Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

Solubilidade de Equações Polinomiais por Radicais Reais e Cálculo do Grupo de Galois em $\mathbb{Q}[X]$

Dissertação de Mestrado

DANIELLE SANTOS AZEVEDO

Porto Alegre, 15 de agosto de 2012

Dissertação submetida por Danielle Santos Azevedo*, como requisito parcial para a obtenção do grau de Mestre em Ciência Matemática, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:

Prof. Dra. Cydara Cavedon Ripoll

Banca examinadora:

Prof. Dra. Cydara Cavedon Ripoll (PPGMAT-UFRGS, Orientador)

Prof. Dr. Alveri Alves Sant'Ana (PPGMAT-UFRGS)

Prof. Dr. Antonio Paques (PPGMAT-UFRGS)

Prof. Dr. Dirceu Bagio (PPGMAT-UFSM)

*Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)

Agradecimentos

Primeiramente, quero dedicar este trabalho a meus pais que apoiaram-me em todos os acontecimentos de minha vida, que em épocas difíceis sempre encontraram uma forma de me ajudar. Eu só me tornei essa pessoa que sou hoje devido aos valores que vocês sempre me ensinaram, os quais eu jamais vou esquecer. Amo vocês de tal forma que todo esse sentimento nem cabe dentro do meu peito. Muito obrigada por tudo, obrigada por existirem na minha vida, sou extremamente feliz por ter vocês.

Agradeço à Deus, por eu ter conseguido chegar até aqui. Sei que tenho um caminho longo para trilhar ainda, mas graças à Ele sei que tudo vai dar certo.

Sou eternamente muito grata à Rene Carlos que sempre me incentiva a alcançar meus objetivos e que me ajuda a conquistá-los. Muito obrigada pelo carinho e amor que você demonstra por mim a cada dia. Tivemos que ficar distantes, fisicamente, mas mesmo assim sempre senti teu apoio, tanto nos momentos bons quanto nos ruins. Obrigada por tudo.

Quero agradecer aos meus amigos maravilhosos Andrea, Grasiela, Josiane e Thiago. Sem vocês que graça teria ir para a sala de café da pós? Nenhuma. Cada um, com seu jeito, me marcou muito. Como não lembrar das aulas de álgebra comutativa com a presença da Deinha, do sotaque bonitinho da Grasi, das minhas conversas (ou fofocas) demoradas com a Josi e, claro, impossível esquecer do meu melhor amigo, Thiago, que sempre sabe quando eu estou precisando de um ombro amigo ou quando estou feliz demais. Adoro vocês.

Fico grata pelos ensinamentos da minha Professora orientadora Cydara Cavedon Ripoll, pessoa que me acompanhou desde o início da minha vida universitária. Muito obrigada por ter me orientado. Com certeza, a senhora é um exemplo para mim e farei questão de segui-lo durante toda a vida. E, agradeço, também, aos professores que aceitaram participar da minha banca: Alveri Alves Sant'Ana, Antonio Paques e Dirceu Bagio.

Resumo

Neste trabalho apresentamos um teorema que explicita condições necessárias e suficientes para que um polinômio $f(X) \in \mathbb{Q}[X]$ seja solúvel por radicais reais, juntamente com algumas aplicações do mesmo. Além disso, mostramos que em $\mathbb{Q}[X]$ sempre é possível encontrar o grupo de Galois de qualquer polinômio $f(X) \in \mathbb{Q}[X]$.

Abstract

In this text we present a Theorem which gives necessary and sufficient conditions for a polynomial $f(X)$ with rational coeficients to be soluble by real radicals, as well as some applications of this result. We also show that it is always possible to explicit the Galois group of any polynomial $f(X) \in \mathbb{Q}[X]$.

Índice

Introdução

Antigamente, um dos grandes problemas da Matemática era conseguir expressar as soluções de equações polinomiais. Estudavam-se as equações procurando e explorando fórmulas que expressassem suas raízes através de expressões radicais. Somente no século XIX é que Évariste Galois mostrou que existem irracionais algébricos que não podem ser expressos por meio de uma fórmula algébrica (como as raízes da equação $X^5 - X - 1$).

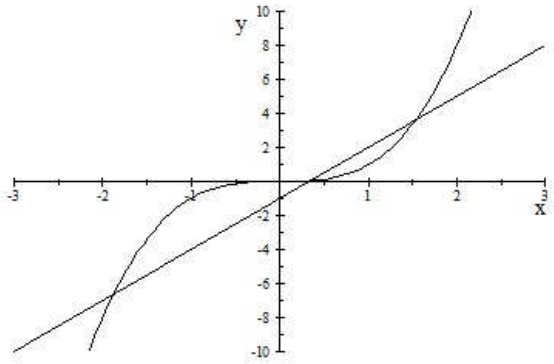
Em seus argumentos Galois utilizou os rudimentos do que hoje chamamos Teoria de Grupos associando a cada equação polinomial um conjunto de permutações das raízes de tal equação. Já a versão contemporânea da teoria de Galois envolve Teoria de Grupos e Extensões de Corpos.

Um curso introdutório sobre Teoria de Galois apresenta um teorema que permite decidir se um polinômio qualquer com coeficientes racionais possui ou não raízes solúveis por radicais. Por exemplo, dado um polinômio $f(X) \in \mathbb{Q}[X]$ irredutível, o corpo $\mathbb{Q}(\text{raízes de } f)$ é chamado corpo de raízes do polinômio $f(X)$ e o grupo de Galois de f é o grupo formado pelos $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\text{raízes de } f)$. Tem-se então que o polinômio $f(X)$ é solúvel por radicais se, e somente se, o grupo de Galois de f sobre $\mathbb{Q}$ é um grupo solúvel[†].

[†]Uma generalização desse teorema é: Sobre um corpo K de característica zero, um polinômio

Como o grupo S_n é solúvel para $n \in \{1, 2, 3, 4\}$, temos que todos os polinômios do 1º, 2º, 3º e 4º graus são sempre solúveis por radicais, havendo até fórmulas explícitas para as raízes dessas equações[‡]. Mas essas fórmulas não bastam para responder se sempre é possível expressar todas as raízes de um polinômio usando apenas radicais reais. Em 1545, Cardano descobriu que a fórmula que hoje conhecemos por fórmula de Tartaglia-Cardano para equações cúbicas já evidenciava esse problema, pois existem equações do 3º grau com todas as três raízes reais cujas expressões por radicais, dadas por essa fórmula, envolvem números complexos. Um exemplo disso é a equação $X^3 - 3X + 1 = 0$.

