Universidade Federal de Santa Catarina

Curso de Pós-Graduação em Matemática e

Computação Científica

Soluções de Equações Polinomiais por Radicais Reais

Janice Teresinha Reichert

Orientadora: Profª. Drª. Eliana Farias e Soares

Florianópolis

Abril de 2001

BU

Universidade Federal de Santa Catarina

Curso de Pós-Graduação em Matemática e Computação Científica

Soluções de Equações Polinomiais por Radicais Reais

Dissertação apresentada ao Curso de Pós-Graduação em Matemática e Computação Científica, do Centro de Ciências Físicas e Matemáticas da Universidade Federal de Santa Catarina, para a obtenção do grau de Mestre em Matemática, com Área de Concentração Álgebra.

Janice Teresinha Reichert

Florianópolis

Abril de 2001

Soluções de Equações Polinomiais por Radicais Reais

por

Janice Teresinha Reichert

Esta Dissertação foi julgada para a obtenção do Título de "Mestre", Área de Concentração em Álgebra, e aprovada em sua forma final pelo Curso de Pós-Graduação em Matemática e Computação Científica.

Celso Melchíades Dória

Coordenador

Comissão Examinadora

Profª. Drª Eliana Farias e Soares (UFSC-Orientadora)

Profª. Drª Albertina Zatelli (UFSC)

Prof. Dr. Yves Lequain (IMPA - RJ)

Prof. Dr. Oscar Ricardo Janesch (UFSC)

Florianópolis, Abril de 2001.

Agradecimentos

Agradeço à meu noivo, Luciano, e a minha família, pelo incentivo dado em todos os momentos.

Aos meus colegas de graduação e Pós-Graduação Airton, Anderson, Andresa,Caren, Christian, Claiton, Danilo, Daniel, Dirceu, Fábio, Graziela, Juliano, Maria Inez, Milton, Patrícia, Paulo ,Rafael e Suzana pela amizade e agradável companhia.

Ao CNPQ (Conselho Nacional de Desenvolvimento Científico e Tecnológico) pelo auxílio financeiro recebido durante o último ano de mestrado.

Meu especial agradecimento a minha orientadora Eliana Farias e Soares, pelo apoio e amizade.

Resumo

Neste trabalho vamos estudar duas questões que são:

(i) Dado um polinômio $f(x)$ irredutível sobre um corpo $F \subseteq \mathbb{R}$ que possui todas as raízes reais, quando é possível expressar as raízes de f em termos de radicais reais.

(ii) Em que situação, corpos intermediários de extensões radicais repetidas $Q \subseteq L$, são também extensões radicais repetidas de Q. Aqui, veremos dois casos que são $|L : Q|$ é ímpar onde precisamos que Q seja um corpo real, $|L : Q|$ potência de 2, onde a característica de Q precisa ser diferente de 2.

Para o primeiro caso, demonstraremos um teorema que caracteriza extensões radicais repetidas.

Sumário

Introdução

Este trabalho baseia-se num artigo de I.M.Isaacs & D.P. Moulton publicado no Journal of Algebra 201 pp. 429-455, (1998).

Um dos problemas mais antigos da Álgebra é a busca de soluções de equações polinomiais que possam ser expressas por combinações finitas de radicais. Este problema só foi resolvido no século XIX por Évariste Galois, que construiu uma teoria que permite, dado um polinômio sobre um corpo de característica zero, decidir se ele tem ou não raízes que podem ser expressas por radicais, hoje conhecida como teoria de Galois.

Um dos principais resultado dessa teoria é o seguinte: As raízes do polinômio irredutível $f(X) \in F[X]$ podem ser expressas por radicais se e somente se o grupo de Galois de $f(X)$ é solúvel.

O fato de as raízes de $f(X)$ poderem ser expressas por radicais significa que o corpo de raízes S de $f(X)$ sobre F está contido em uma extensão L de F que é uma extensão radical repetida de F, isto é, para a qual existe uma cadeia

$$F = L_0 \subset L_1 \subset ... \subset L_n = L$$

onde $L_i = L_{i-1}[\alpha_i]$, com $\alpha_i^{n_i} \in L_{i-1}$ para algum inteiro positivo n_i.

É bem conhecido que corpos intermediários de extensões radicais repetidas não são necessariamente extensões radicais repetidas. A solubilidade do grupo Gal(S:F) não garante, dessa forma, que S seja uma extensão radical repetida de F.

Isso já acontece no caso de polinômios de grau 3: seja $f(X) \in \mathbb{Q}[X]$ com $f(X) = X^3 - 6X + 2$. O polinômio f possui três raízes reais

e naturalmente $f(X)$ é solúvel por radicais. Calculando explicitamente as três raízes de f obtemos:

$$x = \alpha + \frac{2}{\alpha}$$

onde α percorre as três raízes cúbicas de $-1 + \sqrt{7}i$.

Se S fosse uma extensão radical repetida de $\mathbb{Q}$, deveria existir uma maneira alternativa de expressar essas raízes em termos de radicais reais. Mas isso é impossível pelo teorema seguinte:

TEOREMA A: Seja Q um subcorpo dos números reais $\mathbb{R}$ e suponha que $f \in Q[X]$ é irredutível e se fatora completamente sobre $\mathbb{R}$. Se alguma raiz de f está em uma extensão radical repetida real de Q, então $grau(f)$ é uma potência de 2.

Vamos demonstrar um teorema um pouco mais geral que o Teorema A acima: consideramos o caso em que o corpo de raízes de f é um corpo quase real, isto é, um corpo de característica zero que contém somente duas raízes da unidade.

Outro resultado que vamos mostrar é que, em alguns casos, corpos intermediários de extensões radicais repetidas são de fato extensões radicais repetidas:

TEOREMA B: Suponha que Q seja um corpo real e que $Q \subseteq L$ seja uma extensão radical repetida com $|L : Q|$ ímpar. Se $Q \subseteq K \subseteq L$, então K é uma extensão radical repetida de Q.

Vamos mostrar que neste caso a condição de Q ser um corpo real não pode ser removida. Na demonstração do Teorema B começamos observando que não há perda de generalidade se assumirmos que $L \subseteq \mathbb{R}$ e, neste caso, damos uma caracterização muito útil das extensões radicais repetidas. Esta caracterização, um pouco técnica, pode ser vista como um dos principais resultados do trabalho. Ela possui outras aplicações, e, em particular, pode ser usada para provar o seguinte resultado que complementa o Teorema A:

TEOREMA C: Suponha que Q seja um corpo real e que $f \in Q[X]$ seja irredutível de grau ímpar. Se f possui alguma raiz α em uma extensão radical repetida real de Q, então α é a única raiz real de f.

No Teorema B, consideramos corpos intermediários de uma extensão radical repetida de grau ímpar sobre um corpo real. É talvez um pouco suprendente que também no caso oposto a este, ou seja, quando o grau da extensão é uma potência de 2, obtenhamos um resultado parecido. Neste caso, não necessitamos nem que o corpo inicial seja real; é suficiente que sua característica seja diferente de 2. O teorema a que estamos nos referindo é o seguinte:

TEOREMA D: Suponha que $Q \subseteq L$ seja uma extensão radical repetida de corpos de característica diferente de 2. Se $|L : Q|$ é uma potência de 2 e $Q \subseteq K \subseteq L$, então K é uma extensão radical repetida de Q.

Na situação do Teorema D, mostraremos que K é, na verdade, uma extensão quadrática repetida de Q.

Os Teoremas A, B, C e D, bem como o Teorema que dá a caracterização das extensões radicais repetidas, são provados no capítulo 3, que é o principal capítulo dessa dissertação. No capítulo 1 apresentamos alguns resultados de Teoria de Grupos, no capítulo 2 alguns resultados de Extensões de Corpos e Teoria de Galois. Finalmente, no capítulo 4, apresentamos alguns exemplos e observações finais.

Capítulo 1

Teoria de Grupos

Neste Capítulo apresentaremos algumas definições e resultados da teoria de grupos que serão úteis nos capítulos seguintes. Os resultados mais importantes, e que estão diretamente ligados ao tema desta dissertação, serão demonstrados. Quanto aos outros, apenas será indicada a referência onde podem ser encontradas as suas provas. Neste trabalho lidaremos sempre com grupos finitos.

1.1 Alguns Resultados Básicos

Para facilitar a leitura dessa dissertação enunciaremos, nessa seção, alguns resultados básicos, alguns deles muito elementares, que serão usados no decorrer desse trabalho.

Teorema 1.1 *Sejam G um grupo e N_i, $i = 1, 2$, subgrupos normais de G. Se G/N_i é abeliano, para $i = 1, 2$, então $G/(N_1 \cap N_2)$ é abeliano.*

A demonstração é trivial.

A seguinte conseqüência imediata do Teorema dos Homomorfismos será usada:

Teorema 1.2 *Seja $\varphi : G_1 \to G_2$ um homomorfismo entre os grupos G_1 e G_2, com $\ker \varphi = C$. Se H é subgrupo de G_1, então $\varphi(H) \simeq \frac{HC}{C}$.*

Teorema 1.3 *Sejam G um grupo, N normal em G e H subgrupo de G. Então* $\frac{H}{H \cap N} \simeq \frac{HN}{N}$ *e, em particular,* $|H : H \cap N| = |HN : N|$ *e* $|HN : H| = |N : N \cap H|$.

Demonstração: Ver [2], Corolário IV.12.c, p. 103. □

Definição 1.4 *Sejam G um grupo e H subgrupo de G. Dizemos que H é um subgrupo característico de G se $\sigma(H) \subseteq H$ para todo automorfismo σ de G.*

Teorema 1.5 *Sejam G um grupo e H, N subgrupos de G, com $H \subseteq N$ e $N \lhd G$. Então, se H é subgrupo característico de N, H é normal em G.*

Demonstração: Ver [2], Proposição IV.14, p. 106.

□

Definição 1.6 *Sejam G um grupo e H um subgrupo de G. O normalizador de H em G, denotado por $N_G(H)$, é o maior subgrupo de G contendo H, no qual H é normal, isto é,*

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Se K é um subgrupo de G tal que $K \subseteq N_G(H)$, dizemos que K normaliza H.

Definição 1.7 *Sejam G um grupo e H um subgrupo de G. O centralizador de H em G, denotado por $C_G(H)$, é o seguinte subgrupo de G:*

$$C_G(H) = \{g \in G : gh = hg \ \forall \ h \in H\}.$$

Teorema 1.8 *Sejam G um grupo e H um subgrupo de G. Então $C_G(H) \lhd N_G(H)$ e* $\frac{N_G(H)}{C_G(H)}$ *é isomorfo a um subgrupo de $Aut(H)$.*

Demonstração: De fato,

$$\begin{array}{rccccc} \psi: & N_G(H) & \to & Aut(H) & & \\ & g & \mapsto & \tau_g: & H & \to & H \\ & & & & h & \mapsto & g^{-1}hg \end{array}$$

é um homomorfismo com $\ker(\psi) = C_G(H)$.

□

O seguinte resultado sobre o grupo S_p será usado:

Teorema 1.9 *Sejam σ um p-ciclo em S_p, com p primo, e $P =< \sigma >$. Então, $C_{S_p}(P) = P$.*

Demonstração: Podemos supor $\sigma = (12...p)$. Seja $\tau \in C_{S_p}(P)$. Como, $\tau^{-1}\sigma\tau = (\tau(1)\tau(2)...\tau(p))$, se $\tau^{-1}\sigma\tau = \sigma$, devemos ter, para algum $i \in \{1, 2, \ldots, p\}$,

$$\tau(1) = i,\ \tau(2) = i+1,\ \ldots,\ \tau(p-i+1) = p,\ \tau(p-i+2) = 1,\ \ldots,\ \tau(p) = i-1,$$

ou seja, $\tau = \sigma^i$.

□

Definição 1.10 *Sejam G grupo e H um subgrupo de G. O fecho normal de H em G, denotado por H^G, é o menor subgrupo normal em G que contém H, isto é, H^G é a interseção de todos os subgrupos normais de G que contém H.*

Definição 1.11 *Seja p um número primo. Um grupo finito G é um p-grupo se sua ordem é uma potência de p.*

Teorema 1.12 *($1^{\underline{o}}$ Teorema de Sylow)*

Seja G um grupo de ordem $p^m.q$ onde p é primo e não divide q. Então, para todo $0 \leq n \leq m$, existe um subgrupo H de G tal $|H| = p^n$.

Demonstração: Ver [2] p. 159. □

Definição 1.13 *Sejam G um grupo finito, p um primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que têm ordem p^m são chamados p-subgrupos de Sylow de G.*

Teorema 1.14 *(2^{o} Teorema de Sylow)*

Sejam G um grupo finito e p um primo. Então

(1) *todos os p-subgrupos de Sylow de G são conjugados entre si;*

(2) *se P é um p-subgrupo de G, então existe um p-subgrupo de Sylow S de G tal que $P \subseteq S$.*

Demonstração: Ver [2], Teorema $V.3$, p. 162.

□

1.2 Grupos Cíclicos

Teorema 1.15 *Seja G um grupo cíclico de ordem n. Então*

(1) $G \simeq \mathbb{Z}_n$;

(2) *existe um único subgrupo de G de ordem m, para cada divisor m de n;*

(3) *se H_1 e H_2 são subgrupos de G tais que $|H_1|$ divide $|H_2|$, então $H_1 \subseteq H_2$.*

Demonstração: Ver Proposições IV.15, IV.17 e IV.18, pp. 107-108, em [2].

□

Teorema 1.16 *O grupo dos automorfismos de $\mathbb{Z}_n$ é isomorfo a $\mathbb{Z}_n^*$, o grupo multiplicativo dos inteiros invertíveis módulo n. Em particular, $Aut(\mathbb{Z}_n)$ é abeliano, sendo cíclico se n é primo.*

Demonstração: Ver Proposição IV.20, p. 112, em [2].

□

Observação 1.17 Seja E um corpo. Se D é um subgrupo finito do grupo multiplicativo $E - \{0\}$, que denotaremos E^x, então D é cíclico. Assim, os subgrupos de E^x são univocamente determinados por suas ordens. Se $D \subseteq E^x$ é um subgrupo de ordem n, então D é o subgrupo $< \delta >$, em que δ é uma raiz n-ésima primitiva da unidade em E.

1.3 Ações de Grupos

Definição 1.18 *Sejam G um grupo, C um conjunto e $P(C)$ o grupo de permutações de C. Uma representação de G no grupo de permutações de C é um homomorfismo $\rho : G \to P(C)$.*

Nesse caso, dizemos que G atua sobre o conjunto C e o homomorfismo ρ é chamado uma ação de G sobre C. Quando C é um grupo e $\rho(g)$ um automorfismo para todo $g \in G$, dizemos que G atua via automorfismos. Neste caso, dizemos que C é um G-grupo.

Observação 1.19 Nesse trabalho, todas as ações consideradas serão via automorfismo. Por isso, ao nos referirmos a uma ação, deixaremos subentendido que ela é desse tipo.

Notação 1.20 *Se um grupo G atua sobre o grupo C segundo o homomorfismo ρ, então, se $g \in G$ e $c \in C$, denotamos $\rho(g)(c) = c^g$. O grupo dos automorfismos de G, $Aut(G)$, atua de maneira óbvia sobre G. Nesse caso, podemos escrever também $\sigma(g)$ para $\sigma \in Aut(G)$ e $g \in G$.*

Definição 1.21 *Se C é um G-grupo, dizemos que G atua trivialmente em C se $c^g = c$ para todo $g \in G$ e todo $c \in C$. Também dizemos que G atua fielmente em C, se $c^g = c$ para todo $c \in C$ implicar $g = e$.*

Definição 1.22 *Dado um G-grupo C, dizemos que um subgrupo M de C é invariante por $g \in G$, se $M^g \subseteq M$, em que $M^g = \{m^g : m \in M\}$. Também dizemos, neste*

caso, que G estabiliza o subgrupo M. Dizemos que M é G-invariante (ou que é um G-subgrupo de C) se M for invariante por todo $g \in G$.

Definição 1.23 *Seja G um grupo atuando sobre o grupo C, e seja $c \in C$. O estabilizador de c, denotado G_c, é o subgrupo de G*

$$G_c = \{g \in G : \ c^g = c\}.$$

1.4 Ações com Pontos Fixos Não Triviais

Definição 1.24 *Dada uma ação de um grupo G em um grupo C, dizemos que $c \in C$ é um ponto fixo de um subgrupo H de G, se $c^h = c$ para todo $h \in H$. O conjunto dos pontos fixos de H é um subgrupo de C que denotamos por $C_C(H)$.*

Observação 1.25 Essa notação já foi usada na Definição 1.7, mas aquele é um caso particular deste, em que consideramos G atuando em G por conjugação.

Definição 1.26 *Dizemos que um conjunto $\mathcal{P}$ de subgrupos de um grupo G é uma partição de G se $\bigcup_{H \in \mathcal{P}} H = G$ e $H \cap K = \{e\}$ para quaisquer $H, K \in \mathcal{P}$ distintos.*

Lema 1.27 *Seja $\mathcal{P}$ uma partição de um grupo finito G, e suponha que G atua num grupo abeliano A. Se A contém um elemento cuja ordem não divide $|\mathcal{P}| - 1$, então $C_A(H) \neq \{e\}$ para algum $H \in \mathcal{P}$.*

Demonstração: Escreva A aditivamente, e seja $a \in A$, tal que a ordem de a não divide $|\mathcal{P}| - 1$. Primeiramente observe que para cada subgrupo $X \subseteq G$, definindo $a_X := \sum_{x \in X} a^x$, temos $a_X \in C_A(X)$, pois para todo $y \in X$,

$$(a_X)^y = (\sum_{x \in X} a^x)^y = \sum_{x \in X} (a^x)^y = \sum_{x \in X} a^{xy} = \sum_{x \in X} a^x = a_X.$$

Agora, suponha por absurdo que, $\forall H \in \mathcal{P}$, o elemento neutro e é o único ponto fixo de H. Então $a_H = 0$ para todo $H \in \mathcal{P}$. Também $a_G = 0$, pois $a_G \in C_A(G) \subset C_A(H)$

para todo H. Como $\mathcal{P}$ é uma partição de G, temos

$$0 = \sum_{H \in \mathcal{P}} a_H = (|\mathcal{P}| - 1)a + a_G = (|\mathcal{P}| - 1)a.$$

Mas isto contradiz o fato de termos escolhido $a \in A$ cuja ordem não divide $|\mathcal{P}| - 1$.

