x) \in K[x]$ é um polinômio irredutível sobre K, então $f(x)$ possui apenas raízes simples.*

Nas proposições 2.1.14 e 2.1.15, a hipótese de K ser corpo de característica zero é essencial, verifique o exemplo abaixo.

Exemplo 2.1.16. Seja K um corpo de característica p e seja $\beta = \sqrt[p]{\alpha}$ tal que $\alpha \in K$, mas $\beta \notin K$. O polinômio $f(x) = x^p - \alpha \in K[x]$, é minimal de β. Agora considere a extensão $L = K(\beta)$ e tome o polinômio $l(x) = x^p - \beta^p = x^p - \alpha \in L[x]$. Observe que apesar de $f(x)$ ser irredutível em $K[x]$, β é raiz de multiplicidade p em $L[x]$.

Definição 2.1.17. Seja E uma extensão do corpo K. Dizemos que E é um *corpo de fatoração* ou *corpo de decomposição* de um polinômio $f(x) \in K[x]$ sobre K se E é o menor corpo que contém todas as raízes de $f(x)$.

Exemplo 2.1.18. O corpo $\mathbb{C}$ é algebricamente fechado e $\mathbb{C} = \mathbb{R}[i]$ é corpo de decomposição de $x^2 + 1 \in \mathbb{R}[x]$.

Se $f(x) \in \mathbb{Q}[x]$ e $f(x) = x^3 - 2$, $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ e $\bar{\beta}$ são as raízes de $f(x)$. Observe que $\mathbb{Q}[\beta] \ni \bar{\beta}$ mas $\sqrt[3]{2} \notin \mathbb{Q}[\bar{\beta}]$, então $\mathbb{Q}[\sqrt[3]{2}, \beta]$ é corpo de fatoração de $f(x) = x^3 - 2$ sobre $\mathbb{Q}$.

Exemplo 2.1.19. De forma mais geral, podemos mostrar que se $f(x) = x^n - 2 \in \mathbb{Q}[x]$, $\alpha = \sqrt[n]{2}$, $u = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, $\beta = \alpha u$, então $\mathbb{Q}[\alpha, u] = \mathbb{Q}[\alpha, \beta]$ é corpo de fatoração de $f(x) = x^n - 2$ sobre $\mathbb{Q}$.

Como sabemos, $\mathbb{R}[x]/\langle x^2 + 1\rangle$ é corpo que contém as raízes de $f(x) = x^2 + 1 \in \mathbb{R}[x]$ e contém $\mathbb{R}$, isto é, extensão de $\mathbb{R}$. Apresentamos agora uma importante generalização de tal fato.

O Teorema abaixo é também conhecido como o Teorema Fundamental da Teoria de Corpos.

Teorema 2.1.20 (Kronecker)**.** *Seja K um corpo e $f(x)$ um polinômio não constante de $K[x]$. Então existe uma extensão E do corpo K que contém uma raiz de $f(x)$.*

Omitiremos aqui a demonstração do Teorema acima, mas é possível vê-la de forma bem clara em [4]. Entretanto, vale ressaltar que a extensão E procurada é exatamente $K[x]/\langle f_i(x)\rangle$, com $f_i(x)$ um fator irredutível de $f(x)$. Sempre podemos tomar $f_i(x)$ pois $K[x]$ é domínio de fatoração única. Então a raiz de $f(x)$ em E é raiz de $f_i(x)$.

Teorema 2.1.21. *Seja K um corpo e $f(x)$ um polinômio não constante de $K[x]$. Então existe um corpo de fatoração E de $f(x)$ sobre K.*

Para verificar a demonstração deste Teorema consulte [4].

Abaixo seguem Teorema e Corolário cujas demonstrações são encontradas na referência [1].

Teorema 2.1.22. *Seja K um corpo. Existe uma extensão algebricamente fechada de K.*

Corolário 2.1.23. *Dado um corpo K, existe uma extensão algébrica L sobre K que é algebricamente fechada.*

Definição 2.1.24. A uma extensão algébrica E de um corpo K que contém as raízes de todos os polinômios com coeficientes em K é chamada de *fecho algébrico* de K.

Definição 2.1.25. *Extensão Normal* de um corpo K é uma extensão algébrica E tal que todo polinômio irredutível em $K[x]$ que possui uma raiz em E pode ser decomposto em $E[x]$ em termos lineares.

Exemplo 2.1.26. Tome $\mathbb{C}$, extensão de corpo que contém $\mathbb{R}$ e $[\mathbb{C} : \mathbb{R}] = 2$. Tomamos 1 a unidade em $\mathbb{R}$ e $\{1, i\}$ a base de $\mathbb{C}$, $i \in \mathbb{C}$ e $i \notin \mathbb{R}$. Seja $f(x)$ irredutível em $\mathbb{R}[x]$ com raiz em $\mathbb{C}$, e seja $a+bi$, $a, b \in \mathbb{R}$, essa raiz. Agora seja $g(x)$ o polinômio minimal de $a+bi$ sobre $\mathbb{R}$, então $g(x)$ tem grau 2, caso contrário, $[\mathbb{C} : \mathbb{R}] \neq 2$ e $f(x)$ é múltiplo de $g(x)$. Como $f(x)$ é irredutível, $f(x) = g(x) \cdot \lambda$ com $\lambda \in \mathbb{R}$. Concluímos que, assim como $g(x)$ tem as raízes em $\mathbb{C}$ (se $a + bi$ é raiz de $g(x)$, $a - bi \in \mathbb{C}$ é a outra raiz), $f(x)$ também o tem. Logo $f(x)$ pode ser decomposto em termos lineares em $\mathbb{C}[x]$.

Exemplo 2.1.27. $\mathbb{Q}[\sqrt[3]{3}]$ é extensão de $\mathbb{Q}$, $\sqrt[3]{3}$ é algébrico sobre $\mathbb{Q}$ e $f(x) = x^3 - 3$ é o seu polinômio minimal. Mas $\mathbb{Q}[\sqrt[3]{3}]$ não possui as raízes complexas de $f(x) \in \mathbb{Q}[x]$. Assim, $f(x)$ não pode ser decomposto em fatores lineares em $\mathbb{Q}[\sqrt[3]{3}][x]$.

Observe que numa extensão normal E de K, se algum polinômio $f(x) \in K[x]$ irredutível tem alguma raiz em E, então todas as suas raízes estão em E.

2.2 Corpos Finitos

Quando falamos sobre a característica de um corpo, dizemos que este corpo possui uma cópia de $\mathbb{Q}$ (característica zero) ou uma cópia de $\mathbb{F}_p$ para algum p primo (característica p).

Isto é, dado um corpo F, tomamos o homomorfismo $\mathbb{Z} \to F$ que leva 1 de Z em 1_F, logo $n \in \mathbb{Z}$ positivo é levado em $1_F + 1_F + ... + 1_F$, com n parcelas. Quando o núcleo do homomorfismo é zero, temos que $\forall\, n \in \mathbb{Z}$ sua imagem é $n.1_F$ diferente de zero, e portanto podemos tomar o homomorfimo injetivo $\mathbb{Q} \hookrightarrow F$, tal que $m/n \mapsto (m.1_F).(n.1_F)^{-1}$, onde m/n é irredutível. Logo F tem uma cópia de $\mathbb{Q}$. Por outro lado, se o núcleo do homomorfismo for diferente de zero, como o núcleo de um homomorfismo é um ideal e o domínio

deste homomorfismo é $\mathbb{Z}$, o núcleo será um ideal principal. É fácil verificar também que esse ideal é primo, portanto gerado por p, um número primo, isto é, é do tipo $p\mathbb{Z}$. Desta forma, pelo primeiro teorema de homomorfismo de anéis, então $\mathbb{Z}/p\mathbb{Z} \simeq \text{Im } \phi$, onde ϕ é o homomorfismo, ou seja, F tem uma cópia de $\mathbb{F}_p$.

Assim, um *Corpo Finito* F, digamos com q elementos (atenção para a diferença entre corpos finitos e extensões finitas), só pode ter uma cópia de $\mathbb{F}_p$. Além disso, $q = p^n$ onde n é a dimensão de F sobre $\mathbb{F}_p$, visto como espaço vetorial. De fato, tome $\{1, e_1, e_2, ..., e_{n-1}\}$ a base de F sobre $\mathbb{F}_p$ onde 1 é o gerador de $\mathbb{F}_p$. Então, dado $q \in F$, $q = \lambda_1.1 + \lambda_2.e_1 + ... + \lambda_n.e_{n-1}$, onde cada λ_i é um elemento de $\mathbb{F}_p$. Mas temos apenas p elementos distindos em $\mathbb{F}_p$, o que significa que temos p^n elementos distintos em F.

Observe que um Corpo de Característica p não é sempre finito, como exemplo tome o corpo quociente $\mathbb{F}_p(x) = \{f(x)/g(x); f(x), g(x) \in \mathbb{F}_p[x], g(x) \neq 0\}$.

Considere o corpo finito F com q elementos, $q = p^n$, e ϕ o *Automorfismo de Frobenius* (ver [1] p. 246), $\phi : F \to F$ dado por $\phi(x) = x^p$ para todo $x \in F$, então:

Teorema 2.2.1. *O grupo de automorfismos de F é cíclico de ordem n, gerado por ϕ.*

Recomenda-se ao leitor interessado verificar a demonstração deste teorema em [1] (p. 246). O automorfismo ϕ acima tem como característica manter fixos os elementos de $\mathbb{F}_p$, dizendo de outra forma, $\phi \in Aut_{\mathbb{F}_p}(F)$ (tal conjunto é definido no próximo capítulo).

Exemplo 2.2.2. Considere o polinômio $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Observe que $f(x)$ é irredutível sobre $\mathbb{F}_2$, já que possui grau 3 e não possui raízes em $\mathbb{F}_2[x]$. Podemos então tomar a extensão finita E de $\mathbb{F}_2$ como no Teorema 2.1.20, isto é, $E = \mathbb{F}_2[x]/ < f(x) >$. O corpo E assim formado possui $2^3 = 8$ elementos. De fato, podemos ver E como o corpo $\{a\theta^2 + b\theta + c | a, b, c \in \mathbb{F}_2\}$, onde θ é raiz de $f(x)$. Como $f(\theta) = \theta^3 + \theta + 1 = 0$, temos que $\theta^3 = \theta + 1$ (aqui vale lembrar que $-1 = 1$ em $\mathbb{F}_2$) e portanto, não é difícil de verificar que θ^2 e $\theta^4 = \theta^2 + \theta$ também são raízes de $f(x)$. Agora considere G o conjunto de Automorfismos de E, temos que os elementos de G são três, a saber: ϕ_1 tal que $\phi_1(\theta) = \theta^2$; $\phi_2(\theta) = \theta^4$ e $\phi_3(\theta) = \theta$, já que os automorfismos levam raiz de $f(x)$ em raiz de $f(x)$.