De fato, considerando a intersecção dos gráficos de $Y = X^3$ e $Y = 3X - 1$ podemos visualizar que todas as raízes da equação $X^3 - 3X + 1 = 0$ são reais e distintas, uma é negativa e as outras duas são positivas. Veja a figura abaixo:

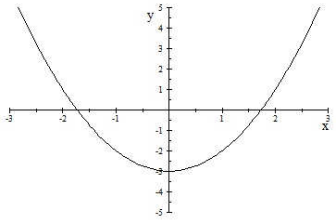


Provemos isso através de argumentos de Cálculo I. Temos que $X^3 - 3X + 1 = X(X^2 - 3) + 1$, então esboçamos o gráfico de $f(X) = X^3 - 3X + 1$ da seguinte

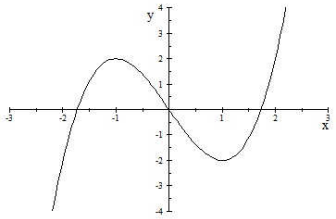
f é solúvel por radicais se, e somente se, o grupo de Galois de f sobre K é solúvel.

[‡]Dada a equação $X^4 + aX^3 + bX^2 + cX + d = 0$ fazemos uma substituição do tipo $X = Y + t$ e obtemos $Y^4 + (4t + a)Y^3 + ... = 0$. Então tomando $t = \frac{-a}{4}$, obtemos uma equação do tipo $Y^4 + k_1Y^2 + k_2Y + k_3 = 0$, sem termo em Y^3. Após alguns cálculos, resolvendo a equação $X^3 + \frac{k_1}{2}X^2 + \frac{({k_1}^2 - 4k_3)}{16}X - (\frac{k_2}{8})^2 = 0$ obtemos raízes x_1, x_2 e x_3 tais que $y = \sqrt{x_1} + \sqrt{x_2} + \sqrt{x_3}$ satisfaz $Y^4 + k_1Y^2 + k_2Y + k_3 = 0$. Para obter as raízes de $X^4 + aX^3 + bX^2 + cX + d = 0$, basta diminuir $\frac{a}{4}$ das raízes de $Y^4 + k_1Y^2 + k_2Y + k_3 = 0$.

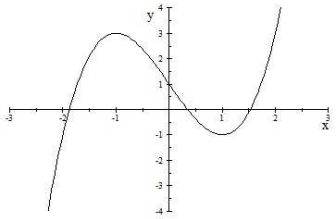
forma: partindo do gráfico da função $Y = X^2 - 3$,



e multiplicando a função acima por X obtemos a função ímpar $Y = X(X^2 - 3)$:



Para obter o gráfico de f, basta deslocarmos verticalmente em uma unidade o gráfico para cima. Note que $f'(X) = 3X^2 - 3$ então $f'(X) = 0 \Leftrightarrow x = \pm 1$. Logo, $x = 1$ é um ponto crítico. Como $f(1) = -1 < 0$, garantimos que $f(X)$ tem 3 raízes reais.



A fórmula de Tartaglia-Cardano para obter as soluções de uma equação do tipo $X^3 + pX + q = 0$ é

$$x = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

o que implica, no nosso caso, que

$$x = \sqrt[3]{\frac{-1}{2} + \sqrt{\frac{1}{4} - 1}} + \sqrt[3]{\frac{-1}{2} - \sqrt{\frac{1}{4} - 1}}$$

isto é,

$$x = \sqrt[3]{\frac{-1}{2} + \sqrt{\frac{-3}{4}}} + \sqrt[3]{\frac{-1}{2} - \sqrt{\frac{-3}{4}}}$$

e tal expressão envolve números complexos; todavia, o esperado seria uma expressão que somente envolvesse números reais, uma vez que todas as raízes desta equação são reais.

Em 1572, Bombelli introduziu o conceito de números complexos, o que não foi bem aceito por Cardano, uma vez que ele estava há cerca de 20 anos procurando alternativas para calcular as raízes que não usassem raízes quadradas de números negativos. Em outras palavras, Cardano procurava outra escrita para a expressão dada acima que não passasse pelos números complexos[§].

É sempre possível expressar todas as raízes de um polinômio f usando radicais reais, quando $f(X) \in \mathbb{Q}[X]$ irredutível tiver todas as raízes reais e for solúvel por radicais?

Em caso negativo, quais são precisamente os polinômios que admitem uma tal expressão? No decorrer do trabalho discutiremos mais especificamente o que foi exposto nesse primeiro momento, juntamente com as questões aqui colocadas. As referências para esta parte são ([6]), ([7]) e ([8]). É em ([6]) que encontramos a resposta para a questão acima e que é um dos principais resultados apresentados neste trabalho:

Teorema 2.1.5 (Teorema de Solubilidade por Radicais Reais) *Seja $f(X) \in \mathbb{Q}[X]$ irredutível tal que todas as raízes de f são reais (mais precisamente, irracionais). Então f é solúvel por radicais reais se, e somente se, a ordem de*

[§]Cardano morreu atormentado por esse questionamento, pois não aceitava a resposta negativa para a mesma, ele pensava que era ele quem não conseguia encontrar uma solução para o problema. Para maiores detalhes veja em [7].

$Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})$ é uma potência de 2. E, nesse caso, as raízes se escrevem usando somente raízes quadradas.

Apresentamos também neste trabalho como calcular o grupo de Galois de um polinômio $f(X) \in \mathbb{Q}[X]$ (ou com coeficientes sobre um corpo no qual a fatoração é efetiva), provando, antes de mais nada, que em $\mathbb{Q}[X]$ a fatoração é efetiva. As referências para esta parte são ([4]) e ([9]).

No capítulo 1, introduziremos os pré-requisitos necessários para o presente trabalho.

No capítulo 2, será mostrado o teorema de solubilidade por radicais reais que dá condições necessárias e suficientes para que um polinômio $f(X) \in \mathbb{Q}[X]$ irredutível que tem todas as suas raízes reais seja solúvel por radicais reais. Além disso, apresentaremos alguns corolários e aplicações desse teorema. É importante mencionar que os conteúdos presentes nas seções 1.1 e 1.2 são utilizados na seção 2.1. Já a seção 1.3 e os apêndices A e B servem de base para as aplicações deste teorema (seção 2.2).

O resultado principal do capítulo 3 pode ser encontrado em ([4]):

Teorema 3.2.13 *Seja K um corpo e seja $f(X) \in K[X]$ um polinômio separável sobre K. Seja S_n o grupo das permutações do conjunto das raízes $\{x_1, \ldots, x_n\}$ de $f(X)$ (raízes que não são conhecidas em geral e que podem ter multiplicidade maior do que um, em geral). Sejam $T_1, \ldots, T_n$ indeterminadas sobre K e seja*

$$t = T_1x_1 + \ldots + T_nx_n$$

Então

(i) $Gal(\Sigma_f(K) : K) = \{\sigma \in S_n; T_1\sigma(x_1) + \ldots + T_n\sigma(x_n)$ é um conjugado de t sobre $K(T_1, \ldots, T_n)\}$;

(ii) Se a fatoração em $K[X]$ é efetiva então para todo $\sigma \in S_n$ é possível reconhecer se $T_1\sigma(x_1) + \ldots + T_n\sigma(x_n)$ é um conjugado de t sobre $K(T_1, \ldots, T_n)$, ou não (isto

é, é possível reconhecer se $\sigma \in Gal(\Sigma_f(K) : K)$ *ou não).*

Como em $\mathbb{Q}[X]$ a fatoração é efetiva, temos como consequência deste teorema que, para todo polinômio $f(X) \in \mathbb{Q}[X]$, é sempre possível encontrar o grupo de Galois desse polinômio.