Assim, $a_H \neq 0$ para algum $H \in \mathcal{P}$, ou seja, $C_A(H) \neq \{0\}$ para algum $H \in \mathcal{P}$. □

Corolário 1.28 *Seja G um $p-$grupo abeliano não cíclico de ordem p^2 tal que G atua num espaço vetorial não nulo sobre um corpo de característica diferente de p. Então algum subgrupo de ordem p em G possui ponto fixo não trivial neste espaço.*

Demonstração: Seja V o espaço vetorial não nulo e seja $A = (V, +)$. Primeiramente vamos construir uma partição $\mathcal{P}$ para $G = \mathbb{Z}_p \times \mathbb{Z}_p$.

Tome $e \neq x_1 \in \mathbb{Z}_p \times \mathbb{Z}_p$. Considere $H_1 =< x_1 >$. Temos que $|H_1| = p$. Agora tome $x_2 \in G \setminus H_1$ e considere $H_2 =< x_2 >$. Então $|H_2| = p$ e $H_1 \cap H_2 =< e >$. Seguindo o processo acima temos $H_i =< x_i >$, $i = 1, ..., p+1$, com $|H_i| = p$, $H_i \cap H_j =< e >$, $\forall i \neq j$ e $H_1 \cup H_2 \cup ... \cup H_{p+1} = G$.

Assim, $\mathcal{P} = \{H_1, H_2, ..., H_{p+1}\}$ é uma partição de G.

Por hipótese, G atua em V, que é um espaço vetorial sobre um corpo de característica diferente de p. Assim, todos os elementos de A possuem ordem diferente de $p = |\mathcal{P}| - 1$. Então, pelo lema anterior, temos que $C_A(H) \neq 0$ para algum $H \in \mathcal{P}$, ou seja, existe algum subgrupo H de ordem p em G que possui ponto fixo não trivial neste espaço. □

Uma outra situação em que vamos aplicar o Lema 1.27 é o caso do Teorema seguinte:

Teorema 1.29 *Seja $G = HK$, com $K \lhd G$, $|K| = p$ (p primo) e $K \not\subseteq H$. Se $H \neq \{e\}$ atua fielmente em K por conjugação e G atua num espaço vetorial sobre um corpo cuja característica não divide $|K|$, então H ou K possui ponto fixo não trivial neste espaço.*

Demonstração: Dado $g \in G$ temos que $g = hk$, $h \in H$, $k \in K$. Portanto, $H^g = H^k$. Também, se $k \in K - \{e\}$ então $K \cap H^k = \{e\}$. Para ver isto observe que, como $K \not\subseteq H$ por hipótese, temos que $K \cap H = \{e\}$, já que $|K| = p$, e, portanto, $K \cap H^k = K^k \cap H^k = (K \cap H)^k = \{e\}$.

Afirmação 1: $\forall k_1, k_2 \in K$, $k_1 \neq k_2$, temos $H^{k_1} \cap H^{k_2} = \{e\}$.

De fato, suponha que $e \neq y \in H^k \cap H$, para algum $e \neq k \in K$. Então $y = h = k^{-1}h_1k$, com $h, h_1 \in H$, donde $kh = h_1k$ e, assim, $h^{-1}khk^{-1} = h^{-1}h_1$. Como $h^{-1}khk^{-1} \in K$ e $h^{-1}h_1 \in H$, temos que $h^{-1}h_1 = e$ e, portanto, $h_1 = h$. Assim, $k = h^{-1}kh$, isto é, h fixa k. Mas isto contraria o fato de H atuar fielmente em K, pois, como $|K| = p$, se h fixa um elemento k de K diferente de e, então h fixa todos os elementos de K. Portanto, $\forall k \neq e$ em K, tem se $H^k \cap H = \{e\}$. Isso implica que se $k_1 \neq k_2$, $k_1, k_2 \in K$, então $H^{k_1} \cap H^{k_2} = \{e\}$ pois $H^{k_1} \cap H^{k_2} = (H \cap H^{k_2k_1^{-1}})^{k_1}$.

Afirmação 2: $K = \{e\} \cup (G \setminus \bigcup_{g \in G} H^g)$.

Como $H \cap K = \{e\}$, temos $\{e\} = H^g \cap K^g = K \cap H^g$. Portanto

$$K \subseteq (G \setminus \bigcup_{g \in G} H^g) \cup \{e\}.$$

Para ver que $(G \setminus \bigcup_{g \in G} H^g) \cup \{e\} \subseteq K$, observe que $|G| = |K||H|$ e como

$$\bigcup_{g \in G} H^g = \bigcup_{k \in K} H^k \quad \text{e} \quad H^{k_1} \cap H^{k_2} = \{e\} \quad \text{se} \quad k_1 \neq k_2,$$

então

$$|\bigcup_{g \in G} H^g| = (|H| - 1)|K| + 1 = |H||K| - |K| + 1.$$

Assim

$$\begin{aligned} |(G - \bigcup_{g \in G} H^g) \cup \{e\}| &= |G| - |\bigcup_{g \in G} H^g| + 1 \\ &= |K||H| - |K||H| + |K| - 1 + 1 \\ &= |K|. \end{aligned}$$

Como conseqüência das Afirmações 1 e 2, temos que, $\mathcal{P} = \{K, H^{k_1}, ..., H^{k_p}\}$ onde $\{k_1, ..., k_p\} = K$, é uma partição de G, com $|\mathcal{P}| = |K| + 1$.

Seja V o espaço vetorial não nulo e $A := (V, +)$. Como V é espaço vetorial sobre um corpo cuja característica não divide $|K|$, todos os elementos de A possuem ordem que não divide $|K| = |\mathcal{P}| - 1$.

Assim, pelo Lema 1.27, temos que $C_A(N) \neq \{e\}$ para algum $N \in \mathcal{P}$. Mas os elementos de $\mathcal{P}$ são K ou H^{k_i}, $k_i \in K$.

Então, ou K possui um ponto fixo não trivial, ou H^{k_i}, para algum $i = 1, ..., p$, possui um ponto fixo não trivial. Afirmamos que, se H^{k_i} possui um ponto fixo não trivial, então H também possui um ponto fixo não trivial. De fato, suponha que H^{k_i} fixa $a \in V$. Logo $a^{k_i^{-1}hk_i} = a \ \forall h \in H$ e, como G atua via automorfismos, temos $a^{k_i h} = a^{k_i}$, ou seja, H fixa $a^{k_i^{-1}}$. Portanto a afirmação fica provada.

Logo K ou H possui ponto fixo não trivial neste espaço.

□

1.5 Séries Subnormais e o Teorema de Jordan-Hölder

Definição 1.30 *Um subgrupo H de um grupo G é subnormal ($H \lhd\lhd G$) se existe uma série de subgrupos*

$$H_0 = H \lhd H_1 \lhd H_2 \lhd ... \lhd H_n = G.$$

Tal série será denominada uma série subnormal de H a G, os subgrupos H_i, $i = 1, ..., n$ são termos da série, e os grupos quocientes $\frac{H_{i+1}}{H_i}$, $i = 0, ..., n-1$, são os fatores da série. Uma série subnormal de G é uma série subnormal de $\{e\}$ a G.

Temos o seguinte corolário do Teorema 1.3:

Corolário 1.31 *Sejam $X \lhd\lhd G$ e H subgrupo de G. Então $|X : X \cap H|$ divide $|G : H|$.*

Demonstração: Sejam $X \lhd X_1 \lhd ... \lhd X_n \lhd G$. Faremos indução em $|G : X|$. O caso $n = 0$ está contido no Teorema 1.3. Agora para $n \geq 1$, podemos supor $X \subsetneq X_1$. Como $|G : X_1| < |G : X|$, temos, pela hipótese de indução, que $|X_1 : X_1 \cap H|$ divide $|G : H|$.

Mas $X \lhd X_1$ e $H \cap X_1$ é subgrupo de X_1. Pelo Teorema 1.3, $|X : H \cap X| = |(H \cap X_1)X : H \cap X_1|$, que divide $|X_1 : X_1 \cap H|$.

Concluímos então que $|X : H \cap X|$ divide $|G : H|$. □

Notação 1.32 Dados um número primo p e um grupo G, denotamos por $O^p(G)$ a interseção de todos os subgrupos normais de G cujos índices em G são uma potência de p.

Observação 1.33 *Claramente $O^p(G) \lhd G$ e $|G : O^p(G)|$ é uma potência de p, o que decorre do Teorema 1.3. Também, $O^p(G)$ está contido em todo subgrupo subnormal de G cujo índice é uma potência de p.*

Definição 1.34 *Sejam U um grupo e G um U-grupo. Se H é um U-subgrupo de G, dizemos que uma série subnormal de H a G é uma U-série se cada termo da série é invariante por U.*

Observação 1.35 *Dado um grupo G, podemos sempre considerar a ação trivial de $U = \{e\}$ em G. Nesse caso todo subgrupo H de G é um U-subgrupo e toda série subnormal de H a G é uma U-série. Nas definições que seguem trataremos de U-séries, estando então o caso de $U = \{e\}$ incluído.*

Definição 1.36 *Uma U-série de composição para um grupo G é uma U-série*

$$\{e\} = M_0 \lhd M_1 \lhd ... \lhd M_n = G$$

tal que cada fator $\frac{M_{i+1}}{M_i}$ não tem subgrupo normal U-invariante.

Observação 1.37 Todo U-grupo finito possui uma U-série de composição e toda U-série subnormal de um grupo finito pode ser refinada para uma U-série de composição.

A demonstração para o caso de $U = \{e\}$ pode ser encontrada em [2] p. 199, e o mesmo argumento utilizado nela se aplica para o caso U qualquer.

Definição 1.38 *Sejam G um grupo, M e N dois G-grupos. Dizemos que M e N são G-isomorfos se existe um isomorfismo $\varphi : M \to N$ tal que $\varphi(m^g) = \varphi(m)^g$, para todo $m \in M$ e $g \in G$. Nesse caso, dizemos que φ é um G-isomorfismo.*

Definição 1.39 *Seja U atuando sobre um grupo G. Duas U-séries subnormais de G são equivalentes se existe uma bijeção entre os fatores não triviais da primeira e os da segunda série tal que os fatores correspondentes são U-isomorfos.*

Teorema 1.40 (Jordan Hölder) *Sejam U um grupo e G um U-grupo. Então todas as U-séries de composição de G são equivalentes.*

Demonstração: Pode ser encontrada em [2] p. 203, para o caso $U = \{e\}$. Tal prova é facilmente generalizada para caso U qualquer. □

Lema 1.41 *Sejam N um grupo finito e $M \lhd\lhd N$; seja M^N o fecho normal de M em N . Então:*

(a) todo automorfismo de N que estabiliza M também estabiliza M^N;

(b) existe uma série subnormal de M a N tal que todo automorfismo de N que estabiliza M também estabiliza cada um dos termos da série.

Demonstração:

(a) Seja σ um automorfismo de N que estabiliza M. Temos $M^N = \bigcap_{M \subseteq K \lhd N} K$. Portanto,

$$\sigma(M^N) = \sigma(\bigcap_{M \subseteq K \lhd N} K) = \bigcap_{M \subseteq K \lhd N} \sigma(K).$$

Como $M \subseteq K \lhd N$ se, e somente se, $M \subseteq \sigma(K) \lhd N$, temos que $\bigcap_{M \subseteq K \lhd N} \sigma(K) = M^N$ e, portanto, todo automorfismo de N que estabiliza M também estabiliza M^N.

(*b*) Faremos indução em $|N : M|$. O lema é claramente verdadeiro para $|N : M| = 1$. Assuma que $|N : M| > 1$ e que o lema seja verdadeiro para qualquer grupo G e subgrupo K satisfazendo suas hipóteses e tal que $|G : K| < |N : M|$. Como o caso $N = M$ é trivial, podemos assumir que $M \subseteq M^N < N$, em que M^N denota o fecho normal de M em N. Note que o fecho normal M^N é próprio em N, pois M é próprio e subnormal. Vemos que $|M^N : M| < |N : M|$. Assim, pela hipótese de indução, podemos achar uma cadeia de subgrupos

$$M = M_0 \lhd M_1 \lhd \ldots \lhd M_{r-1} = M^N$$

em que cada subgrupo M_i é estabilizado pelos automorfismos de M^N que estabilizam M.

Para concluir a prova, basta mostrar que a cadeia $M \lhd M_1 \lhd \ldots \lhd M^N \lhd N$ satisfaz às condições do lema. Para isto devemos tomar um automorfismo σ de N que estabiliza M e mostrar que ele estabiliza M^N, o que é verdadeiro por (*a*). □

1.6 Automorfismos Livres de Pontos Fixos

Lema 1.42 *Sejam G um grupo e σ um automorfismo de G, de ordem n, livre de pontos fixos. Então*

(1) *Todo elemento de G pode ser expresso na forma*

$$x^{-1}(\sigma(x)) \ e \ (\sigma(y))y^{-1}$$

para $x, y \in G$.

(2) *Para todo $x \in G$, temos*

$$x(\sigma(x))\ldots(\sigma^{n-1}(x)) = (\sigma^{n-1}(x)\ldots\sigma(x))x = e.$$

Demonstração:

(1) Se $x^{-1}(\sigma(x)) = y^{-1}(\sigma(y))$ com $x, y \in G$, então $xy^{-1} = \sigma(xy^{-1})$. Logo, como σ é livre de pontos fixos, $xy^{-1} = e$ e $x = y$. Assim, existem tantos elementos distintos em G da forma $x^{-1}(\sigma(x))$ quanto elementos x em G e, conseqüentemente, todo elemento de G pode ser expresso desta forma. Similarmente, todo elemento de G pode ser expresso da forma $(\sigma(x))x^{-1}$. Assim (1) está verificado.

(2) Se $x \in G$,então $x = y^{-1}(\sigma(y))$ para algum y em G, por (1). Conseqüentemente

$$\begin{aligned} x(\sigma(x))...(\sigma^{n-1}(x)) &= y^{-1}(\sigma(y))\sigma(y^{-1}\sigma(y))\ldots\sigma^{n-1}(y^{-1}\sigma(y)) \\ &= y^{-1}\sigma^n(y) = y^{-1}y = e. \end{aligned}$$

A segunda relação de (2) é provada similarmente. □

Corolário 1.43 *Seja G um grupo. Se σ é um automorfismo de G de ordem 2, livre de pontos fixos , então G é abeliano e $\sigma(x) = x^{-1}$ para todo $x \in G$.*

Demonstração: Pelo Lema 1.42 (2) temos que $x\sigma(x) = e$, donde $\sigma(x)=x^{-1}$ para todo $x \in G$. Mas, se $x, y \in G$, temos

$$(xy)^{-1} = \sigma(xy) = \sigma(x)\sigma(y) = x^{-1}y^{-1}.$$

Assim, $y^{-1}x^{-1}=x^{-1}y^{-1}$ e, portanto, temos que G é abeliano. □

Lema 1.44 *Sejam $M \lhd\lhd N$ e suponha que M é invariante por σ, onde $\sigma \in Aut(N)$ possui ordem prima p. Se σ atua livre de pontos fixos em todos os fatores de alguma série subnormal invariante por σ de M a N, então σ atua livre de pontos fixos em todo quociente R/S com $M \subseteq S \lhd R \subseteq N$, onde R e S são invariantes por σ.*

Demonstração: Seja $\mathfrak{X}$ a série subnormal de M a N invariante por σ tal que σ atua sem pontos fixos em cada um dos seus fatores. Afirmamos que a única classe lateral

à direita de M em N que fica fixa por σ é M e, assim, $|N : M| \equiv 1 \bmod p$ (veja Observação 1.45 a seguir).

De fato, suponha que a classe lateral My é invariante por σ e considere o menor termo Y de $\mathfrak{X}$ que contém y. Se $Y = M$, então $My = M$, como queríamos. Assim, podemos supor $Y > M$ e chegar a uma contradição. Considere X exatamente inferior a Y em $\mathfrak{X}$. Então $X \lhd Y$ (pois X, Y $\in \mathfrak{X}$) e ambos X e Y são invariantes por σ, e, por hipótese, σ atua sem pontos fixos no quociente Y/X. Mas $Xy = X(My)$ é invariante por σ e, assim, como σ atua sem pontos fixos em Y/X, $y \in X$, contradizendo a escolha de Y .

Agora sejam R e S como no enunciado do lema e suponha que σ estabilize a classe lateral $Sr \in R/S$. Como $M \subseteq S$ por hipótese, vemos que Sr é uma união de $|S : M|$ classes laterais a direita de M, que são permutadas por σ. Mas, como $|N : M| = |N : S||S : M|$, temos que $|S : M|$ divide $|N : M|$, que não é divisível por p, pois provamos que $|N : M| \equiv 1 \bmod p$.