Veja como calculamos a imagem de ϕ_1:

$$
\begin{aligned}
\phi_1(0) &= 0^2 = 0 \\
\phi_1(1) &= 1^2 = 1 \\
\phi_1(\theta) &= \theta^2 \\
\phi_1(\theta^2) &= (\theta^2)^2 = \theta^4 = \theta^3\theta = (\theta+1)\theta = \theta^2 + \theta \\
\phi_1(\theta+1) &= (\theta+1)^2 = \theta^2 + 2\theta 1 + 1^2 = \theta^2 + 1 \\
\phi_1(\theta^2+1) &= \theta^4 + 2\theta^2 1 + 1^2 = \theta^2 + \theta + 1 \\
\phi_1(\theta^2+\theta) &= (\theta^2+\theta)^2 = (\theta^2)^2 + 2\theta^2\theta + \theta^2 = \theta^4 + \theta^2 = \theta^2 + \theta + \theta^2 = 2\theta^2 + \theta = \theta \\
\phi_1(\theta^2+\theta+1) &= (\theta^2+\theta+1)^2 = (\theta^2+\theta)^2 + 2(\theta^2+\theta)1 + 1^2 = \theta + 1
\end{aligned}
$$

Na tabela abaixo temos as imagens de todos os automorfismos de E:

Elementos de E	Imagem por ϕ_1	Imagem por ϕ_2	Imagem por $\phi_3 = Id$
0	0	0	0
1	1	1	1
θ	θ^2	$\theta^2+\theta$	θ
θ^2	$\theta^2+\theta$	θ	θ^2
$\theta+1$	θ^2+1	$\theta^2+\theta+1$	$\theta+1$
θ^2+1	$\theta^2+\theta+1$	$\theta+1$	θ^2+1
$\theta^2+\theta$	θ	θ^2	$\theta^2+\theta$
$\theta^2+\theta+1$	$\theta+1$	θ^2+1	$\theta^2+\theta+1$

Como esperado, $\phi_i \in G$, $i \in \{1,2,3\}$, mantém fixos os elementos de $\mathbb{F}_2$.

Perceba ainda que $\phi_2 = \phi_1 \circ \phi_1$ e $\phi_3 = \phi_1 \circ \phi_1 \circ \phi_1 = Id$ isto é, G é um grupo cíclico, gerado por ϕ_1, de ordem 3, mesmo grau da extensão $E/\mathbb{F}_2$.

O automorfismo ϕ_1 é o *Automorfismo de Frobenius*.

3 Teoria de Galois

Definição 3.0.3. Uma extensão finita E de um corpo K é chamada *Extensão Galoisiana* se existir um polinômio $f(x) \in K[x]$ tal que E seja um corpo de decomposição de $f(x)$ sobre K.

Exemplo 3.0.4. $\mathbb{Q}(\sqrt[3]{2})$ é subextensão de $\mathbb{Q}(\sqrt[3]{2}, \omega)$ sobre $\mathbb{Q}$, onde ω é uma raiz complexa de $f(x) = x^3 - 2$. A extensão $\mathbb{Q}(\sqrt[3]{2}, \omega)$ de $\mathbb{Q}$ é galoisiana, mas $\mathbb{Q}(\sqrt[3]{2})$ não é galoisina.

Definição 3.0.5. Seja E uma extensão de K. Chamamos de $Aut_K E$ o conjunto de todos automorfismos de E que fixam K, isto é, se $\varphi \in Aut_K E$ então $\varphi|_K = Id$. Também dizemos que φ é um *K-automorfismo* de E.

Dados φ_1, φ_2 e $\varphi_3 \in Aut_K E$, $(\varphi_1 \circ \varphi_2) \circ \varphi_3 = \varphi_1 \circ (\varphi_2 \circ \varphi_3)$, $Id \in Aut_K E$ e $\varphi \circ Id = Id \circ \varphi = \varphi \ \forall \ \varphi \in Aut_K E$, e, por fim, $\forall \ \varphi \in Aut_K E$, $\exists \ \varphi^{-1}$ tal que $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = Id$ pois φ é isomorfismo. Portanto, $Aut_K E$ forma um grupo com a operação composição.

Denotamos por

$$\begin{aligned} G(E/K) &= \{\varphi : E \to E \mid \varphi \text{ é um } K\text{-automorfismo}\} \\ &= \{\varphi | \varphi \in Aut_K E\} \end{aligned}$$

este grupo é chamado de *Grupo de Galois* de E sobre K.

Teorema 3.0.6. *Seja E uma extensão finita de K. Então as seguintes condições são equivalentes:*

i) *$E \supset K$ galoisiana;*

ii) *$E \supset K$ normal;*

iii) *$\forall \ \alpha \in E/K \ \exists \ \varphi \in Aut_K E$ tal que $\varphi(\alpha) \neq \alpha$;*

iv) $[E : K] = |G(E/K)|$.

Exemplo 3.0.7. $\mathbb{Q}[\sqrt{2}]$ é uma extensão galoisiana, pois é também o corpo de decomposição de $f(x) = x^2 - 2$ minimal sobre $\mathbb{Q}$. Como $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, $\mathbb{Q}[\sqrt{2}]$ é extensão normal, ver exemplo (2.1.9) na página 10.

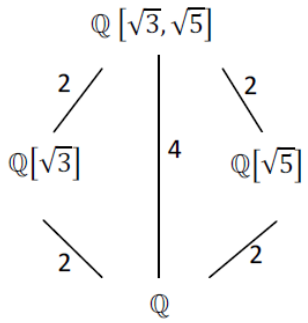
Agora, $\alpha \in \mathbb{Q}[\sqrt{2}],\ \alpha = a + b\sqrt{2},\ a, b \in \mathbb{Q}$. A base desta extensão é $\{1, \sqrt{2}\}$, e sendo φ um $\mathbb{Q}$-automorfismo, $2 = \varphi(2)$, mas

$$\varphi(2) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = (\varphi(\sqrt{2}))^2.$$

Logo $\varphi(\sqrt{2}) = \pm\sqrt{2}$.

E essas são as possibilidades de automorfismos de $\mathbb{Q}[\sqrt{2}]$. Se $\varphi(\sqrt{2}) = \sqrt{2}$ e $\varphi|_{\mathbb{Q}} = Id$ então $\varphi = Id$. Portanto $|G(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})| = 2$.

Exemplo 3.0.8. Considerando $\mathbb{Q}[\sqrt{3}, \sqrt{5}]$ extensão de $\mathbb{Q}$



Verificamos facilmente que $[\mathbb{Q}[\sqrt{3}, \sqrt{5}] : \mathbb{Q}] = 4$ e que $\mathbb{Q}[\sqrt{3}, \sqrt{2}]$ é o corpo de decomposição de $f(x) = (x^2 - 3)(x^2 - 5)$ em $\mathbb{Q}[x]$.

Um isomorfismo leva base em base e $\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\sqrt{5}\}$ é base de $\mathbb{Q}[\sqrt{3}, \sqrt{5}]$ sobre $\mathbb{Q}$, visto como espaço vetorial.

Assim, se φ é um $\mathbb{Q}$-automorfismo de $\mathbb{Q}[\sqrt{3}, \sqrt{5}]$, $\varphi(\sqrt{3}\sqrt{5}) = \varphi(\sqrt{3})\varphi(\sqrt{5})$. Basta então definirmos $\varphi(\sqrt{3})$ e $\varphi(\sqrt{5})$. Mas,

$$\begin{aligned}(\varphi(\sqrt{3}))^2 = \varphi((\sqrt{3})^2) = \varphi(3) = 3 \quad &\Rightarrow \quad \varphi(\sqrt{3}) = \pm\sqrt{3} \\ (\varphi(\sqrt{5}))^2 = \varphi((\sqrt{5})^2) = \varphi(5) = 5 \quad &\Rightarrow \quad \varphi(\sqrt{5}) = \pm\sqrt{5}\end{aligned}$$

Temos então os seguinte $\mathbb{Q}$-automorfismos:

$$\begin{aligned}\varphi_1(\sqrt{3}) &= \sqrt{3}, \quad \varphi_1(\sqrt{5}) = \sqrt{5} \ \Rightarrow \ \varphi_1 = Id. \\ \varphi_2(\sqrt{3}) &= -\sqrt{3}, \quad \varphi_2(\sqrt{5}) = \sqrt{5} \\ \varphi_3(\sqrt{3}) &= \sqrt{3}, \quad \varphi_3(\sqrt{5}) = -\sqrt{5} \\ \varphi_4(\sqrt{3}) &= -\sqrt{3}, \quad \varphi_4(\sqrt{5}) = -\sqrt{5}\end{aligned}$$

Logo, $|G(\mathbb{Q}[\sqrt{3}, \sqrt{5}]/\mathbb{Q})| = 4$.

Definição 3.0.9. Seja E um extensão finita do corpo K e seja $G(E/K)$ o grupo de galois. Se H é um subgrupo $G(E/K)$, o conjunto denotado por

$$E_H = \{x \in E \mid \varphi(x) = x,\ \forall\ \varphi \in H\}$$

é um corpo chamado de *corpo fixo* de H.

Lema 3.0.10 (Artin)**.** *Se $G(E/K)$ é um grupo finito dos K-automorfismos de E, então*

$$|G(E/K)| \leq [E : K]$$

Teorema 3.0.11 (Teorema Fundamental da Teoria de Galois)**.** *Seja L extensão galoisiana de K. Existe uma correspondência biunívoca entre os subcorpos de L que contém K e os subgrupos de $G(L/K)$. Essa correspondência é dada pela função ψ tal que $\psi(H) \mapsto L_H$, $H \subset G(L/K)$ subgrupo, e a inversa $\psi^{-1}(E) \mapsto Aut_E L$, $K \subset E \subset L$, E subcorpo de L.*

Nesta correspondência, se $H = Aut_E L$ então $[L : E] = |H|$. Além disso, E é extensão galoisiana sobre K se e só se H for subgrupo normal de $G(L/K)$, neste caso $Aut_K E \cong G(L/K)/H$.

Exemplo 3.0.12. Seja $\mathbb{Q}(i, \sqrt{2})$ uma extensão galoisiana de $\mathbb{Q}$. Temos que $\{1, i, \sqrt{2}, i\sqrt{2}\}$ é a base do espaço vetorial $\mathbb{Q}(i, \sqrt{2})$ sobre $\mathbb{Q}$ e $\phi(i\sqrt{2}) = \phi(i)\phi(\sqrt{2}),\ \forall\ \phi$ automorfismo de $\mathbb{Q}(i, \sqrt{2})$. Assim determinamos os automorfismos:

$$\begin{aligned}
\phi_1,\ \text{tal que } \phi_1(i) &= i \text{ e } \phi_1(\sqrt{2}) = -\sqrt{2} \\
\phi_2,\ \text{tal que } \phi_2(i) &= -i \text{ e } \phi_2(\sqrt{2}) = \sqrt{2} \\
\phi_3,\ \text{tal que } \phi_3(i) &= -i \text{ e } \phi_3(\sqrt{2}) = -\sqrt{2}
\end{aligned}$$

como elementos de $G(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$ além da identidade. Neste caso sabemos também que $\{Id, \phi_1\},\ \{Id, \phi_2\},\ \{Id, \phi_3\}$ são os subgrupos próprios de $G(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$, e $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$ são os subcorpos próprios de $\mathbb{Q}(i, \sqrt{2})$ que contém $\mathbb{Q}$.