Finalmente, salientamos que, neste trabalho, foram incluídos alguns exemplos não mencionados em nenhuma dessas referências. Mesmo que simples, buscamos com eles ilustrar e discutir os algoritmos de fatoração efetiva e de cálculo do grupo de Galois.

Capítulo 1

Pré-requisitos

1.1 Um Pouco Sobre Teoria de Grupos

Nessa seção iremos relembrar algumas definições e resultados da Teoria de Grupos. Aproveitamos também para fixar algumas notações, uma vez que elas serão úteis para provarmos o resultado principal do presente trabalho. Maiores detalhes podem ser encontrados em [3].

Definição 1.1.1. *Dado G um grupo, dizemos que G é um grupo cíclico se G pode ser gerado por um único elemento.*

Definição 1.1.2. *Seja p um primo. Um grupo G (não necessariamente finito) no qual todo elemento tem sua ordem igual a uma potência de p é chamado um p-grupo.*

Lema 1.1.3. *Seja $G \neq \{e\}$ um p-grupo finito. Então p divide a ordem do centro de G. (que aqui será denotado por $Z(G)$).*

Definição 1.1.4. *Dizemos que um grupo G é solúvel se existir uma cadeia de subgrupos*

$$H = \{e\} \subseteq H_1 \subseteq \ldots \subseteq H_{n-1} \subseteq G$$

tal que

(i) $H_i \lhd H_{i+1}$;

(ii) $\frac{H_{i+1}}{H_i}$ *é abeliano.*

Mostraremos alguns resultados que vão nos permitir garantir que todo p-grupo finito é solúvel.

Proposição 1.1.5. *Seja G um grupo finito e p um primo. A ordem de G é potência de p se, e somente se, todo elemento de G tem ordem potência de p.*

Demonstração: Seja G um grupo tal que $|G| = p^n$ e consideremos α um elemento de G. Pelo Teorema de Lagrange, temos que $o(\alpha)$ divide $|G| = p^n$, onde $o(\alpha)$ denota a ordem do elemento α. Logo,

$$o(\alpha) = p^r, \text{ com } r \leq n$$

Portanto, todo elemento de G tem ordem potência de p.

Suponhamos, agora, que todo elemento de G tem ordem potência de p e que a ordem de G não seja uma potência de p. Logo, existe um primo q, $q \neq p$ tal que $|G| = qm$ para algum $m \in \mathbb{N}$. Então, pelo 1º teorema de Sylov, existe um subgrupo H de G tal que $|H| = q$. Como q é primo, H é cíclico, isto é, existe $x \in H$ tal que $\langle x \rangle = H$. Assim, $|\langle x \rangle| = q$, o que contraria nossa hipótese. Portanto, a ordem de G é potência de p. ■

Proposição 1.1.6. *Seja G um grupo de ordem p^m onde p é um número primo e $m \in \mathbb{N}^*$. Seja H um subgrupo de G de ordem p^r, com $r < m$. Então:*

(i) existe um subgrupo K de G de ordem p^{r+1} contendo H;

(ii) todo subgrupo L de G de ordem p^{r+1} contendo H é tal que $H \lhd L$.

Demonstração: Mostraremos por indução sobre $|G|$, a seguinte afirmação: existe um subgrupo K de G tal que $H \lhd K$ e $|K| = p^{r+1}$.

Se $|G| = p$ então $H = \{e\}$ e, trivialmente, existe um subgrupo K de G, $K = G$, tal que $\{e\} \lhd G$ e $|K| = p = p^{0+1}$.

Se $|G| = p^m$ com $m > 1$, supomos, como hipótese de indução, que a afirmação vale para todos os p-grupos de ordem menor que $|G|$; queremos mostrar que a afirmação vale também para G.

Pelo lema (1.1.3), $Z(G) \neq \{e\}$. Seja $x \in Z(G)$, $x \neq e$ tal que $|\langle x\rangle| = p$, que existe devido ao teorema de Cauchy.

Como $x \in Z(G)$, $\langle x\rangle \lhd G$. Então $\frac{G}{\langle x\rangle}$ é um grupo tal que

$$\left|\frac{G}{\langle x\rangle}\right| = \frac{|G|}{|\langle x\rangle|} = \frac{p^m}{p} = p^{m-1} < |G|$$

1º caso) $x \in H$

Como $x \in H$ temos que $\langle x\rangle \subseteq H$ e como $\langle x\rangle \lhd G$ temos que $\langle x\rangle \lhd H$. Já que $|\langle x\rangle| = p$, $\frac{H}{\langle x\rangle}$ é um subgrupo de ordem p^{r-1} do grupo $\frac{G}{\langle x\rangle}$. Então, como $\left|\frac{G}{\langle x\rangle}\right| < |G|$, pela hipótese de indução, existe um subgrupo K' de $\frac{G}{\langle x\rangle}$ tal que $|K'| = p^r$ e, ainda, $\frac{H}{\langle x\rangle} \lhd K'$.

Considere o homomorfismo canônico sobrejetor

$$\varphi : G \to \frac{G}{\langle x\rangle}$$

$$g \longmapsto g\langle x\rangle$$

e tome $K = \varphi^{-1}(K')$. Como φ é sobrejetora, temos que

$$\frac{K}{\langle x\rangle} = \varphi(K) = \varphi\varphi^{-1}(K') = K'$$

Portanto,

$$|K| = |K'||\langle x\rangle| = p^r p = p^{r+1}$$

Além disso, como $\frac{H}{\langle x\rangle} \lhd K'$ e $K' = \frac{K}{\langle x\rangle}$ temos que $H \lhd K$.

2º caso) $x \notin H$

Como $\langle x\rangle \lhd G$ temos que $H\langle x\rangle$ é um subgrupo de G. Além do mais, $H \cap \langle x\rangle = \{e\}$. De fato, temos

$$|H \cap \langle x\rangle|\big||\langle x\rangle| = p$$

Logo, $|H \cap \langle x\rangle|$ é igual a 1 ou p. Se $|H \cap \langle x\rangle| = p$, como $H \cap \langle x\rangle \subseteq \langle x\rangle$ e ambos tem ordem p, então $H \cap \langle x\rangle = \langle x\rangle$, mas isso contraria o fato de $x \notin H$. Assim, $H \cap \langle x\rangle = \{e\}$.