Uma pequena modificação do argumento da observação 1.45 abaixo, mostra que σ fixa uma das classes laterais de M em Sr e, assim, $M \subseteq Sr$. Mas temos que $M \subseteq S$ donde $Sr = S$, ou seja, σ atua livre de pontos fixos em todo quociente R/S. □

Observação 1.45 Na demonstração anterior usamos o seguinte resultado:

Seja M um subgrupo de N. Seja $\sigma \in Aut(N)$ de ordem prima p que deixa M invariante. Se a única classe lateral de M em N que fica fixa por σ é M então $|N : M| \equiv 1 \bmod p$.

Demonstração: Seja $n + 1 := |N : M|$ e sejam $M, M_{x_1}, \ldots, M_{x_n}$ as classes laterais de M em N. Então, como elemento de S_n, $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$ onde $\sigma_i's$ são ciclos disjuntos.

Como $o(\sigma)$=mmc(comprimentos de σ_i), usando que $o(\sigma) = p$, temos que todos os σ_i tem comprimento p, (já que σ não fixa nenhuma das n classes), e, assim, $n = kp$.

Portanto $n+1 = kp+1$, e como, por hipótese, $|N : M| = n+1$, temos que $|N : M| \equiv 1 \bmod p$.

□

Teorema 1.46 *Sejam $M \subseteq R \subseteq N$ com $M \lhd\lhd N$, onde N é um grupo finito. Suponha que $\sigma \in Aut(N)$ possua ordem 2 e que M seja invariante por σ. Se σ atua sem pontos fixos em cada fator em alguma série subnormal invariante por σ de M a N, então $R \lhd\lhd N$ e R é invariante por σ.*

Demonstração: O resultado é trivialmente verdadeiro quando $R = N$ e, quando $|N| = 1$. Assim, podemos assumir $M \subseteq R < N$ e $1 < |N|$, e trabalhar por dupla indução: em $|N : R|$ e em $|N|$. Se existe um subgrupo S com $R < S < N$ então, como $|N : S| < |N : R|$ e $M \subseteq S \subseteq N$ satisfazem as hipóteses do teorema, temos que $S \lhd\lhd N$ e S é invariante por σ.

Seja $M = M_0 \lhd M_1 \lhd ... \lhd M_n = N$ a série subnormal de M a N do enunciado do teorema. Pela interseção desta série com S, temos que

$$M \lhd M_1 \cap S \lhd ... \lhd M_{n-1} \cap S \lhd S,$$

ou seja, existe uma série subnormal invariante por σ de M a S, e, pelo Lema 1.44, σ atua sem pontos fixos em cada fator $\dfrac{M_{i+1} \cap S}{M_i \cap S}$ dessa série subnormal . Portanto, como $|S| < |N|$, podemos aplicar a hipótese de indução à situação $M \subseteq R \subseteq S$, donde temos que $R \lhd\lhd S$ e R é invariante por σ.

Assim temos $R \lhd\lhd S$ e $S \lhd\lhd N$ donde $R \lhd\lhd N$.

Agora, consideremos o caso que não existe tal S, ou seja, R é um subgrupo maximal de N. Seja $H = M^N$ o fecho normal de M em N, e escreva $D = R \cap H$. Observe que $H < N$, pois M é próprio em N ($M \subseteq R < N$) e subnormal, que $D \lhd R$ pois $H \lhd N$ e que H é invariante por σ pelo Lema 1.41 (a). Além disso, como R é subgrupo maximal, $R \nsubseteq H$ e assim $|D| < |R|$.

Afirmação: D é invariante por σ e $D \lhd N$.

De fato, temos então $M \subseteq R \cap H \subseteq H$, ou seja $M \subseteq D \subseteq H$. Também $|H| < |N|$ e fazendo a interseção da série subnormal $M = M_0 \lhd ... \lhd M_n = N$ com H temos que $M \lhd M_1 \cap H \lhd ...M_{n-1} \cap H \lhd H$, ou seja, existe uma série subnormal invariante por σ de M a H. Podemos então aplicar o Lema 1.44 e concluir que σ atua sem pontos fixos em cada fator da série subnormal de M a H. Assim, aplicando a hipótese de indução, temos que $D \lhd\lhd H$ e D é invariante por σ . Segue que, ou $D = H$ e, neste caso, $D \lhd N$, ou $N_H(D) > D$. Na última situação, $N_N(D) \nsubseteq R$ e assim $N_N(D) > R$. Segue, da maximalidade de R, que $N_N(D) = N$. Portanto, em ambos os casos, temos $D \lhd N$ e a afirmação está provada.

Então, pelo Lema 1.44, σ age em N/D sem pontos fixos, e como σ possui ordem 2, segue, do Corolário 1.43, que N/D é abeliano. Portanto, todo subgrupo de N/D é normal, e, assim, $R \lhd N$ e portanto, em particular, $R \lhd\lhd N$. Também, pelo corolário 1.43, $\sigma(x) = x^{-1}$ e portanto R é invariante por σ. □

1.7 Grupos Solúveis

Definição 1.47 *Um grupo G é solúvel se possui uma série subnormal cujos fatores são abelianos.*

Teorema 1.48 *Sejam G um grupo, H um subgrupo de G, e N um subgrupo normal de G.*

(1) *Se G é solúvel, então H é solúvel.*

(2) *Se G é solúvel, então G/N é solúvel.*

(3) *Se N e G/N são solúveis, então G é solúvel.*

Demonstração: Veja [7], p. 126. □

Definição 1.49 *Seja G um grupo. O grupo dos comutadores de G, denotado por $[G,G]$, é o subgrupo de G gerado pelo conjunto $\{xyx^{-1}y^{-1} : x, y \in G\}$.*

Definição 1.50 *Dado um grupo G, definimos, por indução, $G^{(0)} = G$ e*

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}], i \geq 1.$$

A série $G^{(0)} \supset G^{(1)} \supset G^{(2)}...$ é chamada série derivada de G.

Teorema 1.51 *Seja G um grupo e $H = [G,G]$. Então $H \lhd G$, G/H abeliano e se $N \lhd G$ com G/N abeliano, então $H \subseteq N$.*

Demonstração: Elementar. □

O seguinte corolário é imediato.

Corolário 1.52 *Se $H = H_n \lhd H_{n-1} \lhd ... \lhd H_1 \lhd H_0 = G$ com $\frac{H_i}{H_{i-1}}$ abeliano, então $G^{(i)} \subseteq H_i$.*

Corolário 1.53 *Seja G um grupo. Então G é solúvel se e somente se existe um inteiro n tal que $G^{(n)} = \{e\}$. Mais geralmente, se $N \lhd G$, G/N é solúvel se e somente se $G^{(n)} \subseteq N$ para algum inteiro n.*

Demonstração: Ver [2], p. 204. □

Teorema 1.54 *Sejam G um grupo de ordem p^m e H subgrupo de G. Então existem subgrupos*

$$H_0 = H \subseteq H_1 \subseteq H_2 \subseteq \ldots \subseteq H_m = G$$

tais que $H_i \lhd H_{i+1}$ e $\frac{H_{i+1}}{H_i}$ é um grupo cíclico de ordem p, para todo $i = 0, ..., m-1$. Em particular G é solúvel e todo subgrupo de G é subnormal.

Demonstração: Pode ser encontrada em [2] p. 166.

□

1.8 Anéis de Grupos

Definição 1.55 *Sejam F corpo, G grupo finito. Definimos*

$$FG = \{\sum \lambda_g g;\ \lambda_g \in F,\ g \in G\}$$

com as seguintes operações:

- $(\sum_{g\in G} \lambda_g g)(\sum_{h\in G} \mu_h h) = \sum \lambda_g \mu_h gh$
- $\sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_{g\in G} (\lambda_g + \mu_g) g$

Pode-se provar que FG é um anel com unidade com estas operações. Além disso, FG possui uma estrutura de F-espaço vetorial:

- $\lambda(\sum_{g\in G} \lambda_g g) = \sum_{g\in G} \lambda\lambda_g g$

Definição 1.56 *Dados V um espaço vetorial de dimensão finita sobre um corpo F e G um grupo, suponha que $\forall v \in V$ e $x \in FG$, esteja definido um único elemento vx de V. Suponha que $\forall x, y \in FG$, $\forall v, w \in V$ e $\forall c \in F$, se tenha:*

(a) $(v + w)x = vx + wx$

(b) $v(x + y) = vx + vy$

(c) $(vx)y = v(xy)$

(d) $(cv)x = c(vx) = v(cx)$

(e) $v.1 = v$

Então V é um FG-módulo.

Observação 1.57 *Se o grupo G atua sobre o F-espaço vetorial V, então V pode ser visto de maneira natural como um FG-módulo.*

Teorema 1.58 (Maschke)

Sejam F um corpo e G um grupo em que a característica de F não divide $|G|$. Então, todo FG-módulo V é completamente redutível, isto é, dado W um FG-submódulo de V, existe W_1 um FG-submódulo de V tal que $V = W \oplus W_1$.

Demonstração: Veja [12], p. 253. □

Vamos usar o Teorema de Maschke em uma situação em que podemos garantir a unicidade de W_1, a saber, a situação descrita no teorema abaixo.

Teorema 1.59 *Sejam F um corpo e G um grupo cuja ordem não é divisível pela característica de F. Seja $N \lhd G$. Seja V um FG-módulo e seja $P \subseteq V$ o conjunto dos pontos fixos de N. Então, P é um FG-submódulo de V, e existe um único submódulo W de V tal que $V = P \oplus W$.*

Para demonstrar esse teorema vamos precisar dos resultados abaixo.

Definição 1.60 *Sejam G um grupo e $V \neq \{0\}$ um FG-módulo. Então, V é um FG-módulo irredutível se os seus únicos submódulos são 0 e V.*

Teorema 1.61 *Seja V um FG-módulo. Então, V é completamente irredutível se e somente se V é soma direta de submódulos irredutíveis.*

Demonstração: Ver [9] p. 5, Teorema 1.10. □

Notação 1.62 *Dados um FG-módulo V completamente redutível e M um FG-módulo irredutível, denotaremos por $M(V)$ a soma de todos os submódulos de V que são isomorfos a M.*

Teorema 1.63 *Seja V um FG-módulo completamente irredutível e suponha que V seja a soma direta de submódulos irredutíveis W_i, $i = 1, \ldots, k$. Seja M um FG-módulo irredutível. Então, $M(V) = \sum_{\substack{i \in \{1,2,\ldots,k\} \\ W_i \cong M}} W_i$.*

Demonstração: Veja [9], p.6, Lema 1.13. □

Demonstração: (Teorema 1.59) Claramente P é um subespaço de V.

Se $x \in P$, $g \in G$ e $n \in P$, então,

$$(xg)n = x(gn) = x(gng^{-1}g) = x(gng^{-1})g = xg,$$

o que mostra que P é realmente um submódulo de V.

A existência de W é garantida pelo Teorema de Maschke. Resta mostrar a unicidade.

Aplicando o Teorema de Maschke a P e a W, podemos escrever P como soma direta de submódulos irredutíveis P_i, $i = 1, ..., n$ e W como soma direta de submódulos irredutíveis W_i, $i = 1, ..., m$, o que nos dá uma decomposição de V em soma direta de submódulos irredutíveis.

Mas, dado M submódulo irredutível de V, no qual a ação de N é não trivial, temos, pelo Teorema 1.63, que $M(V) = \sum_{\substack{i \in \{1,...,m\} \\ W_i \cong M}} W_i$. Assim, $W = \sum M(V)$, onde M percorre os submódulos irredutíveis de V, nos quais a ação de N é não trivial. Mas isto mostra a unicidade de W. □

Capítulo 2

Extensões de Corpos e Teoria de Galois

Neste Capítulo trataremos de extensões normais e separáveis e do teorema Fundamental da Teoria de Galois. Na terceira seção será introduzida a noção de extensão radical, e provaremos alguns resultados que serão úteis nos capítulos 3 e 4. Trataremos apenas de extensões finitas.

2.1 Extensões Normais e Separáveis

Definição 2.1 *O grupo de Galois $Gal(L : K)$ de uma extensão $L : K$ é o grupo de todos os K-automorfismos de L com a composição de funções.*

Definição 2.2 *Uma extensão $L : K$ é normal se todo polinômio irredutível f sobre K que possui uma raiz em L se fatora completamente em L.*

Definição 2.3 *O corpo S é corpo de fatoração ou corpo de raízes sobre K para o polinômio $f(X) \in K[X]$ se $K \subseteq S$ e*

(i) f se fatora completamente sobre S;

(ii) se $K \subseteq S' \subseteq S$ e f se fatora completamente sobre S' então $S = S'$.

Teorema 2.4 *Seja $L : K$ uma extensão finita de corpos. Então, são equivalentes:*

(1) *$L : K$ é normal;*

(2) *L é corpo de fatoração de algum polinômio $f(X) \in K[X]$;*

(3) *Para qualquer extensão normal M de K contendo L, todo K-monomorfismo de M é um K-monomorfismo de L.*

Demonstração: Ver Teoremas 8.4 p. 91 e 10.5 p.109 em [7].

□

Teorema 2.5 *Suponha que $L : K$ seja uma extensão normal finita e α, β sejam raízes em L do polinômio irredutível f sobre K. Então existe um K-automorfismo σ de L tal que $\sigma(\alpha) = \beta$, isto é, $Gal(L : K)$ atua transitivamente nas raízes de f.*

Demonstração: Ver Proposição 10.2, p. 107, em [7].

□

Definição 2.6 *Seja L uma extensão algébrica de K. O fecho normal de $L : K$ é uma extensão E de L tal que*

(i) $E : K$ é normal;

(ii) se $L \subseteq M \subseteq E$ e $M : K$ é normal então $M = E$.

O próximo teorema garante que o fecho normal de uma extensão finita sempre existe.

Teorema 2.7 *Se $L : K$ é uma extensão finita, então existe um fecho normal $\overline{L}$ que é uma extensão finita de K. Se $L : K$ é separável, então $\overline{L} : K$ é separável.*

Demonstração: Ver Teorema 10.3, p. 108, em [7].

□

Definição 2.8 *Um polinômio f, irredutível sobre um corpo K, é separável sobre K, se não possui zeros múltiplos em um corpo de fatoração.*

Se $L : K$ é uma extensão de corpos, então um elemento algébrico $\alpha \in L$ sobre K é separável sobre K, se seu polinômio mínimo sobre K é separável sobre K.

Uma extensão algébrica $L : K$ é uma extensão separável, se todo $\alpha \in L$ é separável sobre K.

Lema 2.9 *Seja $L : K$ uma extensão finita de corpos onde K tem característica zero ou característica de K não divide $|L : K|$. Então $L : K$ é uma extensão separável.*

Demonstração: Ver Proposição 8.6, p. 95, em [7]. □

Definição 2.10 *Dizemos que uma extensão finita $L \supseteq K$ é de Galois, se L for normal e separável sobre K.*

Teorema 2.11 *Seja $L \supseteq K$ uma extensão de Galois. Se L é o corpo de raízes do polinômio $f(X) \in K[X]$ irredutível de grau n, então $Gal(L/K)$ é isomorfo a um subgrupo de S_n.*

Demonstração: Se α é raiz de f, então claramente, se $\sigma \in Gal(L/K)$, $\sigma(\alpha)$ é também raiz de f. Assim, σ permuta as raízes de f. Como σ fica determinado por sua ação no conjunto das raízes de f, temos $Gal(L/K)$ isomorfo a um subgrupo de S_n.

□

2.2 O Teorema Fundamental da Teoria de Galois

Seja $L : K$ uma extensão de corpos com grupo de Galois G. Sejam $\mathcal{F}$ o conjunto de todos os corpos intermediários e $\mathcal{G}$ o conjunto de todos os subgrupos de G. Definimos duas funções:

$$* : \mathcal{F} \to \mathcal{G}$$

$$+ : \mathcal{G} \to \mathcal{F}$$

tais que, se $M \in \mathcal{F}$, M^* é o grupo de todos os M-automorfismos de L, e se $H \in \mathcal{G}$, H^+ é o corpo fixo de H.

Enunciaremos agora o Teorema Fundamental da Teoria de Galois. Sua demonstração pode ser encontrada em [7], p. 114, Teorema 11.1.

Teorema 2.12 (Fundamental da Teoria de Galois)

Se $L : K$ é uma extensão normal e separável de grau n, com grupo de Galois G, e se $\mathcal{F}, \mathcal{G}, *, +$ são descritos acima, então:

(1) *O grupo de Galois G possui ordem n;*

(2) *as funções $*$ e $+$ são mutuamente inversas e temos uma correspondência biunívoca entre $\mathcal{F}$ e $\mathcal{G}$;*

(3) *se M é um corpo intermediário então*

$$|L : M| = |M^*| \quad e \quad |M : K| = |G|/|M^*|;$$

(4) *um corpo intermediário M é uma extensão normal de K se, e somente se, M^* é um subgrupo normal de G;*

(5) *se um corpo intermediário M é uma extensão normal de K então o grupo de Galois de $M : K$ é isomorfo ao grupo quociente G/M^*.*

Corolário 2.13 *Sejam $Q \subseteq E$ uma extensão de Galois e corpos F e L com $Q \subseteq F \subseteq E$ e $Q \subseteq L \subseteq E$. Então*

$$Gal(E/LF) = Gal(E/L) \cap Gal(E/F)$$

e, se F/Q é normal, então

$$Gal(E/L \cap F) = Gal(E/L)Gal(E/F).$$

Demonstração:

Seja $\sigma \in Aut(E)$. É claro que σ deixa FL fixo se e somente se σ deixa F e L fixos. Logo temos que $Gal(E/FL) = Gal(E/F) \cap Gal(E/L)$.

Agora, para a outra igualdade:

É claro que $L \cap F$ é o maior corpo contido em L e F, logo $Gal(E/L \cap F)$ é o menor subgrupo de $Gal(E/Q)$ que contém $Gal(E/L)$ e $Gal(E/F)$, isto é, é o subgrupo $Gal(E/L)Gal(E/F)$. □

Teorema 2.14 .