Observe ainda que $\{Id, \phi_1\} = Aut_{\mathbb{Q}(i)}\mathbb{Q}(i, \sqrt{2})$, assim

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(i)] = |Aut_{\mathbb{Q}(i)}\mathbb{Q}(i, \sqrt{2})|.$$

E, $\mathbb{Q}(i)$ é extensão galoisiana, pois é a extensão de decomposição de $f(x) = x^2 + 1$ sobre $\mathbb{Q}$. O subgrupo $\{Id, \phi_1\}$ de $G(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$ é normal. De fato,

$$\begin{aligned}
\phi_2^{-1} \circ Id \circ \phi_2 &= Id, \\
\phi_2^{-1} \circ \phi_1 \circ \phi_2 &: \quad \phi_2^{-1}(\phi_1(\phi_2(i))) = \phi_2^{-1}(\phi_1(-i)) = \phi_2^{-1}(-i) = i = \phi_1(i) \\
&: \quad \phi_2^{-1}(\phi_1(\phi_2(\sqrt{2}))) = \phi_2^{-1}(\phi_1(\sqrt{2})) = \phi_2^{-1}(-\sqrt{2}) = -\sqrt{2} = \phi_1(\sqrt{2}) \\
&\Rightarrow \quad \phi_2^{-1} \circ \phi_1 \circ \phi_2 = \phi_1 \in \{Id, \phi_1\}
\end{aligned}$$

Analogamente verificamos que $\phi_3^{-1} \circ Id \circ \phi_3 = Id$ e $\phi_3^{-1} \circ \phi_1 \circ \phi_3 = \phi_1$.

Portanto, $Aut_{\mathbb{Q}}\mathbb{Q}(i) \cong G(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})/Aut_{\mathbb{Q}(i)}\mathbb{Q}(i,\sqrt{2})$, fato que pode ser facilmente verificado, pois ambos os grupos possuem ordem 2.

Teorema 3.0.13 (Artin)**.** *Seja E um corpo e seja G o grupo de automorfismos de E, com ordem de G igual a n. Seja $K = E_G$ (corpo fixo de G). Então E é uma extensão galoisiana de K e $G = G(E/K)$, e $[E : K] = n$*

Corolário 3.0.14. *Seja E uma extensão galoisiana finita de K e seja $G(E/K)$ o grupo de galois correspondente. Então todo subgrupo de $G(E/K)$ é grupo de galois de alguma extensão de K contida em E.*

De fato, o corolário pode ser facilmente verificado com a aplicação do teorema acima. A demonstração do Teorema pode ser encontrada em [1].

Definição 3.0.15. Sejam as extensões finitas $F = K(\alpha_1, \ldots, \alpha_n)$ e E sobre K, então $EF = E(\alpha_1, \ldots, \alpha_n)$, EF é chamada de *extensão composta* de E e F sobre K.

Teorema 3.0.16. *Seja E uma extensão galoisiana de K e seja F outra extensão de K. Considere L corpo tal que E e F sejam subcorpos de L. Então EF é extensão galoisiana sobre F, e E é extensão galoisiana sobre $E \cap F$. Agora, tome a aplicação*

$$\varphi : G(EF/F) \to G(E/K)$$

tal que $\varphi(\sigma) = \sigma_{|_E}$, então φ é um isomorfismo de $G(EF/F)$ em $G(E/E \cap F) \subset G(E/K)$.

No teorema acima, devemos dar atenção especial ao fato de EF ser extensão galoisiana sobre F. De fato, se E é galoisiana sobre K, é a extensão de decomposição de um $f(x) \in K[x]$, então EF é a menor extensão de F que contém todas as raízes de $f(x)$ visto como elemento de $F[x]$. Observe também que $E/E \cap F$ é galoisiana, pois E/K é galoisiana.

Corolário 3.0.17. *Seja E uma extensão galoisiana finita de K e F uma outra extensão qualquer de K, então $[EF : F]$ divide $[E : K]$.*

É só verificar que a ordem de $G(EF/F)$ divide a ordem de $G(E/K)$ pelo Teorema de Lagrange, pois $G(EF/F)$ é isomorfo a um subgrupo de $G(E/K)$, pelo Teorema (3.0.16).

Importante observar que se excluirmos a hipótese de E ser galoisiana sobre K, não teríamos o mesmo resultado. Basta verificar o seguinte exemplo.

Exemplo 3.0.18. Tome $\zeta = \frac{-1+\sqrt{-3}}{2}$, $\alpha = \sqrt[3]{2}$ e $\beta = \zeta \cdot \alpha$. Agora sejam as extensões $E = \mathbb{Q}(\beta)$, $F = \mathbb{Q}(\alpha)$, $E \neq F$, e

$$EF = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\alpha, \sqrt{-3}).$$

Temos que $E \cap F$ é subcorpo de F, logo tem grau 3 ou 1 sobre $\mathbb{Q}$, pois F tem grau 3 sobre $\mathbb{Q}$. Assim, $E \cap F$ deve ter grau 1 sobre $\mathbb{Q}$ (isto é $E \cap F = \mathbb{Q}$), já que $F \not\subset E$. Como $EF = \mathbb{Q}(\alpha, \sqrt{-3})$, EF/F tem grau 2, logo $E/E \cap F = E/\mathbb{Q}$ tem grau 2. Absurdo. O absurdo aconteceu pois tentamos usar o Teorema (3.0.16) com E não galoisiana.

Teorema 3.0.19. *Sejam E_1 e E_2 extensões galoisianas de K. Então E_1E_2 é extensão galoisiana sobre K, a aplicação $\varphi : G(E_1E_2/K) \to G(E_1/K) \times G(E_2/K)$ tal que $\varphi(\sigma) = (\sigma_{|_{E_1}}, \sigma_{|_{E_2}})$ é injetiva. Se $E_1 \cap E_2 = K$, então φ é isomorfismo.*

O teorema acima determina uma decomposição para o grupo de galois $\varphi : G(E_1E_2/K)$ caso aconteça o isomorfismo. A prova deste teorema pode ser vista em [1].

3.1 Extensões Separáveis

Um polinômio $f(x) \in K[x]$ é *separável* sobre K se suas raízes em um fecho algébrico de K são distintas.

Teorema 3.1.1. *Sejam K e L corpos tais que L é algebricamente fechado e seja α um elemento algébrico sobre K. Se ψ é um homomorfismo de K em L, então o número de homomorfismos $\sigma : K(\alpha) \to L$, tal que $\sigma|_K = \psi$, é igual ao número de raízes distintas do polinômio minimal de α, $f(x) \in K[x]$.*

Seja E é uma extensão algébrica sobre K, e S o conjunto de todos os homomorfismos $\sigma : K(\alpha) \to L$ com $\alpha \in E$ e $\sigma|_K = \psi$, $\psi : K \to L$, homomorfismo. Então chamamos de *grau de separabilidade* a cardinalidade de S, isto é, o grau de separabilidade depende da extensão E sobre K. Denotamos por $[E : K]_s$ o grau de separabilidade de E sobre K.

Teorema 3.1.2. *Se $K \subset F \subset E$, onde E é uma extensão finita sobre K, então $[E : K]_s$ é finita e vale*

$$[E : K]_s = [E : F]_s \cdot [F : K]_s.$$

Além disso, $[E : K]_s \leq [E : K]$, onde $[E : K]$ é o grau da extensão.

Definição 3.1.3. Seja E uma extensão finita de K. E é dita *extensão separável* sobre K se $[E : K]_s = [E : K]$. O elemento α é dito *separável* sobre K se $K(\alpha)$ é separável sobre K.

Teorema 3.1.4. *O corpo E é separável sobre K se e somente se todo elemento $\alpha \in E$ é separável sobre K.*

Teorema 3.1.5. *Seja E uma extensão algébrica de K e sejam $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementos que geram essa extensão. Se α_i é separável sobre K para todo $i \in \{1, 2, \ldots, n\}$ então E é separável sobre K.*

Teorema 3.1.6. *Seja E uma extensão finita de K. Existe um elemento $\alpha \in E$ tal que $E = K(\alpha)$ se, e somente se, existe um número finito de corpos intermediários entre K e E que contém K. Se E é extensão separável, tal elemento α existe.*

O elemento α como acima é chamado *elemento primitivo.*

As definições e os resultados apresentados a seguir nos ajudarão no entendimento de um dos principais teoremas desta seção.

Definição 3.1.7. Seja $f(x) \in K[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. O polinômio $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1 \in K[x]$ é chamado de *derivada de* $f(x)$.

Para $f(x), g(x) \in K[x]$ valem as seguintes propriedades:

1. $(f(x) + g(x))' = f'(x) + g'(x)$
2. $(af(x))' = af'(x)$ para todo $a \in K$.
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Esta definição nos auxilia na verificação da existência de zeros múltiplos de um polinômio $f(x) \in K[x]$.

Teorema 3.1.8. *Um polinômio $f(x)$ sobre K tem zero múltiplo em alguma extensão E se e somente se $f(x)$ e $f'(x)$ tem fator comum, dadas as respectivas decomposições.*

O resultado acima é uma importante ferramenta quando necessitamos verificar a irredutibilidade de um polinômio com coeficientes em corpos de característica 0 e nos ajuda a compreender a prova de outro importante resultado, apresentado a seguir.

Teorema 3.1.9. *Seja $f(x)$ um polinômio irredutível sobre K. Se K tem característica zero, então $f(x)$ não tem zeros múltiplos. Se K tem característica $p \neq 0$, então $f(x)$ tem zero múltiplo se somente se $f(x) = g(x^p)$ para algum $g(x) \in K[x]$.*

Definição 3.1.10. Um corpo K é chamado de *corpo perfeito* se todo polinômio $f(x) \in K[x]$ é separável.

Podemos afirmar que K é corpo perfeito se tem característica zero ou se tem característica p e $K^p = \{a^p | a \in K\} = K$.

De fato, $f(x)$ pode ser fatorado em polinômios irredutíveis de graus menores, e se $f(x) \in K[x]$ com a característica de K igual a zero, pelo teorema acima, os irredutíveis da fatoração de $f(x)$ não possuem múltiplos zeros, isto é, $f(x)$ é separável. Agora, se K tem característica p, suponha $f(x) \in K[x]$ não separável. Então a decomposição de $f(x)$ trará polinômios com raízes múltiplas do tipo $g(x^p)$ e cada termo de g pode ser escrito como $a_k x^{pl_k}$, com $a_k \in K$ e $k \in \{1, 2, \ldots, n\}$. Como $K^p = K$, temos que $a_k x^{pl_k} = b_k^p x^{pl_k}$, com $b_k \in K$, logo $a_k x^{pl_k} = (b_k x^{l_k})^p$. Assim $f(x)$ é decomposto em polinômios do tipo $(h(x))^p$, e portanto esses polinômios não serão irredutíveis. Absurdo.

Dessa maneira podemos mostrar que todo corpo finito K é perfeito, basta tomar $\phi : K \to K$ tal que $\phi(x) = x^p$, com p primo, a característica de K, e mostrar que ϕ é um isomorfismo.

Teorema 3.1.11. *Seja $f(x)$ um polinômio irredutível sobre um corpo K e seja E o corpo de fatoração de $f(x)$ sobre K. Então todos os zeros de $f(x)$ em E tem a mesma multiplicidade.*

Teorema 3.1.12. *Seja K um corpo de característica zero e $f(x) \in K(x)$ um polinômio irredutível sobre K de grau maior ou igual a 1. Então f é separável.*

O teorema acima pode ser facilmente verificado com a aplicação do Teorema 3.1.8 e observado como consequência do Teorema 3.1.9.