Portanto, $|H\langle x\rangle| = p^{r+1}$. Basta-nos agora mostrar que $H \lhd H\langle x\rangle$. Para isso, basta notar que $gHg^{-1} \subseteq H$, para todo $g \in H\langle x\rangle$ o que de fato ocorre, pois $x \in Z(G)$.

Provada a afirmação, o item (i) é satisfeito, trivialmente. Além disso, dado um subgrupo L de G de ordem p^{r+1} contendo H, pela afirmação acima, existe um subgrupo N de L tal que $H \lhd N$ e $|N| = p^{r+1}$. Mas como N é um subgrupo de L e possuem o mesmo número de elementos temos que $N = L$. Portanto, $H \lhd L$. ■

Corolário 1.1.7. *Todo p-grupo é solúvel. Mais precisamente: se G é um grupo de ordem p^m, então existem subgrupos $H_0 = \{e\}$, H_1,..., $H_m = G$ tais que $H_i \lhd H_{i+1}$ e $\frac{H_{i+1}}{H_i}$ é um grupo cíclico de ordem p, $\forall i \in \{0, 1, \ldots, m-1\}$.*

Demonstração: Basta aplicar sucessivamente a proposição anterior começando com $H_0 = \{e\}$, já que todo grupo de ordem p é cíclico e, portanto, abeliano. ■

Na seção 3, trabalharemos com o grupo multiplicativo $K^* = K\backslash\{0\}$ de um corpo K. Para isso, utilizaremos, frequentemente, mais algumas noções sobre grupos, as quais convém relembrar.

Lema 1.1.8. *Seja G um grupo e $z \in G$ tal que $o(z) = n < \infty$. Então, para todo*

$k \in \mathbb{Z}$, $z^k = 1$ se, e somente se, n divide k. E para qualquer divisor d de n temos que $o(z^d) = \frac{n}{d}$.

Lema 1.1.9. *Seja G um grupo abeliano e $z_1, \ldots, z_r \in G$ tais que $o(z_i) < \infty$, $\forall i = \{1, \ldots, r\}$. Então:*
(i) $o(z_1 \ldots z_r)$ divide $mmc\{o(z_1), \ldots, o(z_r)\}$;
(ii) Se $o(z_1), \ldots, o(z_r)$ forem primos entre si, então $o(z_1 \ldots z_r) = o(z_1) \ldots o(z_r)$.

Definimos o expoente $exp(G)$ do grupo G como sendo o $mmc\{o(z); z \in G\}$ caso este exista e $exp(G) = \infty$, caso contrário. Com isso, temos o seguinte lema:

Lema 1.1.10. *Seja G um grupo abeliano e suponhamos que $exp(G) < \infty$. Então,*
(i) existe um $y \in G$ tal que $exp(G) = o(y)$;
(ii) $exp(G) = |G|$ se, e somente se, G for um grupo cíclico.

Demonstração: (i) Suponhamos $exp(G) = {p_1}^{k_1} \ldots {p_r}^{k_r}$, sendo $p_1, \ldots, p_r$ primos distintos dois a dois.

Pela definição de $exp(G)$, para todo $i \in \{1, \ldots, r\}$, existe um $z_i \in G$ tal que $o(z_i) = {p_i}^{k_i} q_i$ para algum $q_i \in \mathbb{N}$ não divisível por p_i.

Portanto, pelo lema (1.1.8), tomando $y_i = {z_i}^{q_i}$ temos $o(y_i) = {p_i}^{k_i}$.

Do lema (1.1.9) item (ii), resulta que

$$o(y_1 \ldots y_r) = o(y_1) \ldots o(y_r) = exp(G)$$

(ii) Seja $y \in G$ tal que $exp(G) = o(y)$. Se $exp(G) = |G|$ então $|G| = o(y)$, logo $G = \langle y \rangle$. Por outro lado, se G é cíclico, então existe $z \in G$ tal que $G = \langle z \rangle$. Por definição, $exp(G) = mmc\{o(z^n); n \in \mathbb{N}\}$ e como $o(z^i)$ divide $|G| = o(z)$, temos que $exp(G) = o(z) = |G|$. ■

1.2 Extensões de Corpos

A abordagem contemporânea da Teoria de Galois não estuda apenas um polinômio dado, mas sim uma certa "extensão de corpos" relacionada a esse polinômio. Portanto, nessa seção, serão mencionados alguns aspectos sobre extensões de corpos que serão úteis neste trabalho. Maiores detalhes podem ser encontrados em [8].

Definição 1.2.1. *Dado K um corpo, dizemos que L é uma extensão de K se K é um subcorpo de L.*
Notação: $L : K$

Definição 1.2.2. *Seja $L : K$ uma extensão de corpos. Então,*
(i) $L : K$ é dita uma extensão simples se $L = K(\alpha)$ para algum $\alpha \in L$;
(ii) O grau da extensão $L : K$ é a dimensão de L como K-espaço vetorial e é denotada por $[L : K]$;
(iii) $L : K$ é dita finita quando o grau da extensão é finito.

Notação 1.2.3. *Em todo este texto, $P_{\alpha|K}(X)$ denotará o polinômio minimal do elemento algébrico α sobre um corpo K.*

Lema 1.2.4. *Uma extensão $L : K$ é finita se, e somente se, $L : K$ é uma extensão algébrica e existe um número finito de elementos $\alpha_1, \ldots, \alpha_s \in L$ tais que $L = K(\alpha_1, \ldots, \alpha_s)$*

Lema 1.2.5. *Se $[L : K] = p$ com p primo então $L : K$ é uma extensão simples. E, além disso, se $car(K) \neq 2$ e $[L : K] = 2$, então existe $\beta \in L$ tal que $L = K(\beta)$, com $\beta^2 \in K$.*

Demonstração: Se $[L : K] = p$ com p primo então existe $\alpha \in L \setminus K$. Assim, $[K(\alpha) : K] > 1$. Como $[K(\alpha) : K] | [L : K] = p$, temos $[K(\alpha) : K] = p = [L : K]$. E já que $K(\alpha) \subseteq L$, $K(\alpha) = L$.

Falta mostrarmos que se $car(K) \neq 2$ e $[L : K] = 2$, existe $\beta \in L$ tal que $L = K(\beta)$, com $\beta^2 \in K$. Pelo que mostramos até o momento, temos que existe $\alpha \in L$ tal que $L = K(\alpha)$. Como $[K(\alpha) : K] = [L : K] = 2$, temos que $P_{\alpha|K}(X)$ tem grau 2, digamos $P_{\alpha|K}(X) = X^2 + bX + c$.