Sejam F, E e L subcorpos de um corpo Ω e suponha que $E \supseteq F$ é uma extensão de Galois. Seja $K = EL$, a composição. Então K é Galois sobre L e $Gal(K/L) \simeq Gal(E/E \cap L)$. Em particular, $|K : L| = |E : E \cap L|$ e $|K : E| = |L : E \cap L|$.

Demonstração: Ver Teorema 29, p.67, em [5].

□

2.3 Extensões Radicais

Definição 2.15 *Uma extensão $F \subseteq L$ é dita uma extensão radical se $L = F[\alpha]$, em que $\alpha \in L$ é um elemento com $\alpha^n \in F$ para algum inteiro positivo n.*

Teorema 2.16 *Seja $\epsilon \in \mathbb{C}$ uma raiz k-ésima primitiva da unidade. Então, $|\mathbb{Q}(\epsilon) : \mathbb{Q}| = \varphi(k)$, em que $\varphi(k)$ denota o número de inteiros positivos menores do que k e primos com k. Também, $\mathbb{Q}(\epsilon) : \mathbb{Q}$ é de Galois e $Gal(\mathbb{Q}(\epsilon)/\mathbb{Q}) \cong \mathbb{Z}_k{}^*$, o grupo multiplicativo dos inteiros módulo k invertíveis, sendo, portanto, abeliano. Se k é primo,$Gal(\mathbb{Q}(\epsilon)/\mathbb{Q})$ é cíclico.*

Demonstração: Ver Teorema 20, p. 57, em [5].

□

Corolário 2.17 *Sob as hipóteses do Teorema 2.16, suponha que $k = p$ seja primo com $p - 1 = 2n$. Então, existe um único corpo $E \subset \mathbb{Q}(\epsilon)$ com $|E : \mathbb{Q}| = n$. Além disso, $E \subset \mathbb{R}$ e E é Galois sobre $\mathbb{Q}$.*

Demonstração: A existência e unicidade de E, e também o fato de E ser Galois sobre $\mathbb{Q}$, decorrem do Teorema da Correspondência de Galois (Teor. 2.12), e do fato de $Gal(\mathbb{Q}(\epsilon)/Q)$ ser cíclico, possuindo, portanto, exatamente um subgrupo de ordem 2. Como $|\mathbb{C} : \mathbb{R}| = 2$, usando o Teorema 2.14 com $F = \mathbb{Q}$, $E = \mathbb{Q}(\epsilon)$, $L = \mathbb{R}$, obtemos que

$$|\mathbb{Q}(\epsilon) : \mathbb{R} \cap \mathbb{Q}(\epsilon)| = |\mathbb{R}(\epsilon) : \mathbb{R}| \leq |\mathbb{C} : \mathbb{R}| = 2.$$

Como $\epsilon \notin \mathbb{R}$, temos $|\mathbb{Q}(\epsilon) : \mathbb{R} \cap \mathbb{Q}(\epsilon)| = 2$ e $E = \mathbb{Q}(\epsilon) \cap \mathbb{R}$. Portanto $E \subset \mathbb{R}$.

□

Corolário 2.18 *Seja $Q \subset \mathbb{C}$ um corpo qualquer e $\epsilon \in \mathbb{C}$ uma raiz p-ésima primitiva da unidade, com p primo. Então $|Q(\epsilon) : Q|$ divide $p - 1$, $Q(\epsilon)$ é Galois sobre Q e $Gal(Q(\epsilon) : Q)$ é cíclico.*

Demonstração: Conseqüência dos Teoremas 2.16 e 2.14.

□

Vamos precisar da seguinte versão do Teorema 2.16 para o caso de um corpo qualquer:

Teorema 2.19 *Seja Q um corpo e α uma raiz da unidade contida em um corpo $\Omega \supseteq Q$. Então $Q(\alpha) : Q$ é uma extensão abeliana.*

Demonstração: Seja n um inteiro positivo tal que α é uma raiz n-ésima primitiva. Então, como $1, \alpha, ..., \alpha^{n-1}$ são n raízes distintas de $X^n - 1$, temos que $Q(\alpha)$ é corpo de raízes do polinômio separável $X^n - 1$ sobre Q. Logo $Q(\alpha) : Q$ é de Galois.

O fato de $Q(\alpha) : Q$ ser abeliana é conseqüência do fato de se ter, $\forall \sigma \in Gal(Q(\alpha) : Q)$, $\sigma(\alpha) = \alpha^i$, onde i é um inteiro positivo que depende de σ. □

Notação 2.20 *Seja $L : K$ uma extensão de corpos, e $\alpha \in L$ algébrico sobre K. Denotamos por $\min_K(\alpha)$ o polinômio mínimo de α sobre K.*

Lema 2.21 *Sejam $Q \subseteq L$ corpos e suponha que $L = Q[\alpha]$, onde $\alpha^n \in Q$ para algum inteiro $n \geq 1$. Seja $d = |L : Q|$. As seguintes afirmativas são verdadeiras:*

(1) *Em qualquer extensão de L, todas as raízes do polinômio mínimo $\min_Q(\alpha)$ possuem a forma $\delta\alpha$, em que δ é uma raiz n-ésima da unidade;*

(2) *Temos $d \leq n$, e se $\alpha^d \in Q$, então d divide n.*

(3) *Existe uma raiz n-ésima da unidade $\epsilon \in L$, tal que $\epsilon\alpha^d \in Q$. Em particular, se Q contém todas as raízes n-ésimas da unidade em L, então $\alpha^d \in Q$.*

Demonstração: (1) Escreva $a = \alpha^n$; assim, α é uma raiz de $X^n - a \in Q[X]$. O polinômio mínimo $f = min_Q(\alpha)$ divide $X^n - a$ e, desta forma, cada raiz β de f é também raiz de $X^n - a$. Deste modo $\beta^n = a$, donde $\beta = \delta\alpha$, onde δ é uma raiz n-ésima da unidade.

(2) Como $d = \text{grau}\ (f)$, onde $f = \min_Q(\alpha)$, é verdadeiro que $\alpha^r \notin Q$ para todo expoente inteiro $0 < r < d$; em particular, temos $d \leq n$. Escreva $n = qd + r$ com $0 \leq r < d$; vemos que $\alpha^r = \alpha^n(\alpha^d)^{-q}$, que pertence a Q, se $\alpha^d \in Q$. Segue, então, que r não pode ser positivo neste caso e, portanto, $r = 0$. Assim, d divide n.

(3) Como grau $(f) = d$ segue, de (1), que o produto das d raízes de f em um corpo de raízes (contando as multiplicidades) possui a forma $\epsilon\alpha^d$ para alguma raiz n-ésima da unidade ϵ no corpo de raízes. Mas este produto é igual a $\pm f(0)$ e, assim, pertence a Q e, conseqüentemente, a L. Como $\alpha^d \in L$, concluímos que $\epsilon \in L$, como queríamos.

□

Corolário 2.22 *Seja $f(X) = X^p - a \in Q[X]$, em que Q é um corpo e p é um número primo. Então, ou f é irredutível, ou f possui uma raiz em Q.*

Demonstração: Seja α uma raiz de f em alguma extensão $E = Q[\alpha]$ e escreva $m = |E : Q|$. Se $m = p$, então f é irredutível e, assim, podemos supor que $m < p$. Em particular, m e p são primos entre si e podemos encontrar inteiros k e ℓ tais que $mk + p\ell = 1$. Como $\alpha^p \in Q$, sabemos, pelo Lema 2.21 (3), que $\epsilon\alpha^m \in Q$ para alguma raiz p-ésima da unidade ϵ. Assim

$$\epsilon^k\alpha = \epsilon^k\alpha^{mk}\alpha^{p\ell} = (\epsilon\alpha^m)^k(\alpha^p)^\ell \in Q.$$

Como $\epsilon^k\alpha$ é uma raíz de f, isto completa a demonstração. □

Definição 2.23 *Dizemos que um corpo L é quase real se L possui característica zero e as únicas raízes da unidade em L são ± 1.*

Exemplo 2.24 $\mathbb{Q}(\sqrt{2}i)$ é um corpo quase real que não é real.

Lema 2.25 *Seja $Q \subseteq L$ uma extensão radical e assuma que $|L : Q| = p$ onde p é um primo ímpar.*

(1) *Se L é Galois sobre Q, então L contém alguma raiz da unidade diferente de ± 1, e assim L não é quase real.*

(2) *Se L não é Galois sobre Q, então $L = Q[\alpha]$ para algum elemento α com $\alpha^p \in Q$.*

Demonstração: Escreva $L = Q[\alpha]$, onde alguma potência de α pertence a Q, e considere o polinômio mínimo $f = \min_Q(\alpha)$.

(1) Se L é Galois sobre Q, então f possui grau $(f) = p \geq 3$ raízes distintas em L. Pelo Lema 2.21 (1), cada raiz possui a forma $\delta\alpha$ para alguma raiz da unidade $\delta \in L$ e, desta forma, L contém três raízes distintas da unidade donde, no mínimo, uma é diferente de ± 1.

(2) Pelo Lema 2.21 (3), sabemos que $\epsilon\alpha^p \in Q$ para alguma raiz da unidade $\epsilon \in L$, donde temos $Q \subseteq Q[\epsilon] \subseteq L$. Se L não é Galois sobre Q, então $L \neq Q[\epsilon]$. Como $|L : Q|$

é primo, concluímos que $Q[\epsilon] = Q$ e $\epsilon \in Q$, donde segue que $\alpha^p \in Q$.

□

Definição 2.26 *Dizemos que a extensão $Q \subseteq E$ é abeliana se é uma extensão de Galois tal que $Gal(E/Q)$ é um grupo abeliano.*

Lema 2.27 *Sejam $Q \subseteq K \subseteq E$, onde K é abeliano sobre Q. Então existe um corpo F com $Q \subseteq K \subseteq F \subseteq E$ tal que F é abeliano sobre Q e contém todas as raízes da unidade em E.*

Demonstração: Seja $D = \{x \in E |\ x^n = 1$ para algum $n > 0\}$. Seja $L := Q[D] \subseteq E$. Como $|E : Q|$ é finito, então $Q[D]$ pode ser obtido por um número finito de elementos $d_1, ..., d_n \in D$. Logo $F := Q[D] = Q[d_1, ..., d_n] = Q[< d_1, ..., d_n >]$. Evidentemente, $< d_1, ..., d_n > \subseteq E^x$, logo $< d_1, ..., d_n >$ é cíclico. Seja $\alpha \in D$ um gerador de $< d_1, ..., d_n >$. Então $L := Q[D] = Q[\alpha]$.

Observe que $\alpha^n = 1$ para algum $n \geq 1$. Então, pelo Teorema 2.19, $L : Q$ é uma extensão abeliana.

Tome $F = KL$. Pelos Teoremas 2.13 e 2.12(4), temos que $KL : Q$ é de Galois. Resta mostrar que é abeliana.

Sejam $\sigma, \tau \in Aut(F/Q)$. Queremos mostrar que $\sigma \circ \tau = \tau \circ \sigma$, isto é , que $\sigma \circ \tau(x) = \tau \circ \sigma(x)$, $\forall x \in F$. Isto é, que $\sigma \circ \tau(x) = \tau \circ \sigma(x), \forall x \in K \cup L$. Ou ainda que $\sigma \circ \tau(x) = \tau \circ \sigma(x), \forall x \in K$, o que é verdadeiro pois $K : Q$ é abeliano, e $\sigma \circ \tau(x) = \tau \circ \sigma(x), \forall x \in L$, o que é verdadeiro pois $L : Q$ é abeliano.

□

Lema 2.28 *Suponha que L e S sejam, respectivamente, uma extensão radical e uma extensão de Galois sobre algum corpo Q. Se L e S são quase reais, então $|L \cap S : Q| \leq 2$.*

Demonstração: Escreva $L = Q[\alpha]$, onde alguma potência de α está em Q, e seja $m = |L : L \cap S|$. Como L é quase real, as únicas raízes da unidade em L são ± 1.

Biblioteca Universitária
UFSC
0.3406831

Assim, $L \cap S$ contém todas as raízes da unidade em L. Segue, pelo Lema 2.21(3), que $\alpha^m \in L \cap S$. Sejam $\beta = \alpha^m$ e $F = Q[\beta] \subseteq L \cap S$. Observe que α é uma raiz do polinômio $f(X) = X^m - \beta \in F[X]$ e, desta forma, temos

$$m = |L : L \cap S| = |F[\alpha] : L \cap S| \leq |F[\alpha] : F| = \text{grau } (\min(\alpha)) \leq m,$$

o que implica que $L \cap S = F = Q[\beta]$.

Escreva $g = \min_Q(\beta)$ e note que g se fatora completamente sobre S pois, por hipótese, S é Galois sobre Q. Mas alguma potência de α está em Q, e o mesmo é verdadeiro para β, donde segue, do Lema 2.21(1), que toda raiz de g é da forma $\epsilon\beta$, para alguma raiz da unidade $\epsilon \in S$. Como S é quase real, as únicas possibilidades são $\epsilon = \pm 1$ e, assim, g possui no máximo 2 raízes . Como as raízes de g são distintas (Lema 2.9), isto mostra que

$$|L \cap S : Q| = \text{grau } (g) \leq 2.$$

□

Capítulo 3

Corpos Reais e Extensões Radicais Repetidas

Neste Capítulo provaremos os Teoremas A, B, C e D enunciados na Introdução. Para isso, em várias situações neste Capítulo, dada uma extensão separável de corpos $L : Q$, vamos considerar uma extensão de Galois $E : Q$, com $L \subset E$ e, usando o Lema 2.27, um corpo $F \subset E$, abeliano sobre Q, tal que F contém todas as raízes da unidade em E.

Denotaremos $G = Gal(E/Q)$, $U = Gal(E/L)$, $N = Gal(E/F)$. Temos que U é um subgrupo de G e $N \lhd G$. Definiremos $M = U \cap N$. Assim, $M \lhd U$. Observe que, pela correspondência de Galois, $|G : U| = |L : Q|$ e $G/N \simeq Gal(F/Q)$ é abeliano. Além disto, pelo Teorema 2.13, $|G : UN| = |L \cap F : Q|$.

3.1 Extensões Radicais de Grau Primo

Definição 3.1 *Seja K um corpo e seja $f \in K[X]$ um polinômio. Dizemos que f é solúvel por radicais se f se fatora sobre uma extensão $L \supseteq K$ para a qual existe uma cadeia de corpos $K = K_0 \subseteq K_1 \subseteq ... \subseteq K_k = L$ tal que $K_i = K_{i-1}[\alpha_i]$ para $1 \leq i \leq k$, onde α_i possui alguma potência em K_{i-1}. Tal extensão de um corpo K é dita extensão radical repetida de K.*

Nesta seção daremos uma caracterização das extensões radicais repetidas $L : Q$ de grau primo p, com p diferente da característica de Q. Nesta situação, L não pode ser uma extensão radical repetida de Q exceto quando L for de fato uma extensão radical. Podemos considerar apenas primos $p > 2$, já que toda extensão quadrática de corpos de característica diferente de 2 é radical. De fato, se $L : Q$ é uma extensão quadrática, então $L = Q[\alpha]$, em que α satisfaz um polinômio quadrático em $Q[X]$ da forma $X^2 + aX + b$, ou seja,

$$X^2 + aX + \frac{a^2}{4} + \frac{4b}{4} - \frac{a^2}{4},$$

donde temos que

$$\left(\alpha + \frac{a}{2}\right)^2 = \frac{a^2 - 4b}{4}.$$

Como $Q[\alpha] = Q[\alpha + \frac{a}{2}]$ e $(\alpha + \frac{a}{2})^2 \in Q$, temos $L : Q$ radical.

O principal resultado desta seção é o seguinte:

Teorema 3.2 *Seja $Q \subseteq L$, com $|L : Q| = p$, em que p é um primo ímpar não igual à característica de Q. Seja $E \supseteq L$ Galois sobre Q e suponha que $F \subseteq E$ seja abeliano sobre Q e contenha as raízes da unidade em E. Sejam G, N, U e M subgrupos como descritos acima. Então L é uma extensão radical de Q não contida em F se, e somente se, as seguintes condições são verificadas:*

(1) $|N : M| = p$;

(2) $M \lhd N$;

(3) *N/M é U-isomorfo a um subgrupo de E^x, onde E^x denota o grupo multiplicativo de E. (A ação de U em N/M é uma ação via automorfismo internos, isto é $\varphi \in U, \sigma \in N$, então $\overline{\sigma}^{\varphi} := \overline{\varphi^{-1}\sigma\varphi}$. A ação de U num subgrupo de E^x é dada por $\xi^{\phi} := \phi(\xi)$, para $\phi \in U$ e $\xi \in D$).*

Demonstração: Suponha que L seja uma extensão radical de Q não contida em F. Como, por hipótese, $|L : Q| = p$, p primo, temos $L \cap F = Q$. Assim,

pelo Corolário 2.13,

$$UN = Gal(E/L \cap F) = Gal(E/Q) = G.$$

Segue que $|N : M| = |N : U \cap N| = |UN : U| = |G : U| = |L : Q| = p$, o que prova (1).

Além disto, todas as raízes da unidade em L estão em F e, portanto, em Q. Como $|L : Q| = p$ e estamos supondo que L é radical sobre Q, podemos aplicar o Lema 2.21 (3), e escrever $L = Q[\alpha]$, onde $\alpha^p \in Q$.

Tome $\tau \in N \setminus M$. Então, como $M = U \cap N$, $\tau \notin U$ e $\alpha^\tau \neq \alpha$. Como $\alpha^p \in Q$, temos que $\alpha^p = (\alpha^p)^\tau = (\alpha^\tau)^p$ e, portanto, $\left(\frac{\alpha^\tau}{\alpha}\right)^p = 1$. Como $\frac{\alpha^\tau}{\alpha} \neq 1$, temos $\frac{\alpha^\tau}{\alpha} = \epsilon$ onde ϵ é uma raiz p-ésima primitiva da unidade. Escreva $D =< \epsilon > \subseteq E^x$, e note que $|D| = p$.