Corolário 3.1.13. *Se K é corpo de característica zero, então toda extensão finita E sobre K é separável.*

Observação 3.1.14. Extensão de corpo finita sobre um corpo K que é normal e separável também é galoisina, pois ela pode ser formada pela adjunção de um elemento algébrico α (elemento primitivo) ao corpo K e, sendo assim, podemos tomar o polinômio minimal de

α, cujo grau é o mesmo da extensão, para que a extensão seja seu corpo de decomposição. De maneira recíproca, se uma extensão finita é galoisiana então é normal, pelo Teorema 3.0.6, e separável. (ver demonstração em [9])

3.2 Raízes da Unidade

Seja K um corpo. Se $\zeta \in K$ é tal que $\zeta^n = 1$, para algum $n \geq 1$ natural, então chamamos ζ de *raiz da unidade*.

Se K tem característica p, então a equação $x^{p^m} = 1$ tem somente uma raiz, 1, logo não existe p^m-ésima raiz da unidade além de 1.

Seja $n > 1,\ n \in \mathbb{N}$ e não divisível pela característica de K, então o polinômio $x^n - 1$ é separável pois a derivada $nx^{n-1} \neq 0$ e sua única raiz é zero, isto é, não tem raiz comum com $x^n - 1$. Portanto em uma extensão de decomposição de $x^n - 1$ sobre K, encontramos n raízes da unidade distintas.

O conjunto das n raízes da unidade formam um grupo cíclico cujo gerador é chamado de raiz n-ésima primitiva da unidade, denotado por ζ_n.

3.3 Extensões de Kummer

Consideremos agora o corpo de decomposição de $f(x) = x^p - a$ sobre um corpo K, com p primo. Assumiremos que o corpo K está contido em um fecho algébrico L e contém raiz p-ésima primitiva da unidade ζ_p. Seja α uma particular raiz p-ésima de a, então as raízes de $f(x)$ são

$$\alpha, \zeta_p\alpha, \zeta_p^2\alpha, \ldots, \zeta_p^{p-1}\alpha, \quad \text{pois} \quad (\zeta_p^n)^p = 1 \quad \forall \quad n.$$

Portanto o corpo de decomposição de $f(x)$ sobre K é gerado por uma única raiz α, ou seja, é o corpo $F = K(\alpha)$.

Proposição 3.3.1. *Seja K, um subcorpo do fecho algébrico L, que contém a raiz p-ésima primitiva da unidade ζ_p, e seja a um elemento de K tal que a não é uma potência de p em K. Então o corpo de decomposição de $f(x) = x^p - a$ tem grau p sobre K, e seu grupo de Galois é cíclico de ordem p.*

Demonstração. Seja F o corpo de decomposição de f sobre K e seja $\alpha \in F/K$ uma das raízes de f. Então existe um automorfismo $\psi \in G(F/K)$ tal que $\psi(\alpha) \neq \alpha$. Uma vez que as raízes de f são da forma $\zeta_p^i\alpha$, com $i = 0, \ldots, p-1$, $\psi(\alpha) = \zeta_p^r\alpha$, para algum $r \neq 0$, pois ψ deve levar raízes de f em raízes de f. Assim os automorfismos de $G(F/K)$ são encontrados da seguinte maneira:

$$\psi(\zeta_p^i\alpha) = \psi(\zeta_p^i) \cdot \psi(\alpha) = \psi(\zeta_p)^i\psi(\alpha),$$

como $\psi(\zeta_p) = \zeta_p$ pois $\zeta_p \in K$, temos

$$\psi(\zeta_p^i\alpha) = \psi(\zeta_p)^i\psi(\alpha) = \zeta_p^i\psi(\alpha) = \zeta_p^{i+r}\alpha$$

e ainda

$$\psi^2(\alpha) = \psi(\psi(\alpha)) = \psi(\zeta^r\alpha) = \psi_p^r\psi(\alpha) = \zeta_p^{2r}\alpha$$

e logo

$$\psi^j(\alpha) = \zeta_p^{jr}\alpha, \quad \text{para} \quad j = 0, 1, \ldots, p-1.$$

Como ζ_p é raiz p-ésima primitiva da unidade, a menor potência do automorfismo ψ que fixa α é ψ^p. Logo, ψ tem ordem pelo menos p em $G(F/K)$. Por outro lado, α é um dos elementos da base de F sobre K, e $f(\alpha) = 0$, logo $[F : K] \leq p$, pois f tem grau p. Como $G(F/K)$ tem no mínimo p elementos, $[F : K] = p$, $f(x)$ é irredutível sobre K e $G(F/K)$ é cíclico de ordem p. ∎

Teorema 3.3.2. *Sejam K um subcorpo de um fecho algébrico L, $\zeta_p \in L \setminus K$ uma raiz p-ésima primitiva da unidade e F uma extensão galoisiana sobre K de grau p. Então obtemos F pela adjunção, ao corpo K, de uma p-ésima raiz.*

Demonstração. Sendo $G(F/K)$ um grupo de ordem prima, é cíclico. Dado $\phi \in G(F/K)$, $\phi \neq Id$, então ϕ gera $G(F/K)$. Se tomarmos F como um espaço vetorial sobre K, temos que ϕ é um operador linear de K, pois

$$\phi(\alpha + \beta) = \phi(\alpha) + \alpha(\beta) \text{ e } \phi(c \cdot \alpha) = c\phi(\alpha) \ \forall \ \alpha, \beta \in F \text{ e } c \in K.$$

Como $G(F/K)$ é cíclico de ordem p, $\phi^p = Id$. Além disso, tomando λ um autovalor de ϕ, então $\lambda^p = 1$, isto é, λ é uma potência de ζ_p. Os autovalores pertencem a L e pelo menos um deles é diferente de 1. De fato, seja T a matriz correspondente ao operador linear ϕ, então temos que $T^p = Id$. Assim, temos que T é diagonalizável e portanto existe uma

matriz diagonal A semelhante a T. Como $T \neq Id$, $A \neq Id$ e assim alguma entrada da diagonal de A é diferente de 1.

Escolhemos α autovetor com autovalor $\zeta_p^i \neq 1$. então $\phi(\alpha) = \zeta_p^i \alpha$ e portanto

$$\phi(\alpha^p) = \phi(\alpha)^p = (\zeta_p^i \alpha)^p = (\zeta_p^i)^p \alpha^p = \alpha^p,$$

logo ϕ fixa α^p. Como ϕ gera $G(F/K)$, o elemento $\alpha^p \in F|_{G(F/K)}$ (Corpo fixo de $G(F/K)$ em L) que é o próprio K. Portanto α é um elemento de F cuja p-ésima potência está em K. Já que $\phi(\alpha) = \zeta_p^i \alpha$ e $\zeta_p^i \notin K$, então $\phi(\alpha) \neq \alpha$ e o elemento $\alpha \notin K$. Como $[F : K]$ é primo, α gera F, ou seja $F = K(\alpha)$.

■

Definição 3.3.3. A extensão F, como no Teorema acima é frequentemente chamada de *extensão de kummer*.

3.4 Extensões Inseparáveis

Dizemos que uma extensão de corpos é Inseparável se não for Separável.

Proposição 3.4.1. *Seja α algébrico sobre K, $\alpha \in L$ fecho algébrico de K, e seja $f(x)$ o polinômio minimal de α sobre K. Se K tem característica zero, então todas as raízes de $f(x)$ tem multiplicidade 1 (f é separável em L). Se K tem característica $p > 0$, então existe um inteiro $\mu \geq 0$ tal que toda raiz de $f(x)$ tem multiplicidade p^μ. Além disso*

$$[K(\alpha) : K] = p^\mu [K(\alpha) : K]_s$$

e α^{p^μ} é separável sobre K.

Corolário 3.4.2. *Para alguma extensão finita E de K, o grau de separabilidade $[E : K]_s$ divide o grau da extensão $[E : K]$. O quociente é 1 se a característica de K é zero, e uma potência de p se a característica de K for $p > 0$.*

Definição 3.4.3. Chamamos de *grau de inseparabilidade* o quociente $[E : K]/[E : K]_s$ e o denotamos por $[E : K]_i$.

Corolário 3.4.4. *Uma extensão finita é separável se e somente se $[E : K]_i = 1$.*

Corolário 3.4.5. *Se $E \supset F \supset K$ são duas extensões finitas, então $[E : K]_i = [E : F]_i [F : K]_i$.*

Definição 3.4.6. Um elemento α algébrico sobre K, corpo de característica $p > 0$, é *puramente inseparável sobre* K se existe um inteiro $n \geq 0$ tal que α^{p^n} é um elemento de K.

Tomando a extensão algébrica E sobre K pode-se verificar também as seguintes afirmações equivalentes: (K corpo de característica $p > 0$)

i) $[E : K]_s = 1$

ii) Todo elemento α de E é puramente inseparável sobre K.

iii) Para todo elemento $\alpha \in E$, o polinômio minimal de α sobre K é do tipo $f(x) = x^{p^n} - a$ para algum $n \geq 0$ e $a \in K$.

iv) Existe um conjunto de geradores $\{\alpha_i\}_{i \in I}$ de E sobre K tal que cada α_i é puramente inseparável sobre K.

Definição 3.4.7. A extensão E sobre K que satisfaz alguma das propriedades acima é chamada de *extensão puramente inseparável*.

3.5 Norma e Traço

Seja E uma extensão finita de K tal que $[E : K]_s = r$. Vimos que $[E : K]_i = p^\mu$ se a característica de K é $p > 0$ e $[E : K]_i = 1$ se a característica de K é zero.

Se α é um elemento de E e considere $\sigma_1, \ldots, \sigma_r$ os homomorfismos distintos de E sobre L, fecho algébrico de K. Definimos a *norma* de E sobre K como

$$\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_K^E(\alpha) = \prod_{v=1}^{r} \sigma_v(\alpha)^{[E:K]_i} = \left(\prod_{v=1}^{r} \sigma_v(\alpha) \right)^{[E:K]_i}.$$

Também definimos traço:

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_K^E(\alpha) = [E : K]_i \sum_{v=1}^{r} \sigma_v(\alpha).$$

O traço é igual a zero se $[E : K]_i > 1$, em outras palavras, se E/K não é separável. (Basta observar que $[E : K]_i = p^\mu$ para algum μ natural.)

Se E é separável sobre K, temos

$$\mathrm{N}_K^E(\alpha) = \prod_{\sigma} \sigma(\alpha)$$

onde o produto é dado usando os distintos homomorfismos de E em L sobre K.

Se E/K é separável, então

$$\mathrm{Tr}_K^E(\alpha) = \sum_\sigma \sigma(\alpha).$$

Teorema 3.5.1.

- *Seja E/K uma extensão finita. Então a norma N_K^E é um homomorfismo multiplicativo de E^* em K^* e o traço é um homomorfismo aditivo de E em K.*

- *Se $E \supset F \supset K$ é uma cadeia de corpos, então*

$$\mathrm{N}_K^E = \mathrm{N}_F^E \circ \mathrm{N}_K^F \quad e \quad \mathrm{Tr}_K^E = \mathrm{Tr}_F^E \circ \mathrm{Tr}_K^F,$$

  isto é, possuem a propriedade transitiva.