Então, como $car(K) \neq 2$, por completamento de quadrados, podemos escrever

$$0 = \alpha^2 + b\alpha + c = \left(\alpha + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c$$

Definindo $\beta = \alpha + \frac{b}{2}$ temos $\beta \in K(\alpha)$, pois $\frac{b}{2} \in K$ e

$$L = K(\alpha) = K(\beta)$$

Além disso, $\beta^2 = \frac{b^2}{4} - c \in K$. ■

Definição 1.2.6. *Dada uma extensão de corpos $L : K$, denominamos Grupo de Galois da extensão o grupo de todos os K-automorfismos de L com a operação de composição, e o denotamos neste texto por $Gal(L : K)$ ou $Aut(L : K)$.*

Definição 1.2.7. *Uma extensão $L : K$ é dita normal se todo polinômio f irredutível sobre K que tem pelo menos uma raiz em L se fatora completamente em $L[X]$, ou equivalentemente, se para todo $\alpha \in L$ algébrico sobre K, $P_{\alpha|K}(X)$ se fatorar em polinômios lineares em $L[X]$.*

Definição 1.2.8. *Dado $f(X) \in K[X]$, um corpo $\Sigma_f(K)$ é dito corpo de raízes do polinômio f sobre o corpo K se $K \subseteq \Sigma_f(K)$ e*
(i) f se fatora completamente em $\Sigma_f(K)$;
(ii) Se $K \subseteq \Sigma' \subseteq \Sigma_f(K)$ e f se fatora completamente em Σ', então $\Sigma' = \Sigma_f(K)$.

Em outras palavras, se $x_1, \ldots, x_n$ são todas as raízes de f então $\Sigma_f(K) = K(x_1, \ldots, x_n)$.

Definição 1.2.9. *Seja $f(X) \in K[X]$. Dizemos que $Gal(\Sigma_f(K) : K)$ é o grupo de Galois de f sobre K.*

Teorema 1.2.10. *Uma extensão $L : K$ é normal e finita se, e somente se, L é corpo de raízes de algum polinômio de $K[X]$.*

Definição 1.2.11. *Dado um corpo K, dizemos que:*
(i) Um polinômio $f(X) \in K[X]$ irredutível sobre um corpo K é separável sobre K se ele não tem raízes múltiplas no seu corpo de raízes;
(ii) Um polinômio irredutível em $K[X]$ é inseparável sobre K se ele não é separável sobre K;
(iii) Um polinômio arbitrário de $K[X]$ é separável sobre K se todos os seus fatores irredutíveis em $K[X]$ são separáveis sobre K.

Lema 1.2.12. *Um polinômio não nulo $f(X) \in K[X]$ tem raízes múltiplas no seu corpo de raízes se, e somente se, f e sua derivada formal têm em $K[X]$ um fator comum de grau maior ou igual a 1.*

Proposição 1.2.13. *(i) Se K é um corpo de característica zero então todo polinômio em $K[X]$ irredutível é separável sobre K;*
(ii) Se K tem característica $p > 0$ então um polinômio $f(X) \in K[X]$ irredutível é inseparável se, e somente se, $f(X) = k_0 + k_1X^p + \ldots + k_rX^{rp}$, onde $k_0, \ldots, k_r \in K$.

Definição 1.2.14. *(i) Seja $L : K$ uma extensão de corpos. Um elemento $\alpha \in L$ é dito separável sobre K se ele for raiz de algum polinômio separável $f(X) \in K[X] \setminus \{0\}$. Equivalentemente, um elemento $\alpha \in L$ é dito separável sobre K, se α é algébrico sobre K e $P_{\alpha|K}(X)$ é separável sobre K;*
(ii) Uma extensão algébrica $L : K$ é dita separável se todo $\alpha \in L$ é separável sobre K.

Proposição 1.2.15. *Seja $L : K$ uma extensão algébrica e M um corpo intermediário, isto é, $K \subseteq M \subseteq L$. A extensão $L : K$ é separável se, e somente se, $M : K$ e $L : M$ são separáveis.*
Além disso, se $L : K$ é normal então $L : M$ também é normal.

Embora seja fácil provar que o conjunto de todos os K-automorfismos de um corpo L é um grupo com a composição, esse fato por si só não avança significativamente no estudo sobre extensões de corpos. O esperado é que o grupo de Galois reflita aspectos da estrutura de $L : K$. De grande avanço foi a descoberta de que, sob certas hipóteses adicionais, existe uma correspondência biunívoca entre
(1) Subgrupos de $Gal(L : K)$;
(2) Subcorpos M de L tais que $K \subseteq M$.

Também é verdade que esta correspondência inverte as relações de inclusão.

Notação 1.2.16. *Para cada corpo intermediário M associaremos o grupo*

$$M^* = Gal(L : M)$$

e para cada subgrupo H de $Gal(L : K)$ associaremos o conjunto $Fix(H)$ definido por

$$Fix(H) = \{x \in L; \alpha(x) = x, \forall \alpha \in H\}$$

Claramente, se $M \subseteq N$ então $M^* \supseteq N^*$, uma vez que toda aplicação que fixa elementos de N certamente fixa os elementos de M. Em particular, note que $M^* \subseteq Gal(L : K)$.

É fácil mostrar também que $K \subseteq Fix(H) \subseteq L$ e que se $H \subseteq N \subseteq G = Gal(L : K)$ então $Fix(H) \supseteq Fix(N)$.

Assim, definindo

$$\mathcal{F} = \{M \text{ corpo } ; K \subseteq M \subseteq L\}$$
$$\mathcal{G} = \{H \text{ grupo } ; H \text{ subgrupo de } G\}$$

baseado no que foi argumentado acima temos as seguintes aplicações:

$$^* : \mathcal{F} \longrightarrow \mathcal{G}$$

$$M \longmapsto M^*$$

$$Fix : \mathcal{G} \longrightarrow \mathcal{F}$$

$$H \longmapsto Fix(H)$$

Nosso objetivo a seguir é apresentar condições extras que garantam que a correspondência acima é biunívoca.

Teorema 1.2.17. *Seja $L : K$ uma extensão finita, normal e separável com grupo de Galois G. Então K é o corpo fixo de G.*

Teorema 1.2.18. (Teorema Fundamental da Teoria de Galois) *Se $L : K$ é uma extensão finita normal e separável (digamos de grau n) com grupo de Galois G e se $\mathcal{F}, \mathcal{G}, ^*, Fix$ são definidas como na notação (1.2.16), então*

(i) O grupo de Galois tem ordem n;

(ii) As aplicações * e Fix são inversas uma da outra, isto é, para todo subgrupo H de G e para todo corpo intermediário M da extensão temos $H = (Fix(H))^*$ e $Fix(M^*) = M$;

(iii) Se M é um corpo intermediário da extensão $L : K$ então

$$[L : M] = |M^*| \text{ e } [M : K] = \frac{|G|}{|M^*|}$$

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

(v) Se um corpo intermediário M da extensão $L : K$ é uma extensão normal de K então o grupo de Galois de $M : K$ é isomorfo ao grupo quociente $\frac{G}{M^*}$.