Como $L[\epsilon]$ é o corpo de raízes sobre Q do polinômio $X^p - \alpha^p \in Q[X]$, vemos que $L[\epsilon]$ é Galois sobre Q. Pelo Teorema 2.14, a composição $L[\epsilon]F$ é Galois sobre Q, pois, ambos $L[\epsilon]$ e F são Galois sobre Q. Como $\epsilon \in F$, $L[\epsilon]F = LF$ e, pelo Teorema 2.13, $Gal(E/LF) = U \cap N = M$.

Logo, pelo Teorema 2.12, $M \lhd N$, o que prova (2).

Como, por (1), $|\frac{N}{M}| = p$ e $\tau \notin M$, temos que a classe lateral $M\tau$ gera N/M e, assim, para um elemento arbitrário $\sigma \in U$, $\tau^\sigma = \mu\tau^s$, para algum inteiro s e algum elemento $\mu \in M$. Para provar (3) mostraremos que $\epsilon^\sigma = \epsilon^s$. Como $\alpha^\tau = \epsilon\alpha$ e σ, e portanto σ^{-1}, assim como μ, fixam α, temos

$$\alpha\epsilon^\sigma = \alpha^\sigma\epsilon^\sigma = (\alpha\epsilon)^\sigma = (\alpha^\tau)^\sigma = \alpha^{\tau\sigma} = \alpha^{\sigma^{-1}\tau\sigma} = \alpha^{\tau^\sigma} = \alpha^{\mu\tau^s} = \alpha^{\tau^s} = \alpha\epsilon^s$$

Então $\epsilon^\sigma = \epsilon^s$ e portanto (3) está verificada.

Suponha que (1), (2), (3) sejam verdadeiras. Vamos provar que L é uma extensão radical de Q não contida em F.

Por (1), temos $|UN : U| = |N : M| = p = |L : Q| = |G : U|$. Assim, $UN = G$.

Pelo Teoremas 2.12 e 2.13 temos $|L \cap F : Q| = |G : UN|$, donde $L \cap F = Q$ e, em particular, $L \not\subseteq F$. Resta agora mostrar que L é radical sobre Q.

Por (1) e (3) temos que E^x possui um subgrupo D que é U-isomorfo a N/M, que possui ordem p. Portanto $D =< \varepsilon >$, em que ε é uma raiz p-ésima primitiva da unidade em E. Escreva $K = L[\varepsilon]$ e $C = Gal(E/K)$. Dessa forma, C é exatamente o conjunto dos elementos em $U = Gal(E/L)$ que fixam ε, ou seja, C é o núcleo da ação de U em D e, portanto, $C \lhd U$. Como, por hipótese, F contém todas as raízes da unidade em E, temos que $\varepsilon \in F$ e, assim, como M fixa os elementos de F, M fixa ε, e temos $M \subseteq C$ e $C \cap M = M$.

Pelo U-isomorfismo entre D e N/M, temos que C atua trivialmente em N/M e, assim, dado $\sigma \in C$, $\tau \in N$, temos

$$\overline{\tau} = \overline{\tau}^{\sigma} = \overline{\sigma^{-1}\tau\sigma} \;\Rightarrow\; \tau^{-1}\sigma^{-1}\tau\sigma \in M \;\Rightarrow\; \tau^{-1}\sigma^{-1}\tau \in M\sigma^{-1} \subset C.$$

Logo, N normaliza C. Como $C \lhd U$ e $UN = G$, temos $C \lhd G$ e, pelo Teorema 2.12 da correspondência de Galois, temos que K é Galois sobre Q.

O grupo G induz transformações Q-lineares em K; escreva $\overline{G}$ para denotar a imagem de G no grupo linear $\Gamma = GL_Q(K)$. A função $\sigma \to \overline{\sigma}$ é um homomorfismo de G em $\overline{G}$, com núcleo $Gal(E/K) = C$. Como $C \cap N = M$, temos, pelo Teorema 1.3, $\overline{N} \simeq \dfrac{NC}{C} \simeq \dfrac{N}{N \cap C} = \dfrac{N}{M}$ e, portanto, $\overline{N}$ possui ordem p. Além disso, $\overline{N}$ pode ser visto como U-grupo ou $\overline{U}$-grupo via as ações

$$\overline{n}^{u} = \overline{n^{u}} \quad \text{e} \quad \overline{n}^{\overline{u}} = \overline{n^{u}}.$$

O isomorfismo acima, entre $\overline{N}$ e $\dfrac{N}{M}$, é claramente um U-isomorfismo. Como, por hipótese, $\frac{N}{M}$ e D são U-isomorfos e C é o núcleo da ação de U em D, temos também que C é o núcleo da ação de U em $\overline{N}$ e, portanto, $\overline{U}$ age fielmente em $\overline{N}$ por conjugação. Como $L \not\subseteq F$, temos que $\overline{N} \not\subseteq \overline{U}$ e, assim, $\overline{G} = \overline{UN}$ satisfaz as hipóteses do Teorema 1.29.

Como $D \subseteq K$, existe um outro subgrupo Δ, de ordem p em Γ, distinto de $\overline{N}$, que é do nosso interesse: aquele que consiste das multiplicações por elementos de D. (Note que $\overline{N}$ fixa o elemento $1 \in K$ enquanto Δ não, e assim $\overline{N}$ e Δ são realmente diferentes). Se $\mu \in \Delta$ corresponde à multiplicação por $\delta \in D$ e a é um elemento de K, então, para $\sigma \in G$, temos

$$\overline{\sigma}\mu\overline{\sigma}^{-1}(a) = \overline{\sigma}(\overline{\sigma}^{-1}(a)\delta) = a\overline{\sigma}(\delta) = a\sigma(\delta).$$

Segue que $\overline{G}$ normaliza Δ em Γ e, também, que Δ e D são G-isomorfos, onde o isomorfismo entre Δ e D e as ações de G são as óbvias.

Como $\overline{N}$ e $\dfrac{N}{M}$ são U-isomorfos e, por hipótese, $\dfrac{N}{M}$ e D são U-isomorfos, então Δ e $\overline{N}$ são U-isomorfos e, portanto, $\overline{U}$ isomorfos.

Lembrando que $\overline{N}$ normaliza e é distinto de Δ, segue que $\overline{N}\Delta$ é um subgrupo abeliano elementar de Γ de ordem p^2, que denotaremos por A. Como $\overline{U}$ atua da mesma maneira em Δ e $\overline{N}$, deduzimos que todo subgrupo de A é $\overline{U}$-invariante. De fato, seja B subgrupo não-trivial próprio de A. Então, como $|A| = p^2$, temos que $|B| = p$ e $B =< x >$, onde $x = \mu\overline{n}$, com $\mu \in \Delta$ e $\overline{n} \in \overline{N}$. Temos, para $\overline{u} \in \overline{U}$, $\mu^{\overline{u}} = \mu^i$ e $\overline{n}^{\overline{u}} = \overline{n}^i$, para algum $i \in \mathbb{N}$, donde $x^{\overline{u}} = \mu^i\overline{n}^i = (\mu\overline{n})^i = x^i \in B$. Concluímos então que todo subgrupo de A é normal em $\overline{U}A = \overline{U}\overline{N}\Delta = \overline{G}\Delta$.

Como assumimos que Q não possui característica p e como $|\overline{N}| = p$, então, pelo Teorema 1.58 (Maschke) aplicado a esta situação, temos que K é completamente redutível como $Q\overline{N}$-módulo. Podemos escrever o Q-espaço K como uma soma direta, $K = P \oplus V$ onde P consiste dos pontos fixos de N e, pelo Teorema 1.59, V é o único Q-subespaço invariante por N, complementar de P, onde N atua sem pontos fixos não triviais. Como N atua não trivialmente em K, vemos que V é não nulo. (O Q subespaço $V \subseteq K$ não é um subcorpo de K já que $1 \notin V$, pois $1^n = 1 \forall n \in N$).

Queremos provar agora que V é invariante por $\overline{U}A$.

Para isso observamos primeiro que K é invariante por $\overline{U}A$. De fato, como $K : Q$ é Galois, temos que K é invariante por U e por N e, portanto, por $\overline{U}$ e $\overline{N}$. Como

$A = \triangle\overline{N}$, e K é obviamente invariante por $\triangle$, temos que K é invariante por $\overline{U}A$.

A seguir, observamos que P é invariante por $\overline{U}A$. De fato, dado $\overline{\sigma} \in \overline{U}A$ e $x \in P$, temos que, se $n \in N$, então $(x^{\overline{\sigma}})^n = x^{\overline{\sigma}n} = x^{\overline{\sigma n}} = x^{\overline{\sigma n \sigma^{-1}}\overline{\sigma}} = x^{\overline{\sigma}}$, ou seja, $x^{\overline{\sigma}}$ é fixo por N e portanto está em P.

De $K = P \oplus V$, obtemos, para $\overline{\sigma} \in \overline{U}A$, $\overline{\sigma}(K) = \overline{\sigma}(P) \oplus \overline{\sigma}(V)$ ou $K = P \oplus \overline{\sigma}(V)$.

Para concluir que $\overline{\sigma}(V) = V$, ou seja, que V é invariante por $\overline{U}A$, basta ver, devido a unicidade de V, que $\overline{\sigma}(V)$ é invariante por N.

Escreva $\overline{\sigma} = \overline{\mu}\overline{\sigma_1}$, onde $\overline{\sigma_1} \in \overline{UN}$ e $\overline{\mu} \in \triangle$, com $\overline{\mu}$ correspondendo à multiplicação por $\delta \in D$.

Dado $v \in V$ e $n \in N$, temos:

$$(v^{\overline{\sigma}})^n = (v^{\overline{\sigma}})^{\overline{n}} = (\delta v)^{\overline{\sigma_1}\overline{n}} = \delta^{\overline{\sigma_1}\overline{n}} v^{\overline{\sigma_1 n \sigma_1^{-1}}\overline{\sigma_1}} = \delta^{\overline{\sigma_1}\overline{n}} v_1^{\overline{\sigma_1}},$$

com $v_1 \in V$.

Como $\delta \in D$ é uma raiz p-ésima da unidade, $\delta \in F$ e $N = Gal(E/F)$, temos que $\delta^{\overline{\sigma_1}\overline{n}} = \delta^{\overline{\sigma_1}}$. Assim, $(v^{\overline{\sigma}})^n = (\delta v_1)^{\overline{\sigma_1}}$. Para ver que $\delta v_1 \in V$, observe que $\mu(K) = K$ e $\mu(P) = P$ já que, se $x \in P$ e $n \in N$, $(\delta x)^n = \delta^n x^n = \delta x$. Assim, de $K = P \oplus V$, obtemos $K = P \oplus \mu(V)$. Mas $\mu(V)$ é invariante por N ($(\mu n)^n = \mu^n v^n = \mu v_1$) e, portanto, pela unicidade de V, temos $\mu(V) = V$. Logo $\delta v_1 \in V$ e está concluída a prova de que V é $\overline{U}A$ invariante.

Como A é abeliano não cíclico de ordem p^2 e atua em $V > 0$, pelo Corolário 1.28, existe algum subgrupo $B \subseteq A$ de ordem p tal que B possui ponto fixo não trivial em V. Seja $W \subseteq V$ o subespaço não nulo dos pontos fixos de B. Vimos que $B \lhd \overline{U}A$; segue, como acima, que W é invariante por $\overline{U}A$. (Este é o ponto principal onde a suposição de que a ação de U em N/M e D ser a mesma é usado; é ela que está por trás do fato de todo subgrupo de A ser normalizado por $\overline{U}$).

O grupo $\overline{U}\,\overline{N} = \overline{G}$ atua em W e $\overline{N}$ não possui ponto fixo não trivial em W, pois $W \subseteq V$ e N, e portanto $\overline{N}$, não possui ponto fixo não trivial em V. Pelo Teorema 1.29, existe um elemento não nulo $\alpha \in W$ fixo por $\overline{U}$, e assim α é fixo por U e $\alpha \in L$. Também, como α não é fixo por $\overline{N}$, $\alpha \notin Q$. Desta forma $L = Q[\alpha]$, e é suficiente

mostrar que $\alpha^p \in Q$ para que L seja uma extensão radical sobre Q.

Como Δ não possui ponto fixo não trivial em K, $\alpha \in W$ é fixo pelo subgrupo $B \subseteq A = \overline{N}\Delta$ e α não é fixo por $\overline{N}$, segue que B contém algum elemento da forma $b = \overline{\tau}\mu$, onde $\overline{\tau}$ gera $\overline{N}$ e $\mu \in \Delta$ é a multiplicação por alguma raiz p-ésima primitiva da unidade δ. Temos

$$\alpha = \alpha^b = (\alpha^{\overline{\tau}})^{\mu} = (\alpha^{\tau})\delta$$

e, assim, $\alpha^{\tau} = \alpha\delta^{-1}$. Deduzimos então que τ fixa α^p, que é, desta forma, fixo por todo $\overline{N}$. Como U fixa α, também fixa α^p; concluímos que α^p é fixo por $\overline{U}\ \overline{N} = \overline{G}$.

Desta forma α^p é fixo por G e, como $G = Gal(E/Q)$, temos que $\alpha^p \in Q$ e portanto L é uma extensão radical sobre Q.

□

Corolário 3.3 *Na situação do Teorema* 3.2, *assuma que L é quase real. Então L é radical sobre Q se, e somente se, as condições* (1), (2) *e* (3) *são verificadas.*

Demonstração: Pelo Teorema anterior, tudo que temos que provar é que se L é radical sobre Q e está contido em F, então L não pode ser quase real. Mas F é abeliano sobre Q por hipótese e, assim, L é Galois sobre Q. Desta forma, pelo Lema 2.25 (1), L não é quase real.

□

3.2 Extensões Radicais Repetidas Quase Reais

Teorema 3.4 *Sejam $Q \subseteq E$, onde E é quase real. Suponha que L e S sejam subcorpos de E que são respectivamente, uma extensão radical repetida e uma extensão de Galois de Q. Então $L \cap S$ é uma extensão quadrática repetida de Q.*

Demonstração: Podemos supor que $L > Q$, e assim podemos encontrar uma extensão radical F de Q tal que $Q < F \subseteq L$. Como S é Galois sobre Q, e S, F são quase reais, temos, pelo Lema 2.28, que $|F \cap S : Q| \leq 2$.

Temos que L é uma extensão radical repetida de F e que a composição FS é Galois sobre F, de acordo com o Teorema 2.14. Como $|L : F| < |L : Q|$, podemos trabalhar por indução em $|L : Q|$ e aplicar a hipótese de indução com F no lugar de Q e FS no lugar de S. Deduzimos que D é uma extensão quadrática repetida de F, onde $D = L \cap FS$. Em outras palavras, existe uma cadeia de extensões de corpos de grau 2, $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_m = D$.

Ainda pelo Teorema 2.14, temos $|FS : F| = |S : F \cap S|$ e, mais geralmente, se X é um corpo tal que $F \subseteq X \subseteq FS$, $|FS : X| = |XS : X| = |S : X \cap S|$ e, portanto, $|X : F| = |X \cap S : F \cap S|$ (veja figura 1).

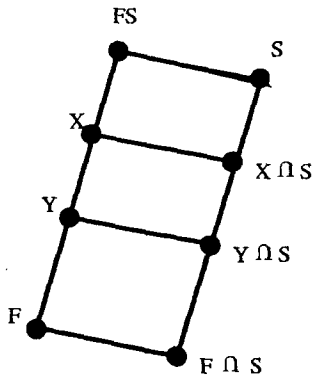

figura 1

Se $X \subseteq Y$ são dois corpos consecutivos na cadeia $\{F_i\}$ de extensões de grau 2 começando com F até D, segue que $|Y \cap S : X \cap S| = |Y : X| = 2$. Concluímos então que os corpos $F_i \cap S$ formam uma cadeia de extensões de grau 2, começando com $F_0 \cap S = F \cap S$ e terminando em $F_m \cap S = D \cap S = L \cap S$. Como $|F \cap S : Q|$ é no máximo 2, temos que $L \cap S$ é uma extensão quadrática repetida de Q, como queríamos.

□

Observação 3.5 Na situação do teorema anterior, quando trabalhamos com corpos de característica diferente de 2, extensões quadráticas são automaticamente extensões radicais e, desta forma, $L \cap S$ é uma uma extensão radical repetida de Q.

Corolário 3.6 *Sejam $Q \subseteq S \subseteq L$, onde L é quase real e S é Galois sobre Q. Se L é uma extensão radical repetida de Q, então $|S : Q|$ é uma potência de 2. Por outro lado, se $|S : Q|$ é uma potência de 2, então pelo menos S é uma extensão radical repetida de Q.*

Demonstração: Se L é uma extensão radical repetida de Q, podemos tomar $E = L$ no teorema anterior e teremos que S é uma extensão quadrática repetida de Q e, conseqüentemente, $|S : Q|$ é uma potência de 2. Por outro lado, se $|S : Q|$ é uma potência de 2, então $Gal(S/Q)$ é um 2-grupo e, pelos Teoremas 1.54 e 2.12, vemos que S é uma extensão quadrática repetida de Q e, assim, uma extensão radical repetida de Q.