- *Se $E = K(\alpha)$ e $f(x)$ for o polinômio minimal de α sobre K, então*

$$\mathrm{N}_K^{K(\alpha)}(\alpha) = (-1)^n a_0 \quad e \quad \mathrm{Tr}_K^{K(\alpha)}(\alpha) = -a_{n-1},$$

  onde n é o grau de $f(x)$, a_0 e a_{n-1} são, respectivamente, termo independente de $f(x)$ e o coeficiente de x^{n-1} em $f(x)$.

Exemplo 3.5.2. Tomamos $\mathrm{N} : \mathbb{C}^* \to \mathbb{R}^*$, a norma de $\mathbb{C}$ sobre $\mathbb{R}$, $\mathbb{C}$ tem característica 0, portanto separável, e $\mathrm{N}(a+bi) = \sigma_1(a+bi).\sigma_2(a+bi)$ (temos dois automorfismos distintos, um que leva i em i e outro que leva i em $-i$). Logo $\mathrm{N}(a+bi) = a^2 + b^2$. É fácil verificar que N de fato é um homomorfismo.

Vemos também que o traço $\mathrm{Tr} : \mathbb{C}^+ \to \mathbb{R}^+$, onde $\mathbb{C}^+$ e $\mathbb{R}^+$ são grupos aditivos, é homomofismo e $\mathrm{Tr}(a+bi) = \sigma_1(a+bi) + \sigma_2(a+bi) = 2a$

Tome agora a transformação linear $m_Z : \mathbb{C} \to \mathbb{C}$ tal que $m_Z(W) = (W) \cdot Z$, $Z = (a+bi) \in \mathbb{C}$ é fácil verificar que a matriz dessa transformação linear na base canônica de $\mathbb{C}$ é $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

E assim verificamos que $\mathrm{N}(a+bi) = det\ A$ e $\mathrm{Tr}(a+bi) = Tr\ A$.

Em geral, dada a extensão L/K, a norma $\mathrm{N} : L^* \to K^*$ não é sobrejetora e o estudo do grupo quociente $K^*/\mathrm{N}(L^*)$ é um problema importante na teoria dos números.

3.6 Extensões Cíclicas

Uma extensão finita E é chamada de *cíclica* sobre um corpo K se E for uma extensão galoisiana e se seu grupo de Galois for um grupo cíclico.

Teorema 3.6.1. *Seja E uma extensão Galoisiana de K e F extensão de K tal que $K \subset F \subset E$. Então F é extensão normal de K se e somente se, $G(E/F)$ é subgrupo normal de $G(E/K)$. E ainda, a aplicação $\varphi : G(E/K) \to G(F/K)$ é um homomorfismo sobrejetor onde $\varphi(\sigma) = \sigma_{|_F}$ e o núcleo de φ é $G(E/F)$. Isto é , $G(F/K) \simeq G(E/K)/G(E/F)$.*

Corolário 3.6.2. *Seja E uma extensão cíclica e F uma extensão tal que $K \subset F \subset E$. Então F é extensão Galoisiana sobre K também cíclica.*

Teorema 3.6.3 (Teorema 90 de Hilbert)**.** *Seja E uma extensão cíclica de grau n sobre um corpo K, e $G(E/K)$ o seu grupo de Galois. Seja β um elemento de E. Então a norma $\mathrm{N}_K^E(\beta) = 1$ se e somente se existe um elemento $\alpha \neq 0$ em E tal que $\beta = \alpha/\sigma(\alpha)$ onde σ é o isomorfismo gerador de $G(E/K)$.*

Demonstração. Se considerarmos que tal elemento α existe, então se vermos a norma como um homomorfismo podemos obter da igualdade $\beta = \alpha/\sigma(\alpha)$ a seguinte igualdade $\mathrm{N}(\beta) = \mathrm{N}(\alpha/\sigma(\alpha))$ o que implica em $\mathrm{N}(\beta) = \mathrm{N}(\alpha)/\mathrm{N}(\sigma(\alpha))$. Mas $\mathrm{N}(\sigma(\alpha)) = \sigma_1(\sigma(\alpha)) \cdot \sigma_2(\sigma(\alpha)) \ldots \sigma_n(\sigma(\alpha))$ pois o grau de inseparabilidade é 1.

Como σ é gerador de $G(E/K)$, $\sigma_i = \sigma^j$, para $i = 1, \ldots, n$ e para algum $j \in \{0, \ldots, n-1\}$. Além disso $\sigma_i \circ \sigma = \sigma_k$, para alguma $k \in \{0, \ldots, n\}$, ou seja $\mathrm{N}(\sigma(\alpha)) = \mathrm{N}(\alpha)$ e portanto $\mathrm{N}(\beta) = 1$.

Antes de terminar a demonstração do teorema, vamos definir caráter de um grupo G sobre um corpo K e anunciar um resultado importante.

Definição 3.6.4. *Caráter* de um monóide G sobre um corpo K é um homomorfismo $f : G \to K^*$.

Teorema 3.6.5 (Artin)**.** *Seja G um monóide e K um corpo e $f_1, f_2, \ldots, f_n$ caráteres distintos de G sobre K. Esses caráteres formam um conjunto de elementos linearmente independentes sobre K.*

Demonstração. Suponha a relação $a_1 f_1 + \ldots + a_n f_n = 0$, com $a_i \in K$, $i = 1, \ldots, n$, de forma que nem todos $a_i's$ sejam nulos. Temos que no mínimo dois $a_i's$ são diferentes de

zero. Tomando o menor n possível tal que os $a_i's$ sejam diferentes de zero, $n \geq 2$. Como f_1 e f_2 são distintos, existe $z \in G$ tal que $f_1(z) \neq f_2(z)$ e ainda

$$\begin{aligned} a_1 f_1(z) + \ldots + a_n f_n(z) &= 0 \\ a_1 f_1(xz) + \ldots + a_n f_n(xz) &= 0 \ \forall \ x \in G \\ a_1 f_1(z) f_1(x) + \ldots + a_n f_n(z) f_n(x) &= 0 \end{aligned}$$

pois f_i é homomorfismo. Se dividirmos a relação acima por $f_1(z)$ teremos

$$a_1 f_1 + a_2 \frac{f_2(z)}{f_1(z)} f_2 \ldots + a_n \frac{f_n(z)}{f_1(z)} f_n = 0$$

(usamos simplesmente f_i no lugar de $f_i(x) \ \forall \ x \in G$). Subtraindo $a_1 f_1 + \ldots + a_n f_n = 0$, temos

$$\left(a_2 \frac{f_2(z)}{f_1(z)} - a_2 \right) f_2 + \ldots + \left(a_n \frac{f_n(z)}{f_1(z)} - a_n \right) f_n = 0$$

onde $a_i \frac{f_i(z)}{f_1(z)} - a_i = \beta_i \ \in K$, pois $f_i(z), \ f_1(z) \ \in K, \ \forall \ i = 2, 3, \ldots, n$. Observe que, pelo menos, $\beta_2 \neq 0$ pois $\dfrac{f_2(z)}{f_1(z)} \neq 1$. Logo obtemos $\beta_2 f_2 + \ldots + \beta_n f_n = 0$, com $n-1$ termos e $\beta_i's$ não simultaneamente nulos, isto é, obtemos um relação com menos termos que a primeira relação tomada. Absurdo, pois supomos n o menor possível.

Portanto, $a_1 f_1 + \ldots + a_n f_n = 0 \ \Leftrightarrow \ a_i = 0 \ \forall \ i = 1, 2, \ldots, n$. Logo $f_1, \ldots, f_n$ são L.I sobre K.

■

Voltando à demonstração do teorema (3.6.3), temos $G(E/K)$ cíclico gerado por σ. Sejam

$$\sigma_0 = \sigma^n = Id, \ \sigma_1 = \sigma, \ \sigma_2 = \sigma^2, \ldots, \sigma_{n-1} = \sigma^{n-1}$$

os elementos de $G(E/K)$. Cada σ_i é um carácter de E sobre E^* e

$$Id + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3 + \ldots + \beta\sigma(\beta) \cdot \ldots \cdot \sigma^{n-2}(\beta)\sigma^{n-1}$$

é uma aplicação não identicamente nula, pois $Id, \sigma, \ldots, \sigma^{n-1}$ são L.I. (teorema (3.6.5)) e

$$1, \beta, \beta\sigma(\beta), \ldots, \beta\sigma(\beta) \cdot \ldots \cdot \sigma^{n-2}(\beta)$$

pertencem a E.

Portanto, existe $\theta \in E$ tal que o elemento

$$\alpha = \theta + \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \ldots + \beta\sigma(\beta) \cdot \ldots \cdot \sigma^{n-2}(\beta)\sigma^{n-1}(\theta) \neq 0.$$

Assim

$$\beta\sigma(\alpha) = \beta \cdot \sigma(\theta) + \beta \cdot \sigma(\beta) \cdot \sigma^2(\theta) + \ldots + \beta \cdot \sigma(\beta) \cdot \sigma^2(\beta) \cdot \ldots \cdot \sigma^{n-1}(\beta) \cdot \sigma^n(\theta).$$

Como $\sigma^n(\beta) = Id(\beta) = \beta$,

$$\sigma(\beta) \cdot \sigma^2(\beta) \cdot \ldots \cdot \sigma^{n-1}(\beta) \cdot \sigma^n(\beta) = N(\beta) = 1,$$

$\sigma^n(\theta) = Id(\theta) = \theta$, temos que

$$\beta\sigma(\theta) = \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \ldots + \beta\sigma(\beta) \cdot \ldots \cdot \sigma^{n-2}(\beta)\sigma^{n-1}(\theta) + \theta = \alpha$$

e $\beta\sigma(\alpha) = \alpha$, então $\beta = \alpha/\sigma(\alpha)$.

■

Exemplo 3.6.6. Tome a extensão $\mathbb{Q}(i)/\mathbb{Q}$ galoisiana. Temos que $G(\mathbb{Q}(i)/\mathbb{Q}) = \{Id, \sigma\}$ tal que $\sigma(i) = -i$. Agora, tome $\beta = (x+iy) \in \mathbb{Q}(i)$. Temos que $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(i)}(\beta) = [Id(\beta).\sigma(\beta)]^{[\mathbb{Q}(i):\mathbb{Q}]_i}$, como $\mathbb{Q}$ tem característica 0, $[\mathbb{Q}(i) : \mathbb{Q}]_i = 1$ e $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(i)}(\beta) = \beta.\sigma(\beta) = (x + iy).(x - iy) = x^2 + y^2$.

Se a norma é igual a 1 significa que o par $(x, y) \in \mathbb{R}^2$ é ponto racional no círculo unitário. Nesse caso, o Teorema 3.6.3 garante a existência de $\alpha \neq 0$, $\alpha \in \mathbb{Q}(i)$, tal que $\beta = \dfrac{\alpha}{\sigma(\alpha)}$. Sendo $\alpha = a + bi$, podemos supor a e b inteiros (multiplicamos por um inteiro apropriado, por exemplo o produto dos denominadores de a e b, ou o mmc deles) e temos $\beta = \dfrac{a+bi}{a-bi} = \dfrac{a^2+2abi-b^2}{a^2+b^2}$, e portanto encontrar $\beta \in \mathbb{Q}(i)$ que satisfaz $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(i)}(\beta) = 1$ é encontrar a solução racional $\left(\dfrac{a^2-b^2}{a^2+b^2}, \dfrac{2ab}{a^2+b^2}\right)$ que por sua vez corresponde à tripla ou terna pitagórica $(a^2 - b^2, 2ab, a^2 + b^2)$.