Definição 1.2.19. *Uma extensão $L : K$ é dita Galoisiana se ela satisfaz as condições do Teorema Fundamental da Teoria de Galois.*

Teorema 1.2.20. (Teorema do Elemento Primitivo para Corpos Infinitos) *Seja K um corpo infinito. Então toda extensão de corpos finita e separável de K é simples.*

Demonstração: Seja $L : K$ uma extensão finita e separável. A prova será feita por indução no número de geradores da extensão.

Suponhamos, inicialmente, que $L = K(\alpha, \beta)$. Como $L : K$ é uma extensão separável, temos que $P_{\alpha|K}$ e $P_{\beta|K}$ são separáveis sobre K. Seja M uma extensão finita de L que contém todas as raízes de $P_{\alpha|K}$ e $P_{\beta|K}$, digamos

$$P_{\alpha|K}(X) = (X - \alpha)(X - \alpha_1) \dots (X - \alpha_m)$$

$$P_{\beta|K}(X) = (X - \beta)(X - \beta_1) \dots (X - \beta_n)$$

com α_i, $\beta_j \in M$, para todo $i \in \{1, \dots, m\}$ e $j \in \{1, \dots, n\}$.

Dado $c \in K$, definimos $\gamma = \alpha + c\beta$ e consideramos o corpo $F = K[\gamma] \subseteq K[\alpha, \beta] = L$. O polinômio

$$h(X) := P_{\alpha|K}(\gamma - cX) \in L[X]$$

satisfaz $h(\beta) = P_{\alpha|K}(\gamma - c\beta) = P_{\alpha|K}(\alpha) = 0$ e, portanto, $(X - \beta)$ divide $h(X)$ em $L[X]$.

Afirmação: $mdc(h(X), P_{\beta|K}(X)) = X - \beta$ para uma conveniente escolha de c.

Já vimos que $X - \beta$ divide esses dois polinômios, temos apenas mostrar que ele é o máximo divisor comum deles. Para isso, primeiro observe que o *mdc* entre dois polinõmios de $L[X]$ pode ser calculado pelo método das divisões sucessivas, assim temos que o *mdc* em $L[X]$ ou em $M[X]$ ($L \subseteq M$) será o mesmo, pois as divisões sucessivas sempre resultarão dentro de $L[X]$. Em particular, $mdc(h(X), P_{\beta|K}(X)) \in L[X]$ (mesmo que estejamos pensando nos polinômios como elementos de $M[X]$).

Pela definição de *mdc*, temos que $X - \beta$ divide $mdc(h(X), P_{\beta|K}(X))$. Então, temos os seguintes casos:

1º Caso: a multiplicidade de β como raiz de $h(X)$ e de $P_{\beta|K}(X)$ em $L[X]$ é maior do que um.

Note que esse caso não ocorre, uma vez que a extensão $L : K$ é, por hipótese, separável.

2º Caso: $h(X)$ e $P_{\beta|K}(X)$ possuem outra raiz em comum além de β no corpo de raízes de $h(X)$ e de $P_{\beta|K}(X)$.

Como as outras raízes de $P_{\beta|K}(X)$ além de β são β_j com $j \in \{1, \ldots, n\}$, temos que a única possibilidade de $h(X)$ e $P_{\beta|K}(X)$ possuírem outra raiz em comum, além de β, é que β_j para algum j seja raiz de $h(X)$ também.

Observe que β_j com $j \in \{1, \ldots, n\}$ é raiz de $h(X)$ se, e somente se, $h(\beta_j) = P_{\alpha|K}(\gamma - c\beta_j) = 0$. E isso ocorre se, e somente se, $\alpha + c\beta - c\beta_j = \gamma - c\beta_j = \alpha_i$ para algum $i \in \{1, \ldots, m\}$, ou seja,

$$c = \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

Como o conjunto dessas frações com $i \in \{1, \ldots, m\}$ e $j \in \{1, \ldots, n\}$ é finito e K é infinito concluímos que, escolhendo $c \in K$ diferente de todas as frações desse tipo, temos que nenhum β_j é raiz comum de $h(X)$ e $P_{\beta|K}(X)$.

Portanto, neste caso, $mdc(h(X), P_{\beta|K}(X)) = X - \beta$.

Como $P_{\beta|K}(X), h(X)$ pertencem a $F[X] = K[\gamma][X]$ então $mdc(h(X), P_{\beta|K}(X)) \in F[X]$; em particular, $\beta \in F$. E, além disso, como $\gamma \in F$ e $\gamma = \alpha + c\beta$, temos que $\alpha \in F$. Logo, $L = K[\alpha, \beta] \subseteq F = K[\gamma] \subseteq L$, ou seja, $L = K[\gamma]$ é uma extensão simples de K.

Suponhamos, agora, que para $n - 1$ termos adjuntados temos que a extensão é simples.

Vamos mostrar que é válido também para uma extensão $L = K(\alpha_1, \ldots, \alpha_n) : K$. Temos que existem α e β em L tais que

$$L = K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) \overset{\text{H.I.}}{=} K(\beta)(\alpha_n) \overset{\text{B.I.}}{=} K(\alpha)$$

Portanto, $L : K$ é simples. ■

Para o presente trabalho, necessitamos também formalizar a ideia de solubilidade por radicais.

Definição 1.2.21. *Uma extensão $L : K$ é dita radical se $L = K(\alpha_1, \ldots, \alpha_m)$ e, para cada $i = 1, \ldots, m$, existem inteiros $n(i)$ tais que*

$$\alpha_i{}^{n(i)} \in K(\alpha_1, \ldots, \alpha_{i-1})$$

Os elementos α_i são ditos uma sequência radical para a extensão $L : K$. Assim,

$$\begin{array}{c} L = K(\alpha_1, \ldots, \alpha_m) \\ \Big| \\ \alpha_m{}^{n(m)} \in K(\alpha_1, \ldots, \alpha_{m-1}) \\ \Big| \\ \vdots \\ \Big| \\ \alpha_2{}^{n(2)} \in K(\alpha_1) \\ \Big| \\ \alpha_1{}^{n(1)} \in K \end{array}$$

Em particular, toda extensão radical é uma extensão finita.

Definição 1.2.22. *Seja $f(X) \in K[X]$, onde K é um corpo de característica zero, e seja $\Sigma_f(K)$ o corpo de raízes de f sobre K.*
(i) O polinômio f é dito solúvel por radicais, se existir um corpo M contendo $\Sigma_f(K)$ tal que $M : K$ é uma extensão radical;
(ii) Um polinômio f é dito solúvel por radicais reais se existir um corpo M contendo $\Sigma_f(K)$, tal que a extensão $M : K$ seja radical e $M \subseteq \mathbb{R}$.