□

Lema 3.7 *Sejam $Q \subseteq L$, em que L é quase real. Então L é uma extensão radical repetida de Q se, e somente se, existe uma cadeia de corpos $Q = L_0 \subseteq L_1 \subseteq ... \subseteq L_m = L$ tal que as extensões $L_{i-1} \subseteq L_i$ são extensões radicais de grau primo para cada i com $1 \leq i \leq m$.*

Demonstração: (" $\Leftarrow$ ") Óbvia pela definição de extensão radical repetida.
(" $\Rightarrow$ ") Suponhamos que L seja uma extensão radical repetida de Q, e podemos supor também que $Q > L$. Vamos construir os corpos L_i. Trabalhando por indução em $|L : Q|$ vemos que é suficiente construir $L_1 \subseteq L$ tal que L_1 é uma extensão radical de grau primo sobre Q e L seja uma extensão radical repetida de L_1.

Como, por hipótese, L é uma extensão radical repetida de Q, podemos tomar um elemento $\alpha \in L$ tal que, $\alpha \notin Q$ mas $\alpha^n \in Q$, para algum $n \in \mathbb{N}$. Tome α de modo que n seja o menor possível e observe que isto força n a ser um número primo. Agora escreva $L_1 = Q[\alpha]$ e, assim, L_1 é radical sobre Q. Colocando $d = |L_1 : Q|$, temos $d \leq n$, pelo Lema 2.21(2). Como L é quase real, por hipótese, e $L_1 \subseteq L$, temos que as únicas raízes da unidade em L_1 são ± 1, que estão em Q e, assim, pelo Lema 2.21(3),

$\alpha^d \in Q$. Mas n é o menor inteiro tal que $\alpha^n \in Q$, donde concluímos que $d = n$ e, como n é primo, temos que d é primo, como queríamos.

Agora é imediato verificar que se $Q = M_0 \subseteq M_0(\alpha_1) \subseteq \ldots \subseteq M_0(\alpha_1, \ldots, \alpha_r) = L$, é uma cadeia radical entre Q e L, então $L_1 \subseteq L_1(\alpha_1) \subseteq \ldots \subseteq L_1(\alpha_1, \ldots, \subseteq \alpha_r) = L$ nos dará uma cadeia radical entre L_1 e L.

□

O próximo teorema nos dá uma caracterização das extensões radicais repetidas quase reais, sendo o principal resultado desta seção.

Teorema 3.8 *Suponha $Q \subseteq L$, onde L é quase real. Seja $E \supseteq L$ tal que E Galois sobre Q e suponha que $F \subseteq E$ é abeliana sobre Q e contém todas as raízes da unidade em E. Como usualmente escreva $G = Gal(E/Q)$, $N = Gal(E/F)$, $U = Gal(E/L)$ e $M = N \cap U$. Então L é uma extensão radical repetida de Q se e somente se existe uma cadeia de subgrupos M_i, $i = 0, ..., r$, U-invariantes (a ação de U sobre G é dada por automorfismo interno), onde $M = M_0 \subseteq M_1 \subseteq ... \subseteq M_r = N$, e todas as seguintes condições são verificadas:*

(1) $|F \cap L : Q|$ *é uma potência de 2;*

(2) *cada índice* $|M_i : M_{i-1}|$ *é primo;*

(3) $M_{i-1} \lhd M_i$ *para cada inteiro* i *com* $0 < i \leq r$;

(4) *cada fator* M_i/M_{i-1} *é U-isomorfo a um subgrupo de* E^x;

Antes de passarmos à demonstração, vamos fazer algumas observações que deixarão mais claras as condições do teorema. Supondo (2), (3) e (4), sejam $D_i \subseteq E^x$ subgrupos U-isomorfos a M_i/M_{i-1}. Vemos que $|D_i|=|M_i/M_{i-1}|$ é primo (por (2)) e, assim, os subgrupos D_i são exatamente os grupos $< \delta >$ onde δ percorre as raízes p-ésimas primitivas da unidade em E para divisores primos p de $|N : M|$. Em particular, (4) garante a existência em E de todas estas raízes p-ésimas da unidade. Para ver exatamente que primos são estes, observe que, pelos Teoremas 2.12 e 2.13,

$$\begin{aligned} |N:M| &= |Gal(E/F) : Gal(E/F) \cap Gal(E/L)| \\ &= |Gal(E/F) : Gal(E/FL)| = |E:F|/|E:FL| \\ &= |FL:F| = |L:L \cap F| \end{aligned}$$

e, portanto,

$$|N:M| = |NU:U| = |L:L \cap F|.$$

Se (1) é verdadeiro, então os divisores primos ímpares de $|N:M|$ são exatamente os divisores primos ímpares de $|L:Q|$, e isto mostra que uma conseqüência das quatro condições é que E contém uma raiz p-ésima primitiva da unidade para cada divisor primo p de $|L:Q|$.

Agora observe que $G/N \simeq Gal(F/Q)$, que é abeliano por hipótese. Assumindo (2) e (3), vemos que os grupos M_i/M_{i-1} são abelianos, pois $|M_i : M_{i-1}|$ é primo e, portanto, os termos sucessivos da série derivada de G estão contidos nos subgrupos M_i com índice decrescente i (Corolário 1.52). Isto diz que os termos da série derivada de G eventualmente estão em M e, conseqüentemente, G/H é solúvel para todo subgrupo normal H de G com $H \supseteq M$ (Corolário 1.53). Em particular, isto vale para todo subgrupo normal H de G que contém U. Traduzindo esta última conclusão para teoria de corpos, vemos que (2) e (3) garantem que se $Q \subseteq K \subseteq L$ e K Galois sobre Q, então $Gal(K/Q)$ é solúvel. Isto é exatamente o que esperaríamos pelo Teorema Fundamental da Teoria de Galois se L realmente é uma extensão radical repetida de Q.

Demonstração: Suponha primeiro que $F \cap L = Q$ e, portanto, pelo Teorema 2.13, $UN = G$. Nesta situação, mostraremos que L é uma extensão radical repetida de Q se, e somente se, existe uma cadeia de subgrupos para os quais as condições (2), (3) e (4) do teorema são satisfeitas. Pelo Lema 3.7, L é uma extensão radical repetida de Q se, e somente se, existe uma cadeia de corpos $Q = L_0 \subseteq L_1 \subseteq ... \subseteq L_m = L$ tal que

as extensões $L_{i-1} \subseteq L_i$ são extensões radicais de grau primo para cada inteiro i com $1 \leq i \leq m$.

Resta mostrar que a existência de uma cadeia de corpos como acima é equivalente às três condições (2), (3) e (4) do teorema.

Pelo Teorema 2.12, sabemos que todo corpo intermediário A com $Q \subseteq A \subseteq L$ corresponde a um subgrupo W com $U \subseteq W \subseteq G$ tal que $|L : A| = |W : U|$. Também, nesta situação, onde $UN = G$, existe uma correspondência bijetiva entre os subgrupos W com $U \subseteq W \subseteq G$ e subgrupos R U-invariantes com $M \subseteq R \subseteq N$ (Subgrupos W e R se correspondem se $R = W \cap N$ ou, equivalentemente, se $W = UR = \{u \circ r; u \in U, r \in R\}$). Se W e R se correspondem, temos $|W : U| = |R : M|$.

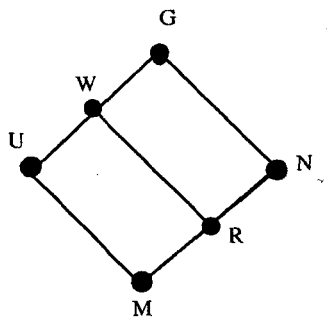

figura 2

Segue, do comentado acima, que a existência de uma cadeia de subgrupos U-invariantes satisfazendo a condição (2) é exatamente equivalente a existência de uma torre de corpos começando em Q e terminando em L, onde cada extensão sucessiva possui grau primo.

Agora considere corpos intermediários A e B com $Q \subseteq A \subseteq B \subseteq L$ onde $|B : A| = p$, um número primo, e sejam R e S, respectivamente, os correspondentes subgrupos U-invariantes de N. Assim, temos $M \subseteq S \subseteq R \subseteq N$ e $|R : S| = p$. Escreva $W = Gal(E/A)$ e $V = Gal(E/B)$. Temos $R = W \cap N$ e $S = V \cap N = V \cap W \cap N = V \cap R$. Vamos mostrar que B é uma extensão radical de A se e somente se $S \lhd R$ e R/S é U-isomorfo a um subgrupo de E^x.

Se $p = 2$, então B é uma extensão quadrática de A e, automaticamente, uma

extensão radical. Também, neste caso, $|A : B| = 2$, isto é, $|R : S| = 2$ e, assim, $S \lhd R$ e R/S é U-isomorfo ao subgrupo $< -1 > \subseteq E^x$. Podemos assumir então que $p > 2$ e usar o Teorema 3.2 e Corolário 3.3 com A e B no lugar dos corpos Q e L.

O corpo E do enunciado do teorema é Galois sobre A e, assim, serve como o corpo E do Teorema 3.2. Para o corpo F do Teorema 3.2, tome a composição AF, que é abeliano sobre A, pelo Teorema 2.14, e certamente contém todas as raízes da unidade em E. No Teorema 3.2 temos $U = Gal(E/L)$, que corresponde aqui a $V = Gal(E/B)$. Também no Teorema 3.2 tínhamos $N = Gal(E/F)$, que aqui corresponde a $Gal(E/AF) = Gal(E/A) \cap N = R$. Finalmente o grupo M do Teorema 3.2 era $U \cap N$, que aqui corresponde ao grupo $V \cap R = S$. Então podemos aplicar o Corolário 3.3 com V, R e S no lugar de U, N e M respectivamente, e segue que B é radical sobre A se, e somente se, $S \lhd R$ e R/S é V-isomorfo a um subgrupo de E^x. Resta mostrar neste caso, então, que R/S é U-isomorfo a $< \epsilon >$ se, e somente se, R/S é V-isomorfo a $< \epsilon >$, onde ϵ é uma raiz p-ésima primitiva da unidade em E. Como $U \subseteq V$, vemos que se R/S e $< \epsilon >$ são V-isomorfos automaticamente serão U-isomorfos. Para provar a recíproca, isto é, supondo R/S e $< \epsilon >$ U-isomorfos mostrar que são V-isomorfos, observe que S atua trivialmente (por conjugação) em R/S, e também em $< \epsilon >$, pois $\epsilon \in F$ e $S \subseteq N = Gal(E/F)$. Mas $V = US$ e, assim, vemos que se R/S e $< \epsilon >$ são U-isomorfos, são também V-isomorfos, como queríamos.

Finalmente, vamos considerar o caso em que não assumimos que $L \cap F = Q$. Aplicando os argumentos anteriores com $L \cap F$ no lugar de Q (e UN no lugar de G) vemos que L é uma extensão radical repetida de $L \cap F$ se, e somente se, as condições (2), (3) e (4) são verificadas. Observe que $L \cap F$ é uma extensão de Galois sobre Q pelo fato de F ser abeliano sobre Q. Supondo (1) verdadeiro, isto é, $|F \cap L : Q|$ uma potência de 2, temos que $L \cap F$ é uma extensão radical repetida de Q pelo Corolário 3.6. Se todas as quatro condições são verdadeiras, então L é uma extensão radical repetida de $L \cap F$, que é uma extensão radical repetida de Q e, assim, L é uma extensão radical repetida de Q, como queríamos. Por outro lado, se L é uma extensão

radical repetida de Q, a condição (1) é satisfeita, pelo Corolário 3.6. Também, sendo L uma extensão radical repetida de Q, então L é uma extensão radical repetida de $L \cap F$ e assim (2), (3) e (4) são verdadeiras. Isto completa a demonstração.

□

3.3 Extensões Quadráticas Repetidas

Nesta seção provaremos os Teoremas A e D.

Observação 3.9 A composição de extensões quadráticas repetidas é ainda uma extensão quadrática repetida. De fato, sejam $L_1 : K$ e $L_2 : K$ extensões quadráticas repetidas, com $K \subseteq K_0 \subseteq \cdots \subseteq K_n = L_1$ e $K \subseteq K_0' \subseteq \cdots \subseteq K_m' = L_2$, em que todas as extensões intermediárias são quadráticas.

Vamos começar mostrando que $|K_0'L_1 : L_1| = 1$ ou 2 . Mas isto decorre do Teorema 2.14, pois $|K_0' : K_0' \cap L_1| = |K_0'L_1 : L_1|$. Da mesma forma, temos que $|K_1'K_0'L_1 : K_0'L_1| = 1$ ou 2. Observe que $K_1'K_0'L_1 = K_1'L_1$. Prosseguindo desta maneira, e eliminando as extensões triviais, obtemos a cadeia de extensões quadráticas

$$K \subseteq K_0 \subseteq \cdots \subseteq K_n = L_1 \subset K_0'L_1 \subseteq \cdots \subseteq K_m'L_1 = L_1L_2,$$

o que mostra que $L_1L_2 : K$ é uma extensão quadrática repetida.

Lema 3.10 *Seja $Q \subseteq L$ uma extensão quadrática repetida de corpos de característica diferente de 2, e seja E o fecho normal de L sobre Q. Então E é Galois sobre Q e $|E : Q|$ é uma potência de 2. Em particular, todo corpo intermediário entre Q e E é uma extensão quadrática repetida de Q.*

Demonstração: O grau de $|L : Q|$ é uma potência de 2 e, conseqüentemente, não é divisível pela característica de Q que, por hipótese, é diferente de 2. Segue, pelo Lema 2.9, que L é separável sobre Q e, conseqüentemente, E é de fato Galois sobre Q. Escreva $G = Gal(E/Q)$.

Como L é uma extensão quadrática repetida de Q, assim também será L^σ para todo automorfismo $\sigma \in G$. Como a composição de duas extensões quadráticas repetidas de Q é ainda uma extensão quadrática repetida, vemos que o corpo $J =< L^\sigma | \sigma \in G >$ é também uma extensão quadrática repetida de Q. Mas J é invariante sob G. Portanto, pelo Lema 2.4, J é Galois sobre Q, donde temos que $J = E$. Assim E é uma extensão quadrática repetida de Q e $|E : Q|$ é uma potência de 2, como queríamos.

Mas G é um 2-grupo e, assim, pelo Teorema 1.54, para todo subgrupo $H \subseteq G$ existe uma cadeia de subgrupos começando com H e terminando em G, cada qual com índice 2 no próximo subgrupo. Segue do Teorema 2.12, da correspondência de Galois, que se $Q \subseteq K \subseteq E$, então existe uma cadeia de corpos começando em K e terminando em Q, cada qual com grau 2 sobre o próximo corpo. Isto completa a demonstração.

□

O próximo teorema inclui o Teorema A e generaliza-o para corpos quase reais.

Teorema 3.11 *Sejam $Q \subseteq E$, em que E é quase real, e suponha que $f \in Q[X]$ seja irredutível e se fatore completamente sobre E. Se alguma raiz de f está em uma extensão radical repetida de Q contida em E, então o corpo de raízes S para f sobre Q em E tem grau potência de 2, sendo, portanto, uma extensão quadrática repetida de Q. Em particular,* grau (f) *é uma potência de 2 e qualquer corpo K entre Q e S é uma extensão quadrática repetida de Q.*

Demonstração: Seja $L \subseteq E$ extensão radical repetida de Q contendo uma raiz α de f. Então $\alpha \in L \cap S$, onde S é o corpo de raízes para f sobre Q em E. Segue que S é o fecho normal de $L \cap S$ sobre Q. Pelo Teorema 3.4, sabemos que $L \cap S$ é uma extensão quadrática repetida de Q e, conseqüentemente, grau $(f) = |Q[\alpha] : Q|$ é uma potência de 2. Também, pelo Lema 3.10, temos que S é de Galois sobre Q e $|S : Q|$ é uma potência de 2. Portanto, pelo Corolário 3.6, S é uma extensão radical repetida

de Q e a demonstração está completa.

□

Provamos, a seguir, o Teorema D.

Teorema 3.12 *Suponha $Q \subseteq L$, uma extensão radical repetida de corpos de característica diferente de 2. Se $|L : Q|$ é uma potência de 2, então todo corpo intermediário entre Q e L é uma extensão quadrática repetida de Q.*

Demonstração: (Lenstra)

Pelo Lema 3.10, é suficiente mostrar que L é uma extensão quadrática repetida de Q. Vamos trabalhar por indução sobre o grau de L sobre Q. Se $L = Q$ é óbvio que vale a tese. Podemos então supor que $L > Q$, e tomar um elemento $\alpha \in L$ tal que $\alpha \notin Q$, mas $\alpha^p \in Q$ para algum inteiro positivo p. Escolhendo α tal que p seja o menor possível, é claro que p é primo.

Seja $K = Q[\alpha]$; então, como $|L : Q| > |L : K|$ e L é uma extensão radical repetida de K de grau potência de 2, a hipótese de indução se aplica à extensão L sobre K, isto é, L é uma extensão quadrática repetida de K.

Resta mostrar, então, que K é uma extensão quadrática repetida de Q.

Seja $a = \alpha^p \in Q$. Então α é uma raiz do polinômio $f(X) = X^p - a \in Q[X]$. Se f é irredutível sobre Q, então $|K : Q| = \text{grau } (f) = p$. Mas como $|L : Q|$ é uma potência de 2, também $|K : Q|$ é uma potência de 2 e, como p é primo, vemos que $|K : Q| = 2$ e K é uma extensão quadrática sobre Q. Se, por outro lado, f é redutível sobre Q, temos, pelo Corolário 2.22, que f possui alguma raíz $\beta \in Q$. Então α/β é uma raíz p-ésima da unidade que gera K sobre Q. Neste caso, K é Galois sobre Q e, como $|K : Q|$ é uma potência de 2, segue dos Teoremas 2.12 e 1.54 que existe uma cadeia de corpos, começando com K e terminando em Q, cada qual com grau 2 sobre o próximo e, portanto, K é uma extensão quadrática repetida de Q.