No teorema abaixo deve-se observar o fato de o corpo K ter característica $p \geqslant 0$, isto mostra o quanto esse resultado é abrangente e portanto de fundamental importância para a solubilidade por radicais, como veremos na próxima seção.

Teorema 3.6.7. *Seja K um corpo de característica $p \geqslant 0$ e assuma que exista uma raiz n-ésima primitiva da unidade em K, com n primo com p.*

i) *Seja E uma extensão cíclica de grau n. Então existe $\alpha \in E$ tal que $E = K(\alpha)$ e α satisfaz a equação $x^n - a = 0$ para algum $a \in K$.*

ii) *Por outro lado, seja $a \in K$. Seja α uma raiz de $x^n - a = 0$. Então $K(\alpha)$ é cíclico sobre K, de grau d, d divisor de n e $\alpha^d \in K$.*

Demonstração. Seja ζ a raiz n-ésima primitiva da unidade em K e seja $G(E/K)$ o grupo cíclico.

Temos que $\mathrm{N}(\zeta^{-1}) = 1$. Aplicando o Teorema (3.6.3), temos que $\exists\ \alpha \in E$ tal que $\zeta^{-1} = \alpha/\sigma(\alpha)$, então $\sigma(\alpha) = \zeta\alpha$.

Como ζ está em K,

$$\begin{aligned}
\sigma^i(\alpha) &= \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma(\alpha)}_{i\ vezes} \\
&= \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{i-1\ vezes}(\zeta\alpha) \\
&= \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{i-2\ vezes}(\zeta\sigma(\alpha)) \\
&= \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{i-2\ vezes}(\zeta^2\alpha) \\
&= \sigma(\zeta^{i-1}\alpha) = \zeta^{i-1}\sigma(\alpha) = \zeta^{i-1}\zeta\alpha = \zeta^i\alpha
\end{aligned}$$

para $i = 1, \ldots, n$.

Portanto, os elementos $\zeta^i\alpha$ são as conjugações distintas de α sobre K e então $K(\alpha)$ tem, no mínimo, grau n. Como $[E : K] = n$, segue que $E = K(\alpha)$.

Além disso,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \zeta^n\alpha^n = \alpha^n,$$

isto é, α^n é fixo por σ e por todas as potências de σ. Logo $\alpha^n \in K$ e tomando $\alpha^n = a$, α satisfaz $x^n - a = 0$.

Por outro lado, seja $a \in K$ e α raiz de $x^n - a = 0$. Então $\zeta^i\alpha$ também é raiz de $x^n - a = 0$, para todo $i = 1, \ldots, n$. De fato,

$$(\zeta^i\alpha)^n - a = (\zeta^n)^i\alpha^n - a = \alpha^n - a = 0,$$

portanto todas as raízes de $x^n - a$ estão em $K(\alpha)$, pois $\zeta^i \in K\ \forall\ i = 1, \ldots, n$ e assim $K(\alpha)$ é Galoisiana.

Seja $G(K(\alpha)/K)$, o grupo de Galois. Então

$$\sigma \in G(K(\alpha)/K)\ \Rightarrow\ (\sigma(\alpha))^n - a = \sigma(\alpha^n) - a = a - a = 0,$$

isto é, $\sigma(\alpha)$ é uma raiz de $x^n - a$. Se $\sigma(\alpha) = \omega_\sigma\alpha$, $\omega_\sigma^n\alpha^n - a = 0$ como $\alpha^n = a$, $\omega_\sigma^n = 1$, isto é ω_σ é uma raiz n-ésima da unidade.

Uma aplicação φ que leva $\sigma \mapsto \omega_\sigma$ é um homomorfismo de $G(K(\alpha)/K)$ no grupo das raízes n-ésimas da unidade, que é cíclico. Como φ é injetiva, $\varphi(G(K(\alpha)/K))$ é subgrupo

de um grupo cíclico de ordem d, com d divisor de n. Se σ é o gerador de $G(K(\alpha)/K)$, então ω_σ é a raiz d-ésima primitiva da unidade. No que temos,

$$\sigma(\alpha^d) = (\sigma(\alpha))^d = (\omega_\sigma \alpha)^d = \alpha^d$$

isto é α^d é fixo por σ e portanto fixo por $G(K(\alpha)/K)$. Logo $\alpha^d \in K$.

■

Teorema 3.6.8 (Forma aditiva do Teorema 90 de Hilbert)**.** *Seja K um corpo, E um extensão cíclica sobre K, $[E:K] = n$. Seja σ o gerador de $G(E/K)$ e $\beta \in E$. O traço $\mathrm{Tr}_K^E(\beta)$ é igual a 0, se e só se, existir $\alpha \in E$ tal que $\beta = \alpha - \sigma(\alpha)$.*

($\Leftarrow$) Se $\beta = \alpha - \sigma(\alpha)$, então

$$\mathrm{Tr}_K^E(\beta) = [E:K]_i \sum_i^n \sigma_j(\beta),$$

$[E:K]_i = 1$ pois E é Galoisiana, $\sigma_j \in G(E/K)\ \forall\ j \in \{1, \ldots, n\}$. Considere

$$\sigma_1 = \sigma, \sigma_2 = \sigma^2, \ldots, \sigma_{n+1} = \sigma_1$$

$$\begin{aligned}
\mathrm{Tr}_K^E(\beta) &= \sigma_1(\beta) + \sigma_2(\beta) + \ldots + \sigma_n(\beta) \\
&= \sigma_1(\alpha - \sigma(\alpha)) + \sigma_2(\alpha - \sigma(\alpha)) + \ldots + \sigma_n(\alpha - \sigma(\alpha)) \\
&= \sigma_1(\alpha) - \sigma_2(\alpha) + \sigma_2(\alpha) - \sigma_3(\alpha) + \ldots + \sigma_n(\alpha) - \sigma_1(\alpha) = 0.
\end{aligned}$$

($\Rightarrow$) Se $\mathrm{Tr}_K^E(\beta) = 0$, considere $\theta \in K$ tal que $\mathrm{Tr}_K^E(\theta) \neq 0$ e seja

$$\alpha = \frac{1}{\mathrm{Tr}(\theta)}[\beta\sigma(\theta) + (\beta + \sigma(\beta))\sigma^2(\theta) + \ldots + (\beta + \sigma(\beta) + \ldots + \sigma^{n-2}(\beta)) \cdot \sigma^{n-1}(\theta)].$$

Então

$$\begin{aligned}
\sigma(\alpha) = \frac{1}{\mathrm{Tr}(\theta)}[\sigma(\beta)\sigma^2(\theta) + \sigma(\beta)\sigma^3(\theta) &+ \sigma^2(\beta)\sigma^3(\theta) + \ldots \\
&+ \sigma(\beta)\sigma^n(\theta) + \sigma^2(\beta)\sigma^n(\theta) + \ldots + \sigma^{n-1}(\beta)\sigma^n(\theta)].
\end{aligned}$$

Logo $\alpha - \sigma(\alpha) = \beta + \frac{\sigma^n(\theta)}{Tr(\theta)} \cdot \mathrm{Tr}(\beta)$ e

$$\beta = \alpha - \sigma(\alpha)$$

observe que $\alpha \in E$ pois β e $\sigma(\alpha)\ \in E$.

■

O seguinte teorema assemelha-se ao Teorema 3.3.2 e ambos podem ter em suas demonstrações elementos das formas multiplicativa e aditiva do Teorema 90 de Hilbert. Além disso, mostra a possibilidade de outra raiz de polinômio em corpos de característica $p > 0$. Tal raiz será considerada quando avaliarmos a solubilidade por radicais de uma extensão.

Teorema 3.6.9 (Artin-Schreier)**.** *Seja K um corpo de característica p.*

i) *Seja E uma extensão cíclica de K de grau p. Então existe $\alpha \in E$ tal que $E = K(\alpha)$ e α satisfaz a equação $x^p - x - a = 0$ para algum $a \in K$.*

ii) *Por outro lado, dado $a \in K$, o polinômio $f(x) = x^p - x - a$ tem uma raiz em K, nesse caso todas as raízes estão em K, ou então $f(x)$ é irredutível. Neste último caso, se α é raiz, $K(\alpha)$ é cíclico de grau p sobre K.*

Demonstração. Seja $-1 \in K$, observe que se σ é gerador do grupo de galois $G(E/K)$, então $\sigma_i(-1) = -1,\ \forall\ i \in \{1, \ldots, p\}$ e, por conseguinte,

$$\mathrm{Tr}_K^E(-1) = \sigma_1(-1) + \sigma_2(-1) + \ldots + \sigma_p(-1) = p \cdot (-1) = 0.$$

Observação: Novamente, consideramos

$$\sigma_1 = \sigma, \sigma_2 = \sigma \circ \sigma, \ldots, \sigma_p = \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{p\ vezes},$$

já que $G(E/K)$ é cíclico.

Pelo Teorema (3.6.8), temos que $\exists\ \alpha \in E$ tal que $-1 = \alpha - \sigma(\alpha)$, ou seja, $\sigma(\alpha) = \alpha + 1$. Logo, temos que

$$\sigma_i(\alpha) = \sigma_{i-1}(\alpha + 1) = \sigma_{i-1}(\alpha) + 1 = \sigma_{i-2}(\alpha + 1) + 1 = \sigma_{i-2}(\alpha) + 2 = \ldots = \alpha + i$$
$$\forall\ i \in\ \{1, \ldots, p\}$$

Como α tem p conjugações, isto é, $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_p(\alpha)$, que são raízes do polinômio minimal de α, logo $[K(\alpha) : K] \geq p$, como $[E : K] = p$ e $\alpha \in E$, $K(\alpha) = E$.

Além disso, temos que

$$\begin{aligned}
\sigma(\alpha^p - \alpha) &= \sigma(\alpha^p) - \sigma(\alpha) \\
&= \sigma(\alpha)^p - \sigma(\alpha) \\
&= (\alpha + 1)^p - (\alpha + 1) \\
&= \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha
\end{aligned}$$

Mas se $\alpha^p - \alpha$ é fixo por σ, temos que $(\alpha^p - \alpha) \in K$. Tomemos $a = \alpha^p - \alpha$ e concluímos que α é a raiz de

$$x^p - x - a = 0,$$

concluindo o item *i)*.