Assim, dizer que f é solúvel por radicais significa que todas as suas raízes podem ser expressas por radicais, ou seja, através de uma fórmula escrita apenas com operações aritméticas e de radiciação, sendo que a quantidade dessas operações deve ser finita. Ainda, f é solúvel por radicais reais se todas as suas raízes puderem ser expressas por radicais reais, ou seja, além de serem expressas através de uma fórmula escrita apenas com operações aritméticas e de radiciação, a partir dos elementos de K, sendo que a quantidade dessas operações deve ser finita, não pode existir radiciação de ordem par de número negativo.

1.3 O Caso Particular das Extensões Ciclotômicas

Nesta seção, o objetivo principal é estudar extensões do tipo $K(\zeta) : K$, onde $\zeta \in \Omega$ é uma raiz da unidade que não pertence a K e Ω é um corpo algebricamente fechado que contém K.

1.3.1 Sobre as Extensões Ciclotômicas de K

Considere K um corpo e $K^* = K \setminus \{0\}$ o seu grupo multiplicativo. Denote por $\mathcal{R}_n$ o conjunto de todas as raízes do polinômio $X^n - 1$. Para cada $n \geq 1$ denotaremos por

$$W_n(K) = \{a \in K^*; a^n = 1\} = \{a \in K^*; o(a)|n\} \subseteq K^*$$

que será chamado o grupo das raízes n-ésimas da unidade em K. Além disso, o subconjunto de todas as raízes n-ésimas primitivas da unidade pertencentes a K será denotado por $\mathcal{P}_n(K)$. Assim,

$$\mathcal{P}_n(K) = \{ \text{ raízes } n\text{-ésimas primitivas da unidade em } K\} = \{a \in K^*; o(a) = n\}$$

Por fim, denotando por $\mathcal{U}_{\mathbb{Z}_n}$ o grupo multiplicativo que consiste dos elementos invertíveis do anel $\mathbb{Z}_n$, ou seja, das classes $\bar{l} = l + (n)$ tais que $l \in \mathbb{Z}$ e $mdc(l, n) = 1$, temos que, se $z \in \mathcal{P}_n(K)$, então

$$\mathcal{P}_n(K) = \{z^l; 1 \leq l \leq n; mdc(l, n) = 1\}$$

Em particular, a ordem de $\mathcal{P}_n(K)$ é dada por $\varphi(n)$ onde φ é a função de Euler.

Como foi visto na proposição (.1.5), para garantirmos a existência de tais raízes em algum sobrecorpo próprio de K, basta supormos que n não seja divisível pela $car(K)$, pois, então, $\mathcal{P}_n(\Omega) \neq \emptyset$.

De fato, se $car(\Omega) = p$ com p primo dividir n então temos que $n = pq$ com $q < n$. Então $X^n - 1 = X^{pq} - 1$. Como estamos em um corpo de característica p, para todo $a \in \Omega$ temos que $a^p \equiv a \pmod{p}$. Logo,

$$X^n - 1 = X^{pq} - 1 = X^q - 1$$

que tem no máximo q raízes, portanto $|W_n(\Omega)| \leq q < n$. Assim, por (.1.5), teremos que $P_n(\Omega) = \emptyset$.

Definição 1.3.1. *Seja K um corpo e Ω um corpo algebricamente fechado tal que $K \subseteq \Omega$. Para todo $n \geq 1$ que não seja divisível pela $car(\Omega)$, o corpo $K(\mathcal{R}_n)$ será chamado a n-ésima extensão ciclotômica de K.*

No caso em que $K = \mathbb{Q}$ a n-ésima extensão ciclotômica de $\mathbb{Q}$ é dita o n-ésimo corpo ciclotômico. Note que $car(\mathbb{Q})$ não divide n, para todo $n \geq 1$.

Para qualquer subcorpo K de $\mathbb{R}$ temos que $W_n(K) = \{1\}$ se n é ímpar e $W_n(K) = \{1, -1\}$ se n é par. E assim, $\mathcal{P}_n(K) = \emptyset$ para qualquer $n > 2$. O que nos mostra que, nesse caso, a n-ésima extensão ciclotômica de K é não trivial, isto é, é distinta de K.

Teorema 1.3.2. *Seja n um natural não divisível pela $car(K)$. Seja $L = K(\mathcal{R}_n)$ a n-ésima extensão ciclotômica de K. Então:*

(i) $L : K$ é Galoisiana e $L = K(\zeta)$, para todo $\zeta \in \mathcal{P}_n(\Omega)$;

(ii) Por $\sigma \longmapsto \sigma|_{\mathcal{R}_n}$ $(\sigma \in Aut(L : K))$ é definido um homomorfismo injetivo ϕ de $Aut(L : K)$ no grupo $\mathcal{S}_{\mathcal{R}_n}$ de todas as permutações de $\mathcal{R}_n$;

(iii) $Aut(L : K)$ é isomorfo a um subgrupo de $\mathcal{U}_{\mathbb{Z}_n}$, portanto, é comutativo e $[L : K] = |Aut(L : K)|$ é um divisor de $\varphi(n)$;

(iv) $[L : K] = \varphi(n)$ se, e somente se, $Aut(L : K)$ for isomorfo a $\mathcal{U}_{\mathbb{Z}_n}$.

Demonstração: (i) É claro que

$$W_n(L) = \{1, \zeta, \ldots, \zeta^{n-1}\}$$

para $\zeta \in \mathcal{P}_n(\Omega)$. Note que $\mathcal{P}_n(\Omega) \neq \emptyset$, já que n não é divisível pela $car(K)$.

Obviamente, $L = K(\zeta)$ então $L : K$ é normal e finita. Além disso, pela proposição (.1.5), temos que $X^n - 1$ é separável, então, pela definição de elemento separável, temos que ζ é separável. Logo, como $L = K(\zeta)$ e ζ é separável, temos que $L : K$ é separável. Portanto, $L : K$ é Galoisiana.

(ii) Sabemos que para todo $\sigma \in Aut(L : K)$, a restrição $\sigma|_{\mathcal{R}_n}$ é uma permutação de $\mathcal{R}_n$. Consideremos, então,

$$\phi : Aut(L : K) \longrightarrow \mathcal{S}_{\mathcal{R}_n}$$

$$\sigma \longmapsto \sigma|_{\mathcal{R}_n}$$

ϕ é um homomorfismo injetivo, pois se $\sigma|_{\mathcal{R}_n} = id_{\mathcal{R}_n}$ então $\sigma(\alpha) = \alpha$ para todo $\alpha \in \mathcal{R}_n$. E como $\sigma \in Aut(L : K)$, temos que $\sigma \in Aut(L : K(\mathcal{R}_n))$ mas $L = K(\mathcal{R}_n)$, portanto, $\sigma = id_L$

O subgrupo $\{\sigma|_{\mathcal{R}_n}; \sigma \in Aut(L : K)\}$ do grupo $\mathcal{S}_{\mathcal{R}_n}$, ou seja, a imagem deste homomorfismo, será chamado o grupo de $X^n - 1$ sobre K, o qual será denotado por

$G_{X^n-1|K}$.

$$G_{X^n-1|K} = \{\sigma|_{\mathcal{R}_n}; \sigma \in Aut(L:K)\}$$

.