□

3.4 Extensões Radicais Repetidas de Grau Ímpar

O Teorema B, a seguir, prova que, em alguns casos, corpos intermediários de extensões radicais repetidas são ainda extensões radicais repetidas.

Teorema 3.13 *Sejam Q um corpo real e $Q \subseteq L$ uma extensão radical repetida, com $|L : Q|$ ímpar. Se $Q \subseteq K \subseteq L$, então K é uma extensão radical repetida de Q.*

Demonstração: Podemos assumir $L \subseteq \mathbb{C}$. Tome uma extensão Galoisiana $E \supseteq Q$ com $L \subseteq E \subseteq \mathbb{C}$ (Teorema 2.7 e Lema 2.9) e escreva $G = Gal(E/Q)$. Como Q é real, E é invariante sob a conjugação complexa (Teorema 2.4); seja $\sigma \in G$ a restrição da conjugação à E. Escreva $U = Gal(E/L) \subseteq G$ e note que $|G : U| = |L : Q|$, que é ímpar, por hipótese e, assim, pelo teorema de Sylow, algum conjugado U^τ de U em G contém σ (veja Observação 3.14, a seguir).

Como $L : Q$ é uma extensão radical repetida se, e somente se, $L^\tau : Q$ é uma extensão radical repetida e, como $Gal(E/L^\tau) = U^\tau$, podemos supor que $\sigma \in U$. Como $U = Gal(E/L)$, temos que $L \subseteq \mathbb{R}$ e, em particular, L é quase real, o que nos permite aplicar o Teorema 3.8.

Seja $F \subseteq E$ abeliano sobre Q, tal que F contenha todas as raízes da unidade em E; escreva $N = Gal(E/F)$ e $M = N \cap U$, como usualmente. Queremos mostrar que K é uma extensão radical repetida de Q. Para isto vamos verificar as condições do Teorema 3.8 para K. Assim, defina $V = Gal(E/K) \supseteq U$ e $R = V \cap N \supseteq M$; vamos trabalhar com V e R no lugar de U e M.

Por (1) aplicado a L, sabemos que $|F \cap L : Q|$ é uma potência de 2. Mas, por hipótese, $|L : Q|$ é ímpar e, assim, $F \cap L = Q$ e $K \cap F = Q$, e (1) está verificada para K. Também, nesta situação, $UN = G$ e, assim, $|N : M| = |G : U| = |L : Q|$, que é ímpar. Falta verificar (2), (3) e (4) para K.

As condições (2), (3) e (4) para L nos dizem que $M \lhd\lhd N$ e que existe uma U-série de composição $\mathfrak{X}$ de N, tendo M como um de seus termos, tal que cada fator de $\mathfrak{X}$ acima de M é U-isomorfo a um grupo de raízes da unidade de ordem prima. Como

$|N : M|$ é ímpar, estes primos são todos ímpares e, assim, a conjugação complexa atua livre de pontos fixos em cada um destes grupos das raízes da unidade. Como σ, a restrição da conjugação a E, pertence a U, σ atua livre de pontos fixos em cada fator de $\mathfrak{X}$ acima de M. Como σ tem ordem 2, já que E não é real (Terema 3.11), podemos aplicar o Teorema 1.46 para concluir que $R \lhd\lhd N$.

Como $R \lhd\lhd N$, podemos aplicar o Lema 1.41 para construir uma série subnormal de R a N, tal que todo automorfismo de N que estabiliza R também estabiliza cada um dos fatores da série. Como $R \lhd V$ e $N \lhd G$, a conjugação por elementos de V é um automorfismo de N que estabiliza R e, portanto, a série subnormal construída é uma V-série. Essa série pode ser refinada a uma V-série de composição para N, que tem R como um dos seus termos. Mas $V = UR$. De fato, observamos primeiro que UR é realmente subgrupo de V, já que $U, R \subseteq V$ e $R \lhd V$. Também, $UR = Gal(E/L)(Gal(E/K) \cap Gal(E/F)) = Gal(E/L).Gal(E/FK)$, onde a última igualdade segue do Corolário 2.13. Apesar de não termos aqui L/Q ou KF/Q normais, podemos concluir, como na prova do Corolário 2.13, já que temos que $Gal(E/L).Gal(E/KF)$ é subgrupo de G, que $Gal(E/L).Gal(E/KF) = Gal(E/L \cap KF)$. Mas, como $L \cap F = Q$, temos que $L \cap KF = K$, concluindo o que queríamos: $V = UR$. Mas R atua (via automorfismos internos) trivialmente em cada um dos fatores de $\mathcal{Y}$ acima de R e, portanto, esses fatores são U-simples e, pelo Teorema 1.40 de Jordan Hölder, são U-isomorfos a algum dos fatores acima de M na U-série de composição $\mathfrak{X}$. Em particular, cada fator Y de $\mathcal{Y}$ acima de R é U-isomorfo a algum subgrupo $D \subseteq E^x$ de ordem prima. As condições (2) e (3) do Teorema 3.8 são portanto verificadas.

Para completar a demonstração é suficiente mostrar que Y e D são de fato V-isomorfos. Mas D consiste de raízes da unidade e, assim, $D \subseteq F$ e N atua trivialmente em D, pois $N = Gal(E/F)$. Em particular, R atua trivialmente em D (pois $R \subseteq N$). Como R também atua trivialmente em Y, $V = UR$ e, como sabemos que Y e D são

U-isomorfos, é verdadeiro que Y e D são V-isomorfos, como queríamos.

□

Observação 3.14 Na demonstração anterior usamos o seguinte:

Se $|G : U|$ é ímpar, então algum conjugado U^τ de U em G contém σ.

De fato, como $|G : U|$ é ímpar, algum 2-subgrupo de Sylow S de G está contido em U. Como $\sigma \in G$ tem ordem 2, σ está contido em algum 2-subgrupo de Sylow de G (Teorema 1.14). Seja S_1 tal subgrupo. Mas sabemos que todos os subgrupos de Sylow de uma determinada ordem são conjugados (Teorema 1.14), donde temos que $S_1 = S^\tau \subseteq U^\tau$, para algum $\tau \in G$, e portanto $\sigma \in U^\tau$.

Seja $f \in Q[X]$ irredutível, onde Q é um corpo real e f possui ao menos uma raiz em alguma extensão radical repetida real de Q. Pelo Teorema A, sabemos que, se todas as raízes de f são reais, então grau(f) é uma potência de 2. No caso oposto a este, o Teorema C afirma que f pode ter somente uma única raiz real. Vamos demonstrá-lo agora.

Teorema 3.15 *Sejam Q um corpo real e $f \in Q[X]$ irredutível de grau ímpar. Se f possui alguma raiz α em alguma extensão radical repetida real L de Q, então α é a única raiz real de f.*

Demonstração: Por hipótese, f possui alguma raiz α em alguma extensão radical repetida real L de Q, que podemos considerar contido em $\mathbb{C}$. Consideremos um corpo E Galois sobre Q, com $Q \subseteq L \subseteq E \subseteq \mathbb{C}$ (Teorema 2.7 e Lema 2.9). Seja $F \subseteq E$ abeliano sobre Q e tal que F contenha todas as raízes da unidade em E. Sejam $G = Gal(E/Q)$, $U = Gal(E/L)$, $N = Gal(E/F)$ e $M = U \cap N$, como usualmente. Assim, as quatro condições do Teorema 3.8 são satisfeitas para uma cadeia de subgrupos apropriada. Note que f se fatora completamente sobre E, e nos resta mostrar então que α é a única raiz real de f em E.

Mostraremos, primeiro, que podemos assumir que $L \cap F = Q$. Para ver isto, escreva $K = L \cap F$ e note que $Q[\alpha] \subseteq K[\alpha]$. Segue que grau $(f) = |Q[\alpha] : Q|$ divide

$|K[\alpha] : K||K : Q|$, pois $|K[\alpha] : Q| = |K[\alpha] : K||K : Q|$ e também $|K[\alpha] : Q| = |K[\alpha] : Q[\alpha]||Q[\alpha] : Q|$. Como, por hipótese, grau (f) é ímpar e $|K : Q|$ é uma potência de 2, pela primeira condição do Teorema 3.8, temos que grau (f) divide $|K[\alpha] : K|$. Como grau $(f) \geq |K[\alpha] : K|$, temos grau $(f) = |K[\alpha] : K|$. Segue disto que f é irredutível sobre K. Já que L é uma extensão radical repetida de K (por ser uma extensão radical repetida de Q) podemos trabalhar com K no lugar de Q deixando E e F conforme anteriormente. (Note que E é Galois sobre K, já que E Galois sobre Q. E, também, que F é abeliano sobre K). Podemos, assim, assumir que $L \cap F = Q$, como queríamos, e assim temos $UN = G$ (Teorema 2.13).

Seja $\beta \in E$ uma raiz real de f; mostraremos que $\alpha = \beta$. Como $G = UN$ atua transitivamente nas raízes de f em E (pelo Teorema 2.5) e U fixa α (pois $\alpha \in L$ e $U = Gal(E/L)$), existe um elemento em N que manda α em β.

Pelo Teorema 3.8, temos uma série subnormal U-invariante $\mathfrak{X}$ de M a N com fatores U-isomorfos a subgrupos de E^x de ordem prima. Seja X o menor termo em $\mathfrak{X}$ que contem um elemento τ que manda α em β. Se $X = M$, então $\tau \in M \subseteq U = Gal(E/L)$, e τ fixa $\alpha \in L$. Neste caso $\beta = \alpha^\tau = \alpha$, como queríamos. Podemos assim assumir que $X > M$. Seja Y o termo exatamente inferior a X na série $\mathfrak{X}$. Em particular, $M \subseteq Y \lhd X$ e X/Y é U-isomorfo a $< \epsilon >$, onde ϵ é uma raíz p-ésima primitiva da unidade em E para algum primo p.

Seja agora $\sigma \in G$ a restrição da conjugação complexa a E. Note que $\sigma \in U$, já que L é real. Assim $X^\sigma = X$ (pois $X \in \mathfrak{X}$ que é U-invariante e $\sigma \in U$) e, em particular, $\tau^\sigma \in X$ e $\tau^\sigma\tau^{-1} \in X$. Também, como β e α são ambos reais, temos que

$$\alpha^{\tau^\sigma} = \alpha^{\sigma\tau\sigma^{-1}} = \sigma\tau\sigma^{-1}(\alpha) = \sigma\tau(\alpha) = \sigma(\beta) = \beta = \alpha^\tau.$$

Assim $\tau^{-1}\tau^\sigma$ fixa α e, conseqüentemente, está em X_α, onde X_α é o estabilizador de α em X.

Pela minimalidade de X, vemos que nenhum elemento de Y manda α em β e, assim, não podemos ter $X = X_\alpha Y$. Como $Y \lhd X$ possui índice primo, deduzimos

que $X_\alpha \subseteq Y$. Temos que $G_\alpha = \{\delta \in G : \delta(\alpha) = \alpha\} = Gal(Q(\alpha)/Q)$. Assim, $|G : G_\alpha| = |Q(\alpha) : Q| =$ grau (f), que é ímpar. Como $X \lhd\lhd G$, temos, pelo Corolário 1.31, que $|X : X_\alpha| = |X : X \cap G_\alpha|$ divide $|G : G_\alpha|$. Logo, $|X : X_\alpha|$ é ímpar, o que implica que $|X/Y|$ é ímpar.

Como $\sigma \in U$ inverte os elementos de $< \epsilon >$ (pois σ é a restrição da conjugação complexa a E), deduzimos que σ inverte os elementos de X/Y e, desta forma, nenhum elemento de X/Y diferente da identidade é fixo por σ. Mas $\tau^{-1}\tau^\sigma \in X_\alpha \subseteq Y$. Logo $\tau^\sigma Y \subseteq \tau Y$, o que mostra que a classe lateral $Y\tau$ é um ponto de X/Y fixo por σ. Donde concluímos que $\tau \in Y$, o que contraria a escolha de X, concluindo a demonstração.

□

Corolário 3.16 *Seja $Q \subseteq \mathbb{R}$ um corpo real. Seja $f(X) \in Q[X]$ irredutível cujas raízes são todas reais. Seja $L \subseteq \mathbb{R}$ o corpo de fatoração de $f(X)$ sobre Q. Então L está contido numa extensão radical repetida real de Q se e somente se $|L : Q|$ é potência de 2.*

Demonstração: (" $\Rightarrow$") Suponha que $|L : Q|$ não seja potência de 2 e seja H um 2-subgrupo de Sylow de $Gal(L/Q)$; então $H \subsetneq Gal(L/Q)$. Seja H^+ o corpo fixo de H. Temos $Q \subsetneq H^+$ e, para $\alpha \in H^+/Q$, o polinômio $f(x) = min_Q(\alpha)$ é irredutível de grau ímpar maior que 1. Como $|L : Q|$ é normal, todas as raízes de $f(x)$ estão em L e são reais (pois $L \subseteq \mathbb{R}$), o que é absurdo pelo Teorema 3.15.
(" $\Leftarrow$") Se $|L : Q|$ é uma potência de 2, então $Gal(f(X)/Q)$ é um 2-grupo, logo existe uma seqüência subnormal $\{e\} = H_0 \lhd H_2 \lhd \ldots \lhd H_r = Gal(f(X)/Q)$ tal que $|H_i : H_{i-1}| = 2 \ \forall i$. Os corpos fixos correspondentes nos dão o que queremos. □

Capítulo 4

Exemplos e Observações Adicionais

Sejam Q um corpo real e $f \in Q[X]$ irredutível de grau n. Suponha que f possua uma raiz em alguma extensão radical repetida real de Q. Pelo Teorema A, grau $(f) = n$ é uma potência de 2. Damos abaixo um exemplo de que pode acontecer de f ter as n raízes reais.

Seja p um primo tal que $p \equiv 1 \bmod 2n$ (existe pelo Teorema de Dirichlet), e seja E a única extensão de grau n sobre $\mathbb{Q}$ contida no corpo gerado pelas raízes p-ésimas da unidade (Corolário 2.17). Ainda por esse Corolário, E é um corpo real e $Gal(E/\mathbb{Q})$ é um 2-grupo (cíclico). Segue que E é uma extensão radical repetida de $\mathbb{Q}$ (Teoremas 1.54 e 2.12). Tomando f como o polinômio mínimo sobre $\mathbb{Q}$ para algum elemento gerador de E, temos o exemplo procurado.

Por outro lado, se $n = \text{grau } (f)$ é ímpar, então o Teorema C nos diz que f possui somente uma raiz real. Isto nos sugere que, em geral, quando n não é necessariamente ímpar ou potência de 2, o número de raízes reais de f é no máximo a maior potência de 2 que divide n. Isto não é verdadeiro. Daremos um exemplo de um polinômio irredutível $f \in \mathbb{Q}[X]$ de grau 6, que possui quatro raízes reais, sendo que exatamente uma delas está em uma extensão radical repetida real de $\mathbb{Q}$. (Isto também mostra que nem todas as raízes reais de um polinômio irredutível sobre $\mathbb{Q}$ são necessariamente semelhantes, pois é possível que alguma delas esteja em uma extensão radical repetida

real e as outras não).

Exemplo 4.1 Seja $f(x) = (x^3 - 3x + 3)^2 - 3 = x^6 - 6x^4 + 6x^3 + 3x^2 - 9x + 6$.

Note que f de fato é irredutível pois, pelo critério de Eisenstein, tomando $q = 3$, temos:

(a) $3 \nmid 1$;

(b) $3 \setminus -6$, $3 \setminus 6, 3 \setminus 3$ *e* $3 \setminus -9$;

(c) $3^2 \nmid 6$.

Agora, fatorando $f(x) = (x^3 - 3x + 3 + \sqrt{3})(x^3 - 3x + 3 - \sqrt{3})$, investigaremos as raízes complexas de cada fator.

Seja $h(x) = x^3 - 3x + a$, onde a é um número real. Pelo teste da derivada segunda, verificamos que $h(x)$ possui ponto de máximo local em $x = -1$ e ponto de mínimo local em $x = 1$. Também o gráfico de $y = h(x)$ encontra o eixo x três vezes se, e somente se, $h(-1) > 0$ e $h(1) < 0$. Como $h(-1) = a + 2$ e $h(1) = a - 2$, segue que h possui três raízes reais se, e somente se, $-2 < a < 2$. Vemos que isto é claramente satisfeito quando $a = 3 - \sqrt{3}$, enquanto não é satisfeito por $a = 3 + \sqrt{3}$. Assim, $u(x) = x^3 - 3x + 3 + \sqrt{3}$ possui apenas uma raiz real, enquanto $v(x) = x^3 - 3x + 3 - \sqrt{3}$ possui três raízes reais. Portanto, $f(x)$ possui quatro raízes reais, como queríamos.

Observe que cada um dos polinômios u e v é irredutível sobre $\mathbb{Q}[\sqrt{3}]$, já que, do contrário, um destes polinômios, e desta forma f, teria uma raiz em $\mathbb{Q}[\sqrt{3}]$, o que é impossível pelo fato de f ser irredutível sobre $\mathbb{Q}$ e grau $(f) = 6$.

Pelo Teorema A, nenhuma raiz de v pode estar em uma extensão radical repetida de $\mathbb{Q}[\sqrt{3}]$ e, assim, nenhuma está em uma extensão radical repetida de $\mathbb{Q}$.

Resta mostrar que a única raiz real de u está em uma extensão radical repetida de $\mathbb{Q}$ (observe que isto não contradiz Teorema A, visto que u não se fatora completamente sobre $\mathbb{R}$). Para isto, é suficiente mostrar que ela está em uma extensão radical repetida de $\mathbb{Q}[\sqrt{3}]$.

O seguinte resultado nos será útil.