Para provar o item *ii)* tome $a \in K$ e considere α uma raiz de $f(x)$, então

$$\alpha^p - \alpha - a = 0$$

e portanto

$$(\alpha+i)^p - (\alpha+i) - a = \alpha^p + i^p - \alpha - i - a = (\alpha^p - \alpha - a) + i^p - i = 0, \ \forall\, i \in \{1, 2, ..., p-1\},$$

logo $f(x)$ tem p raízes distintas. Devemos lembrar que todo corpo de característica p possui uma cópia de $\mathbb{F}_p$ e os elementos inteiros $i = 1, 2, ..., p$ em K são vistos como elementos de $\mathbb{F}_p$, por isso $i^p = i$ para todo i. Observemos também que se alguma raiz de $f(x)$ está em K, então todas as outras raízes também estarão, pois $\alpha + i \in K \Rightarrow \alpha \in K$ para todo $i \in K$. Supondo que nenhuma das raízes estão em K, então o polinômio $f(x)$ é irredutível. De fato, se $f(x)$ não for irredutível poderíamos escrever $f(x) = g(x)h(x)$, com $g(x)$ e $h(x) \in K[x]$ e o grau de $g(x)$ é igual a um d com $1 \leq d < p$. Temos ainda que $g(x)$ é da forma

$$g(x) = (x - (\alpha + i_1))(x - (\alpha + i_2)) \dots (x - (\alpha + i_d))$$

com $i_j = 1, 2, \dots, p$ e $j = 1, 2, \dots, d$ e portanto $g(x)$ terá o termo x^{d-1} com coeficiente igual a

$$\sum_{j=1}^{d} (-(\alpha + i_j)) = -d\alpha + l$$

para algum inteiro l. Como $d \neq 0$ em K e $(-d\alpha + l) \in K$. temos que $\alpha \in K$, absurdo!

Logo $f(x)$ é irredutível. Agora, adjuntando α a K, temos que $K(\alpha)$ contém todas as raízes de $f(x)$, logo $K(\alpha)$ é normal e galoisiana. Seja $G(K(\alpha)/K)$ o grupo de Galois correspondente. Então $\sigma(\alpha) = \sigma(\alpha + 1)$ para algum $\sigma \in G(K(\alpha)/K)$, pois $\alpha + 1$ também é raiz de $f(x)$, assim

$$\sigma_i(\alpha) = \sigma_{i-1}(\alpha + 1) = \sigma_{i-1}(\alpha) + 1 = \ldots = \alpha + i$$

$\forall\, i \in \{1, \dots, p\}$, ou seja, $G(K(\alpha)/K)$ é gerado por σ e portanto $K(\alpha)$ é extensão cíclica.

■

3.7 Solubilidade por Radicais

Apresentaremos agora algumas definições e resultados importantes da teoria de grupos que nos auxiliarão nas demosntrações dos principais teoremas deste trabalho.

Definição 3.7.1. Uma cadeia de subgrupos de um grupo G do tipo

$$G_0 \subset G_1 \subset \ldots \subset G_n = G$$

é dita *abeliana* (respect.*cíclica*) se cada elemento G_i é subgrupo normal de G_{i+1} e o grupo quociente G_{i+1}/G_i é abeliano (respect. cíclico).

Definição 3.7.2. Um grupo G é chamado de *grupo solúvel* se existe uma cadeia de subgrupos

$$\{e\} = H_0 \subset H_1 \subset \ldots \subset H_n = G$$

tal que H_i é subgrupo normal de $H_{i+1} \ \forall \ i \in \{0, 1, \ldots, n-1\}$ e o grupo quociente H_{i+1}/H_i é abeliano.

Pelas definições acima podemos perceber que um Grupo solúvel deve adminitir uma cadeia abeliana de subgrupos tais que o menor elemento dessa cadeia é o subgrupo $\{e\}$.

Verifica-se facilmente que:

- Todo grupo abeliano é solúvel.
- Grupos simples (um grupo G é chamado de simples se seus únicos subgrupos normais são $\{e\}$ e G) não abelianos não são solúveis.
- Grupo Diedral e grupos cuja ordem é potência de primo são grupos solúveis.

Definição 3.7.3. Dada uma cadeia de subgrupos de um grupo G, um refinamento dessa cadeia é uma nova cadeia obtida pela inserção de um número finito de subgrupos.

Proposição 3.7.4. *Seja G um grupo finito. Uma cadeia abeliana de subgrupos de G admite um refinamento cíclico. Seja G um grupo finito solúvel, então G adminite uma cadeia cíclica de subgrupos cujo o último elemento é $\{e\}$.*

Quando se prova a primeira afirmação da proposição acima, consequentemente provamos a segunda. A prova dessa proposição mostra a existência de uma cadeia finita e cíclica de $G' = G/X$ onde X é o grupo cíclico gerado por um elemento não nulo $x \in G$. Enxergando

G' como aplicação, teremos uma cadeia cíclica de G garantida pela inversa dessa aplicação. Por fim, um refinamento dessa cadeia de G pode ser feita com a inserção do subgrupo $\{e\}$.

Teorema 3.7.5. *Seja G um grupo e H um subgrupo normal. Então G é solúvel se e somente se H e G/H são solúveis.*

Demonstração. Suponha G um grupo solúvel e H um subgrupo normal de G. Seja

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

a cadeia de subgrupos dada pela solubilidade de G e seja $H_i = H \cap G_i$. Então H_i é normal em H_{i+1}. Temos então uma injetividade $H_{i+1}/H_i \to G_{i+1}/G_i$ e como G_{i+1}/G_i é abeliano, H_{i+1}/H_i é abeliano e H é solúvel.

Considere o homomorfismo canônico $\pi : G \to G/H$. Temos $\pi|_{G_i}$, tal que $\pi(G_i) = \overline{G_i} \subset G/H$, homomorfismo sobrejetor para todo $i \in \{0, \ldots, n\}$. Assim podemos provar facilmente que G solúvel implica em G/H solúvel.

Reciprocamente, considerando o mesmo homomorfismo π, mostramos que se G/H é solúvel e $\overline{G_i} \subset G/H$ tal que $\overline{G_i} = G_i/H$ teremos $H = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$. Como $(G_{i+1}/H)/(G_i/H)$ é abeliano, $\overline{G_{i+1}}/\overline{G_i}$ é abeliano e isomorfo a G_{i+1}/G_i, isto é, também abeliano. Como H é solúvel, teremos G solúvel.

■

Teorema 3.7.6. *Se $n \geq 5$, então S_n não é solúvel.*

Demonstração. Suponha $H \subset S_n$ um subgrupo que contém todos os 3-ciclos de S_n e N subgrupo normal de H. Se H/N é abeliano, então N contém todos os 3-ciclos. De fato, sejam $\sigma = (ijk)$, $\tau = (krs) \in S_n$, 3-ciclos com i, j, k, r e s inteiros distintos ($n \geq 5$ garante a existência desses dois 3-ciclos). Observe que o comutador $\sigma\tau\sigma^{-1}\tau^{-1} = (rki)$.

Seja H^C o conjunto dos comutadores de H, como H/N é abeliano, $H^C \subset N$. E assim, como i, j, k, r e s são arbitrários, todos os 3-ciclos estão em N. De fato, tome $a, b \in H$ então

$$aN, bN \in H/N \;\Rightarrow\; aN \cdot bN = bN \cdot aN \;\Rightarrow\; abN = baN$$

então $a \sim b$ o que implica que $ab(ba)^{-1} \in N$ mas $(ba)^{-1} = a^{-1}b^{-1}$. Logo, $aba^{-1}b^{-1} \in N$. Como a e b são arbitrários em H concluímos que $H^C \subset N$.

Agora, se S_n é solúvel existe a cadeia de subgrupos

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_m = S_n$$

com H_i normal em H_{i+1}, $i \in \{0, \ldots, m-1\}$ e H_{i+1}/H_i abeliano. $H_m = S_n$ contém todos os 3-ciclos, então H_{m-1} também contém todos os 3-ciclos e, por recorrência, concluiremos que H_0 contém todos os 3-ciclos, que é um absurdo.

■

Alguns resultados a seguir não serão demontrados, contudo o leitor poderá encontrar as demonstrações com detalhes nos livros indicados nas referências.

Definição 3.7.7. Seja K um corpo e $f(x) \in K[x]$, então $f(x)$ é *solúvel por radicais* sobre K se $f(x)$ pode ser decomposto em alguma extensão $K(a_1, \ldots, a_n)$ de K e existem inteiros $l_1, l_2, \ldots, l_n$ tais que $a_1^{l_1} \in K$, $a_2^{l_2} \in K(a_1)$, ..., $a_n^{l_n} \in K(a_1, \ldots, a_{n-1})$.

Podemos também dizer que um polinômio em $K[x]$ é solúvel por radicais se todo zero ou raiz desse polinômio pode ser escrito como expressão que envolva elementos de K e as operações de soma, subtração, multiplicação e aplicação de radicais. De fato, basta observar que se α é uma raiz de $f(x)$, solúvel por radicais sobre K, então $\alpha \in K(a_1, \ldots, a_n)$, isto é, $\alpha = f(a_1, \ldots, a_n)$ e ainda

$$b = a_i^{l_i} \ \in \ K(a_1, \ldots, a_{i-1}) \quad \Rightarrow \quad a_i = \sqrt[l_i]{b}.$$

Definição 3.7.8. Uma extensão F de um corpo K é chamada de *solúvel por radicais* se é separável e se existe uma extensão finita E de K tal que $K \subset F \subset E$ e E pode ser decomposto na seguinte cadeia

$$K = E_0 \subset E_1 \subset \ldots \subset E_m = E$$

onde cada extensão E_{i+1}, $i \in \{0, 1, \ldots, m-1\}$ é obtida:

- com a adjunção de uma raiz da unidade em E_i.
- com a adjunção de uma raiz de um polinômio $x^n - a \in E_i[x]$, com n primo com a característica de E_i.

- com a adjunção de uma raiz de um polinômio $x^p - x - a \in E_i[x]$ onde $p > 0$ é a característica de E_i.

Definição 3.7.9. Seja $\mathcal{C}$ uma classe de extensão de corpos. Então $\mathcal{C}$ é uma *classe distinta* se satisfaz as seguintes condições:

1. Seja $K \subset F \subset E$ uma cadeia de corpos. A extensão $K \subset E$ está em $\mathcal{C}$ se e somente se $K \subset F$ e $F \subset E$ estão em $\mathcal{C}$.

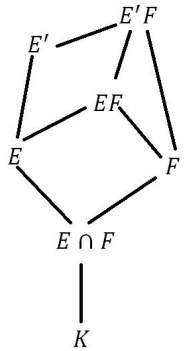
2. Se $K \subset E$ está em $\mathcal{C}$, F é uma extensão qualquer de K; E, F estão contidos em algum corpo, então $F \subset EF$ está em $\mathcal{C}$.

3. Se $K \subset F$ e $K \subset E$ estão em $\mathcal{C}$, E, F são subcorpos de um mesmo corpo, então $K \subset FE$ está em $\mathcal{C}$.

Definição 3.7.10. Uma extensão finita E/K, separável é chamada *Extensão Solúvel* se a menor extensão Galoisiana F de K, tal que $K \subset E \subset F$, tenha $G(F/K)$ solúvel.

Proposição 3.7.11. *Extensões solúveis formam uma classe distinta de extensões.*

Demonstração. Seja E uma extensão solúvel sobre K e F outro corpo que contém K. Assuma que E, F são subcorpos de L, corpo algebricamente fechado. Seja E' a extensão galoisiana sobre K tal que $G(E'/K)$ é solúvel e $E \subset E'$. Então $E'F$ é galoisiana sobre F e $G(E'F/F)$ é um subgrupo de $G(E'/K)$, pelo teorema (3.0.16), $G(E'F/F) \simeq G(E'/E \cap F)$, como $E'/E \cap F$ é extensão galoisiana, temos que o grupo $G(E'/E \cap F)$ é normal, pelo Teorema Fundamental da Teoria de Galois, portanto pelo Teorema (3.7.5), $G(E'/E \cap F)$ é solúvel, já que $G(E'/K)$ é solúvel e contém $G(E'/E \cap F)$.



Portanto $G(E'F/F)$ também é solúvel. Como a composta EF/F é subextensão de $E'F/F$, esta última galoisiana e solúvel, temos que EF/F é solúvel, pois uma subextensão de uma extensão solúvel também é solúvel. Satisfazendo a condição (2) de classe distinta.

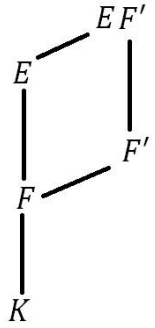
Assumindo que $E \supset F \supset K$, que E/F é solúvel e que F/K também é solúvel, tome F' a extensão galoisiana sobre K tal que $G(F'/K)$ é solúvel e $F \subset F'$. Temos que EF'/F' é solúvel (demonstração análoga à demonstração acima, do item (2) de classe distinta).

Assim, existe uma extensão galoisiana L sobre F' tal que $G(L/F')$ é solúvel. Seja σ algum k-homomorfismo injetivo de L em $\overline{K}$, fecho algébrico de K, então $\sigma(F') = F'$. Então $\sigma(L)$ é uma extensão galoisiana e solúvel de F', pois $\sigma(L)$ é isomorfo a L solúvel e galoisiana sobre F'. Considere M a extensão composta de todas as extensões formadas por K-homomorfismos injetivos $\sigma's$ de de L em $\overline{K}$. M será galoisiana sobre K, portanto galoisiana sobre F'.

Então

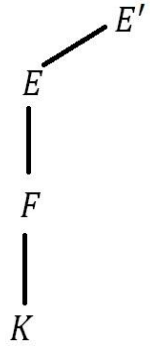
$$G(M/F') \subset \prod_{\sigma} G(\sigma(L)/F'),$$

pois a aplicação $\varphi : G(M/F') \to \prod G(\sigma(L)/F')$ é injetiva pelo Teorema (3.0.19).

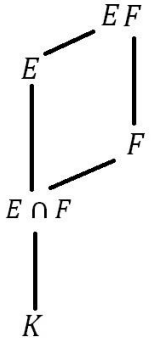


Portanto $G(M/F')$ é solúvel. Pelo Teorema (3.6.1), $\psi : G(M/K) \to G(F'/K)$ tal que $\psi(\sigma) = \sigma|_{F'}$ é um homomorfismo sobrejetor, portanto $G(F'/K) \simeq G(M/K)/G(M/F')$, isto é, $G(M/K)/G(M/F')$ é normal e solúvel. Então $G(M/K)$ é solúvel.

Como $E \subset M$, concluímos que E/K é uma extensão solúvel, concluindo assim a verificação da volta do item (1) de classe distinta.



A ida da condição (1) pode ser verificada, já que F/K é subextensão de E/K, portanto solúvel. E'/F é galoisiana e portanto $G(E'/F)$ é normal sobre o grupo $G(E'/K)$ que é solúvel, portanto $G(E'/F)$ é solúvel, então E/F é solúvel.



Por fim, tomando E e F extensões solúveis de K, pela verificação do item (2) de classe distinta podemos concluir que EF é solúvel sobre F e pelo fato de F ser sólúvel sobre K e, pela demonstração da ida do item (1) de classe distinta, temos que EF é solúvel sobre K. Terminando aqui a verificação do item (3) de classe distinta.

■

Teorema 3.7.12. *Seja E uma extensão separável de K. Então E é solúvel por radicais se e só se E/K é solúvel.*

Primeiro assumiremos que E/K é solúvel e seja E' a extensão finita de galois solúvel de K tal que $E \subset E'$. Seja m o produto de todos os primos que dividem $[E' : K]$ diferentes da característica. Considere agora a extensão $F = K(\zeta)$ onde ζ é o primitivo da raiz m-ésima da unidade de F, portanto é extensão galoisiana, com $G(F/K)$ cíclico, portanto abeliano, portanto solúvel.

Tomando a extensão $E'F$, temos que, pelo Teorema (3.0.16), existe um isomorfismo entre $G(E'F/F)$ e o subgrupo $G(E'/E' \cap F)$ de $G(E'/K)$. Observe que, sendo $G(F/K)$ grupo abeliano, seu subgrupo $G(F/E' \cap F)$ é normal e pelo Teorema Fundamental de Galois $E' \cap F$ é galoisiano sobre K e pelo mesmo motivo teremos $G(E'/E' \cap F)$ subgrupo normal de $G(E'/K)$ e portanto solúvel. Pelo isomorfismo, temos $G(E'F/F)$ solúvel.

Pelo Teorema 3.7.4 temos que $G(E'F/F)$ admite uma cadeia de subgrupos cíclicos e assim teremos uma cadeia de subcorpos entre F e $E'F$ tal que cada elemento dessa cadeia é cíclico de ordem prima sobre o corpo anterior (relação garantida pelo Teorema Fundamental de Galois).

Aplicando o Teoremas 3.6.7 e 3.6.9, concluímos que $E'F$ é solúvel por radicais sobre F. Como F foi obtida pela adjunção de uma raiz da unidade em K, temos que $E'F$ é solúvel por radicais sobre K, e assim teremos E solúvel por radicais sobre K.

Por outro lado, se assumirmos que E/K é solúvel por radicais, para algum homomorfismo injetor σ de E em um fecho algébrico L, a extensão gerada por $\sigma(E)/K$ também será solúvel por radicais.

Portanto a menor extensão galoisiana E' de K que contém E, na qual é uma composição de E com suas conjugações, é solúvel por radicais.

Sejam m o produto de todos os primos diferentes da característica que dividem o grau $[E : K]$ e novamente seja $F = K(\zeta)$ onde ζ é a raiz m-ésima da unidade. Basta provar que $E'F$ é solúvel sobre F, pois disso obtemos que $E'F$ é solúvel sobre K e portanto $G(E'/K)$ é solúvel pois é a imagem de um homomorfismo de $G(E'F/K)$.

Mas $E'F/F$ pode ser decomposto em uma cadeia de extensões tais que cada elemento dessa

cadeia tem grau primo sobre a extensão imediatamente anterior como nos Teoremas de Hilbert e de Artin-Schreier, com as raízes correspondentes no corpo E.

Portanto $E'F/F$ é solúvel, terminando a prova do Teorema.

Corolário 3.7.13. *O polinômio $f(x) \in K[x]$ é solúvel por radicais sobre K se, e só se, o grupo de Galois do corpo de decomposição de $f(x)$ sobre K é um grupo solúvel.*

Observação 3.7.14. Existem polinômios de grau $n \geq 5$ que não são solúveis por radicais. De fato, alguns polinômios tem suas extensões correspondentes não solúveis, onde o Grupo de Galois é isomorfo a S_5. Com a aplicação direta do Teorema 3.7.6 e do Corolário 3.7.13 mostramos a insolubilidade por radicais desses polinômios.

Exemplo 3.7.15. Seja $f(x) = g(x)h(x), g(x) = (x^5 - x - 1)$ e $h(x) = (x^3 - 1)$ polinômios de $\mathbb{F}_5[x]$. Observe que $g(x)$ não tem raízes em $\mathbb{F}_5$ e, pelo Teorema 3.6.9, é irredutível e ainda, existe a extensão $\mathbb{F}_5(\alpha)$ cíclica de grau 5, com α uma raiz de $g(x)$ (Observe que em $\mathbb{F}_5(\alpha)$ estão todas as outras 4 raízes de $g(x)$, todas do tipo $(\alpha + i)$ onde $i \in \mathbb{F}_5$ e $i \neq 0$). Como $\mathbb{F}_5(\alpha)$ é corpo de decomposição de $g(x)$ e cíclica é portanto solúvel.

Por sua vez, $h(x)$ tem grau 3, como $h(x)$ tem $1 \in \mathbb{F}_5$ como única raiz em $\mathbb{F}_5$, pode-se escrever $h(x) = (x^2 + x + 1)(x - 1)$. Tomando $t(x) = (x^2 + x + 1)$, irredutível sobre $\mathbb{F}_5$, garante-se a existência da extensão $\mathbb{F}_5(\beta)$, com $\beta \notin \mathbb{F}_5$ uma raiz de $t(x)$, consequentemente de $h(x)$, de grau 2, cíclica, abeliana e portanto solúvel.

Agora, seja E a extensão composta de $\mathbb{F}_5(\alpha)$ e $\mathbb{F}_5(\beta)$. Temos que E é corpo de decomposição do polinômio $f(x)$ e, pela Proposição 3.7.11, E é solúvel. Por fim, usamos o Teorema 3.7.13 e concluímos que $f(x)$ é solúvel por radicais.

4 Conclusão

Pudemos verificar que a solubilidade por radicais de um polinônio está diretamente relacionada à extensão de corpo onde tal polinômio possui suas raízes. Pelo fato de haver a relação entre extensões de corpos e grupos, garantidos no Teorema Fundamental de Galois, estudamos o comportamento dos grupos para definirmos quando a extensão é solúvel.

Vimos que garantir a solubilidade por radicais em corpos de característica p, especificamente, é possível graças aos Teoremas de Hilbert e Artin-Schreier que possibilitaram estender os resultados no Teorema 3.7.12 demonstrado.

A expectativa agora é que o trabalho apresentado possa servir como subsídio para estudantes de Matemática. Esperamos que, de fato, as observações e os detalhes das demostrações possam facilitar a leitura e o entendimento dos teoremas chave para solubilidade por radicais.

Referências Bibliográficas

[1] LANG, Serge.,*Algebra - Graduate Texts in Mathematics 211*, Springer-Verlag, 3rd edition, New York, 2002.

[2] HERSTEIN I.N., *Topics in Algebra*, 2nd edition, Xerox College Publishing, Lexington, 1975.

[3] ARTIN, Michael. *Algebra*, Prentice Hall, New Jersey, 1991.

[4] GALLIAN, Joseph A. *Contemporary Abstract Algebra*, 6th ed, Houghton Mifflin, 2006.

[5] MILNE, James S. *Fields and Galois Theory*, Version 4.30, disponível em www.jmilne.org/math/, 2012.

[6] GONÇALVES, Adilson. *Introdução à Álgebra*, 5ª Edição, IMPA, Rio de Janeiro, 2003.

[7] ENDLER, Otto. *Soluções de Equações por Radicais em Corpos de Característica* $p \geq 0$, Matemática Universitária Nº 5 - páginas 25 a 32, IMPA, 1987.

[8] GARCIA, Arnaldo. *Elementos de Álgebra*, IMPA, Rio de Janeiro, 2003.

[9] VIEIRA, A. C. *Apostila de Álgebra II*, Departamento de Matemática UFMG, 2013.

[10] FIGUEIREDO, D. G. *Números Irracionais e Transcendentes*, Coleção Iniciação Científica, 3ª Edição, SBM, 2002.