Teorema 4.2 *Seja Q um corpo real e suponha que $f \in Q[X]$ seja um polinômio cúbico irredutível que possui exatamente uma raiz real α. Então α está em uma extensão radical repetida real de Q.*

Note que a recíproca do teorema anterior também é verdadeira. Se um polinômio irredutível cúbico f possui uma raiz real em uma extensão radical repetida real de Q, então, pelo Teorema C, α é a única raiz real de f. O Teorema A também pode ser usado: se f possuísse duas raízes reais então, como f é um polinômio cúbico, temos que f se fatoraria completamente sobre $\mathbb{R}$ e, pelo Teorema A, teríamos que grau (f) seria uma potência de 2, o que não é verdadeiro. Assim f possui exatamente uma raiz real.

Provaremos um teorema mais geral que o Teorema 4.2. Relembramos:

Teorema 4.3 *Se K é um corpo de característica zero, e $K \subseteq L \subseteq M$, onde $M : K$ é uma extensão radical, então o grupo de Galois de $L : K$ é um grupo solúvel.*

Demonstração: A demonstração pode ser encontrada em [7] p. 141. □

Definição 4.4 *Um número primo é de Fermat se for da forma $F_n = 2^{2^n} + 1$, $n \geq 0$.*

Teorema 4.5 *Sejam Q um corpo real, p um primo de Fermat e $f \in Q[X]$ um polinômio irredutível de grau p, solúvel por radicais sobre Q. Se f não se fatora completamente sobre $\mathbb{R}$, então f possui alguma raiz que está em uma extensão radical repetida real de Q.*

Demonstração: Seja S o corpo de raízes para f sobre Q em $\mathbb{C}$, e seja $H = Gal(S/Q)$. Assim, H é isomorfo a um subgrupo solúvel de S_p, (Teoremas 2.11 e 4.3). Como dois p-ciclos que geram subgrupos distintos, geram A_p, temos, no caso $p \geq 5$ e trivialmente se $p < 5$, que H possui um subgrupo normal P de ordem p. Pelos Teoremas 1.8 e 1.9, H/P é isomorfo a um subgrupo de Aut(P), que, pelo Teorema 1.16, é um grupo cíclico de ordem p -1, que, em nosso caso, onde p é um primo de Fermat, possui ordem

potência de 2. Segue, pela correspondência de Galois, que existe um corpo T com $Q \subseteq T \subseteq S$, tal que T é abeliano sobre Q e onde $|S : T| = p$ e $|T : Q|$ é uma potência de 2.

Defina $E = S[\epsilon]$, onde ϵ é uma raiz p-ésima primitiva complexa da unidade. (É possível que se tenha $\epsilon \in S$ e, neste caso, teremos $E = S$). Note que $Q[\epsilon]$ é Galois sobre Q e $|Q[\epsilon] : Q|$ divide $p - 1$ (Corolário 2.18), que é uma potência de 2. Como $E = SQ[\epsilon]$ é uma composição de extensões de Galois sobre Q, vemos que E é Galois sobre Q e, pelo Teorema 2.14,

$$|E : S| = |Q[\epsilon] : Q[\epsilon] \cap S| \quad \text{e} \quad |Q[\epsilon] : Q| = |Q[\epsilon] : Q[\epsilon] \cap S||Q[\epsilon] \cap S : Q|.$$

Donde $|E : S|$ divide $|Q[\epsilon] : Q|$ e assim $|E : Q| = |E : S||S : T||T : Q| = 2^n p$, para algum inteiro positivo n.

Seja $\sigma \in G = Gal(E/Q)$ a restrição da conjugação complexa a E (Teorema 2.4), e escreva $U =< \sigma >$ e $L = E \cap \mathbb{R}$. Como E não é real, σ é diferente da identidade. Portanto, U tem ordem 2. Como $U \subseteq Gal(E/L)$ e $|E : L| \leq |\mathbb{C} : \mathbb{R}| = 2$, temos que $|E : L| = 2$ e $U = Gal(E/L)$. Por hipótese, grau$(f) = p$ é ímpar e, portanto, f possui ao menos uma raiz real, digamos $\alpha \in L$. Mas f não se fatora completamente sobre $\mathbb{R}$, e, portanto, também não sobre L. Assim, L não é Galois sobre Q e U não é normal em G.

Para completar a demonstração usaremos o Teorema 3.8 para mostrar que L é uma extensão radical repetida de Q. Para isto precisamos de um corpo $F \subseteq E$ abeliano sobre Q que contenha todas as raízes da unidade em E. Pelo fato de T ser abeliano sobre Q, pelo Lema 2.27, podemos escolher F contendo T. Como $Gal(F/Q)$ é abeliano, se $\alpha \in F$, teríamos $Q[\alpha]$ normal sobre Q, o que implicaria que f se fatoraria completamente sobre $Q[\alpha] \subseteq \mathbb{R}$, contrariando a hipótese. Portanto $\alpha \notin F$. Assim $T \subseteq F \cap S < S$ e, como $|S : T| = p$ é primo, temos que $F \cap S = T$. Também, como $\epsilon \in F$, $SF = E$ e, assim, pelo Teorema 2.14, $|E : F| = |S : T| = p$. Escrevendo $N = Gal(E/F)$ como usual, vemos que $|N| = p$. Agora podemos verificar as quatro

condições do Teorema 3.8. Como $N \lhd G$, (pois $Gal(F/Q)$ é abeliano), $|N| = p$ e $|U| = 2$, temos que $|UN| = 2p$. Assim, $|F \cap L : Q| = |G : UN|$, que é uma potência de 2, pois $|G| = 2^n p$. Isto verifica a primeira condição do Teorema 3.8.

Observe que $M = U \cap N$ é trivial, e como $|N| = p$, a segunda e terceira condição são verificadas para a cadeia de subgrupos $M \subseteq N$.

Para verificar a quarta condição, precisamos mostrar que N é U-isomorfo a $< \epsilon >$. Mas o elemento σ de U, o único diferente da identidade, inverte os elementos de $< \epsilon >$. Assim, é suficiente mostrar que U atua não trivialmente em N. (Como $Aut(N)$ é cíclico, pelo Teorema 1.16, a única possibilidade da ação não trivial de U no grupo N é inverter todos os elementos de N). Como U tem ordem 2, é suficiente mostrar que U não é normal em UN. Observe que $UN \lhd G$, já que $G/N \simeq Gal(F/Q)$ é abeliano. Se $U \lhd UN$, então U é um subgrupo característico de UN pois, pelo Teorema 1.14, U seria o único subgrupo de ordem 2 de UN. Mas, pelo Teorema 1.5, isso implicaria $U \lhd G$. Sabemos que este não é o caso e, portanto, U inverte os elementos de N e, assim, N é U-isomorfo a $< \epsilon >$.

□

Completamos assim o argumento de que o polinômio de grau 6 irredutível sobre Q, do Exemplo 4.1, de fato possui exatamente quatro raízes reais, uma das quais está em uma extensão radical repetida de Q.

Na situação do Teorema 4.5, sabemos que α está em uma extensão radical repetida real de Q, mas não se tem necessariamente que a extensão $Q \subseteq Q[\alpha]$ é radical (repetida). Isto mostra que, em geral, subcorpos de extensões radicais repetidas reais de um corpo real Q não são necessariamente extensões radicais repetidas de Q. Mais adiante daremos um exemplo disto sobre os números racionais $\mathbb{Q}$.

Definição 4.6 *O discriminante* Δ *do polinômio cúbico* $x^3 + bx + c$ *é* $4b^3 + 27c^2$.

Observação 4.7 As raízes do polinômio cúbico $x^3 + bx + c$ são dadas por

$$x = \sqrt[3]{-\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} + \sqrt[3]{-\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}}.$$

Cada raiz cúbica pode assumir três valores complexos, mas o produto das duas deve ser $\frac{-b}{3}$.

Teorema 4.8 *Seja $f \in Q[X]$ um polinômio cúbico irredutível, onde Q é um corpo quase real. Suponha que α é uma raíz de f em alguma extensão de Q e que $Q[\alpha]$ é uma extensão radical repetida de Q. Então o discriminante de f é $-3m^2$ para algum elemento $m \in Q$.*

Demonstração: Seja S o corpo de raízes para f sobre Q e seja Δ o discriminante de f. Como $|Q[\alpha] : Q| = 3$, vemos que $Q[\alpha]$ precisa de fato ser uma extensão radical de Q. Como $Q[\alpha]$ não é Galois sobre Q, pelo Lema 2.25 $Q[\alpha] = Q[\beta]$ para algum β com $\beta^3 \in Q$. O polinômio $X^3 - \beta^3$ é irredutível em $Q[X]$ e, portanto, se fatora sobre S. Logo, S contém a raíz cúbica primitiva da unidade $w = (\frac{-1+\sqrt{-3}}{2})$ e, assim, S contém $\sqrt{-3}$. Como Q é quase real, temos que $w \notin Q$ e $Gal(S/Q)$ possui ordem 6, pois $|Q[\alpha] : Q| = 3$ e $|Q[w] : Q| = 2$. Logo, $Gal(S/Q)$ é isomorfo ao grupo simétrico S_3.

Como S_3 contém um único subgrupo de ordem 3, temos que S contém uma única extensão quadrática T de Q e T é Galois sobre Q. Mas Δ não é um quadrado em Q, pois se $\sqrt{\Delta} \in Q$, pela expressão das raízes de uma equação cúbica, $Gal(S/Q)$ teria ordem 3. Portanto, $\sqrt{\Delta}$ e $\sqrt{-3}$ estão em T e o único automorfismo de T diferente da identidade leva $\sqrt{\Delta}$ em $-\sqrt{\Delta}$ e $\sqrt{-3}$ em $-\sqrt{-3}$. Assim, $\sqrt{\Delta}/\sqrt{-3}$ é fixo por $Gal(T/Q)$ e, conseqüentemente, está em Q. Em outras palavras, $\Delta/(-3)$ é um quadrado em Q, como queríamos, isto é, $\Delta/(-3) = m^2 \in Q$.

□

Exemplo 4.9 Existe um polinômio cúbico irredutível sobre $\mathbb{Q}$ possuindo uma única raiz real α, onde $\mathbb{Q}[\alpha]$ não é uma extensão radical repetida de $\mathbb{Q}$. Vamos mostrar que $f(X) = X^3 - 3X + 3$ possui esta propriedade.

De fato, pelo critério de Eisenstein, é fácil ver que f é irredutível. Também, como o termo constante de f não está entre -2 e 2, sabemos, pela mesma análise feita no Exemplo 4.1, que f possui somente uma raiz real α.

Temos, neste caso, $\Delta(f) = -135$, que não é da forma $-3m^2$ com $m \in Q$. Portanto, pelo Teorema 4.8, temos que $Q[\alpha]$ não é uma extensão radical repetida de Q.

Existe um teorema análogo ao Teorema 4.2 para polinômios quadráticos. Embora este resultado possa também ser provado usando o Teorema 3.8, vamos usar um argumento alternativo.

Teorema 4.10 *Sejam Q um corpo real e $f \in Q[X]$ um polinômio de grau quatro irredutível que possui exatamente duas raízes reais. Então, cada raiz real de f está em uma extensão radical repetida real de Q.*

Demonstração: Sejam α, β, γ, δ as quatro raízes distintas de f, em que α e β são reais e γ e δ são complexas conjugadas. Defina os números $r = \alpha\beta + \gamma\delta$, $s = \alpha\gamma + \beta\delta$ e $t = \alpha\delta + \beta\gamma$, e observe que r é real (pois $\alpha\beta, \gamma\delta \in \mathbb{R}$) e que s e t são distintas, já que $s - t = \alpha\gamma + \beta\delta - \alpha\delta - \beta\gamma = (\alpha - \beta)(\gamma - \delta) \neq 0$. Também s e t são não reais e conjugadas.

Afirmamos que r está contido em alguma extensão radical repetida real L de Q. Para ver isto, observe que o grupo S_4 e, portanto o grupo de Galois de f sobre Q, permuta o conjunto $\{r, s, t\}$. Este grupo fixa, assim, os coeficientes do polinômio $g(x) = (x - r)(x - s)(x - t)$, donde deduzimos que $g \in Q[X]$. Se g é redutível sobre Q, então $|Q[r] : Q| \leq 2$ e, neste caso, $Q[r]$ é uma extensão radical de Q e podemos tomar $L = Q[r]$. Por outro lado, se g é irredutível sobre Q, como r é a única raiz real de g, segue, pelo Teorema 4.2, que L existe.

Seja $u = \alpha\beta\gamma\delta$. Observe que $u \in Q \subseteq L$, pois qualquer Q-automorfismo fixa este elemento. Temos $r\alpha\beta = (\alpha\beta)^2 + u$, e, assim, $\alpha\beta$ satisfaz uma equação quadrática sobre

L. Assim $L[\alpha\beta]$é um corpo real de grau no máximo 2 sobre L e, conseqüentemente, $L[\alpha\beta]$ é uma extensão radical repetida de Q. Substituindo L por $L[\alpha\beta]$, podemos assumir que $\alpha\beta \in L$.

Agora seja $v = \alpha+\beta+\gamma+\delta \in Q \subseteq L$. Então $(\alpha+\beta)(v-(\alpha+\beta)) = (\alpha+\beta)(\gamma+\delta) = s+t = (r+s+t)-r \in L$ já que $r+s+t \in Q$. Assim $\alpha+\beta$ satisfaz uma equação quadrática sobre L, e pensando da mesma forma que antes, podemos substituir L por $L[\alpha+\beta]$ e assumir que $\alpha+\beta \in L$. Finalmente, como ambos $\alpha\beta$ e $\alpha+\beta$ estão em L, vemos que $|L[\alpha] : L| \leq 2$ e, assim, α e β estão na extensão radical repetida real $L[\alpha]$ de Q.

□

Vamos mostrar agora que a hipótese de Q ser real no Teorema 3.13 não pode ser removida.

Exemplo 4.11 Existem corpos $Q \subseteq K \subseteq L \subseteq \mathbb{C}$, onde L é uma extensão radical repetida de Q e $|L : Q|$ é ímpar, mas onde K não é uma extensão radical repetida de Q.

De fato, seja $L = \mathbb{Q}[\epsilon]$, onde ϵ é uma raiz primitiva 19-ésima da unidade; assim, $|L : \mathbb{Q}| = 18$ (Teorema 2.16). Seja Q a única extensão quadrática de $\mathbb{Q}$ em L e seja K o único corpo de grau 3 sobre Q em L (Teorema 2.16 e Teorema 1.15). Agora $L = Q[\epsilon]$ é uma extensão radical de Q de grau 9. Afirmamos que a extensão cúbica $Q \subseteq K$ não é uma extensão radical repetida de Q. Para isto é suficiente mostrar que K não é uma extensão radical de Q.

As únicas raízes da unidade em L são as 38-ésimas (veja Obs.4.12, a seguir) e, assim, as únicas raízes da unidade em K são ± 1. Sabemos que K é Galois sobre Q já que $Gal(L/Q)$ é abeliano e, como $|K : Q| = 3$, vemos, pelo Lema 2.25 (1) que K não pode ser radical sobre Q.

Observação 4.12 *Se $L = Q[\epsilon]$ onde ϵ é uma raiz 19-ésima primitiva da unidade. Então as únicas raízes da unidade em L são as 38-ésimas.*

De fato, seja $\alpha \in L$ uma raiz n-ésima primitiva.

Afirmamos que, se $n \neq 2$, então n não pode ser primo com 19. De fato, caso contrário, $\alpha\epsilon$ seria uma raiz (19.n)-ésima primitiva e, como, $\varphi(19.n) = 18.\varphi(n)$, devemos ter $\varphi(n) = 1$ para que $\varphi(19.n)$ divida 18.

Também, se p é um número primo tal que $p|n$, temos que $\beta = \alpha^{\frac{n}{p}}$ é uma raiz p-ésima primitiva e, pelo argumento acima, devemos ter $p = 2$ ou $p = 19$.

Portanto, as únicas possibilidades são $n = 2$, $n = 19$ ou $n = 19.2$.

Observe também que, realmente, as raízes 38-ésimas estão em L, já que $-\epsilon$ é uma delas.

Referências Bibliográficas

[1] Adilson Gonçalves. Introdução à Álgebra. IMPA - Rio de Janeiro, 1999.

[2] Arnaldo Garcia e Yves Lequain. Álgebra, um Curso de Introdução. IMPA, Rio de Janeiro, 1988.

[3] Carlos Gustavo Moreira. *Um Teorema sobre Solubilidade de Equações Polinomiais por Radicais Reais.* Matemática Universitária **12** (1990), pp. 87-93.

[4] Carlos Gustavo Moreira. *Sobre solubilidade por Radicais Reais.* Matemática Universitária **16** (1994), pp. 60-66.

[5] Emil Artin. Galois Theory. Notre Dame Math.Lectures, 1944.

[6] Francisco Cesar Polcino Milies. Anéis e Módulos. IME, Universidade de São Paulo - São Paulo, 1972.

[7] Ian Stewart. Galois Theory. Chapman e Hall Ltd, London, 1973.

[8] I. M. Isaacs. *Solutions of Polinomials por Real Radicals.* Amer. Math. Monthly **92** (1985), 571-575.

[9] I. M. Isaacs. *Character Theory of Finite Groups.* Academic Press - New York, 1976.

[10] I. M. Isaacs e David Petrie Moulton. *Real Fields e Repeated Radical Extensions.* Journal of Algebra **201** (1998), 429-455.

[11] Joseph J. Rotman. The Theory of Groups - An Introducion. Allyn and Bacon, Inc. - Boston, 1973.

[12] Nathan Jacobson. Basic Algebra II. W. H. Freeman and Company - New York, 1985.

[13] N. Tschebotaröv e H. Schwerdtgeyer, Grundzüge der Galoischen Theorie - P. Noordhoff, 1950.