(*iii*) Para cada $\sigma \in Aut(L:K)$, a restrição de σ ao subconjunto $\mathcal{R}_n = W_n(L)$ é um automorfismo do grupo $W_n(L)$, uma vez que a restrição $\sigma|_{\mathcal{R}_n}$ é uma permutação de $\mathcal{R}_n$.

Então, a imagem $G_{X^n-1|K}$ está contida no subgrupo $Aut(W_n(L))$ do grupo $\mathcal{S}_{\mathcal{R}_n}$. Compondo o homomorfismo injetivo ϕ definido acima com o inverso do isomorfismo indicado no corolário (.1.8) temos que $Aut(L:K)$ é isomorfo a um subgrupo V de $\mathcal{U}_{\mathbb{Z}_n}$.

Além disso, $|Aut(L:K)| = [L:K]$ pois $L:K$ é Galoisiana. Resta mostrar que $|Aut(L:K)|$ divide $\varphi(n)$. Devido ao isomorfismo acima encontrado temos que $|Aut(L:K)| = |V|$ e como V é um subgrupo de $\mathcal{U}_{\mathbb{Z}_n}$ temos que $|V|$ divide $|\mathcal{U}_{\mathbb{Z}_n}| = \varphi(n)$ Portanto, $|Aut(L:K)|$ divide $\varphi(n)$.

(*iv*) Esse item decorre do fato que $[L:K] = \varphi(n)$ se, e somente se, $V = \mathcal{U}_{\mathbb{Z}_n}$. ■

Antes de demonstrarmos o resultado principal dessa seção, vamos relembrar um lema muito importante relacionado ao teorema de Gauss:

Lema 1.3.3. *Sejam $F, G \in \mathbb{Q}[X]$ mônicos e tais que $FG \in \mathbb{Z}[X]$. Então, $F, G \in \mathbb{Z}[X]$.*

Teorema 1.3.4. *Seja L o n-ésimo corpo ciclotômico. Então $[L:\mathbb{Q}] = \varphi(n)$ e, portanto, $Aut(L:\mathbb{Q})$ é isomorfo a $\mathcal{U}_{\mathbb{Z}_n}$.*

Demonstração: Seja $\zeta \in \mathcal{P}_n(\mathbb{C})$.

Afirmação: Para todo primo p que não divide n, os polinômios minimais

$$P(X) = P_{\zeta|\mathbb{Q}}(X) \text{ e } P_1(X) = P_{\zeta^p|\mathbb{Q}}(X)$$

de ζ e ζ^p coincidem.

De fato, suponhamos $P(X) \neq P_1(X)$. Como $P(X)$ e $P_1(X)$ são ambos irredutíveis e dividem $X^n - 1$, já que ζ e ζ^p são raízes desse polinômio, temos que

$$P(X)P_1(X)J(X) = X^n - 1 \tag{1.1}$$

para algum $J(X) \in \mathbb{Q}[X]$. Mas como ζ é raiz de $P_1(X^p)$ temos que

$$P(X)H(X) = P_1(X^p)$$

para algum $H(X) \in \mathbb{Q}[X]$.

Do Lema (1.3.3), resulta que $P(X), P_1(X), J(X), H(X) \in \mathbb{Z}[X]$. Consideremos $\pi : \mathbb{Z} \longmapsto \mathbb{Z}_p$ o homomorfismo canônico.

Como para todo $a \in \mathbb{Z}$, temos $a^p \equiv a \pmod{p}$, ou equivalentemente, $\overline{a}^p = \overline{a}$, temos $\pi(a)^p = \pi(a), \forall a \in \mathbb{Z}$.

Denotando por $P^\pi(X)$ o polinômio obtido pela aplicação de π nos coeficientes de um polinômio $P(X) \in \mathbb{Z}[X]$, temos que

$$P(X)H(X) = P_1(X^p) \Longrightarrow P^\pi(X)H^\pi(X) = ({P_1}^\pi(X^p)) = ({P_1}^\pi(X))^p \tag{1.2}$$

onde a última igualdade decorre da afirmação e do fato que os termos intemediários do Binômio de Newton se anulam.

Logo, $P^\pi(X)$ e ${P_1}^\pi(X)$ possuem um divisor comum $D(X) \in \mathbb{Z}_p[X]\backslash\mathbb{Z}_p$. Logo, $D(X)^2$ divide $P^\pi(X){P_1}^\pi(X)$ e, portanto, por (1.1) também $X^n - \pi(1)$. Mas isso é impossível, pois $X^n - \pi(1)$ é separável, já que p não divide n. Então, $P(X) = P_1$, ou seja, ζ e ζ^p têm o mesmo polinômio minimal.

Como todo $\eta \in \mathcal{P}_n(\mathbb{C})$ é da forma $\zeta^{p_1 \cdots p_r}$, onde $p_1, \ldots, p_r$ são primos (não necessariamente distintos) que não dividem n, pois $\mathcal{P}_n(\mathbb{C}) = \{\zeta^l; 1 \leq l \leq n; mdc(l, n) = 1\}$, basta aplicar a afirmação, provada acima, aos elementos $\zeta, \zeta^{p_1}, \ldots, \zeta^{p_1 \cdots p_r}$ sucessi-

vamente. Obtemos assim que

$$P_{\eta|\mathbb{Q}}(X) = P(X)$$

para todo $\eta \in \mathcal{P}_n(\mathbb{C})$. Logo, $P(X)$ tem pelo menos $\#\mathcal{P}_n(\mathbb{C}) = |\mathcal{U}_{\mathbb{Z}_n}| = \varphi(n)$ raízes distintas, pois todo elemento de $\mathcal{P}_n(\mathbb{C})$ é raiz de $P(X)$.

Concluimos que $\varphi(n) \leq \partial P(X) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [L : Q] = \#Aut(L : \mathbb{Q})$. Mas pelo teorema (1.3.2)(ii) temos que $\varphi(n)$ é um múltiplo de $\#Aut(L : \mathbb{Q})$. Portanto, $[L : \mathbb{Q}] = \varphi(n)$. ■

A partir da demonstração desse teorema, vemos que todos os elementos de $\mathcal{P}_n(\mathbb{C})$ têm o mesmo polinômio minimal, ou seja, usando as mesmas notações da demonstração temos que se $\eta \in \mathcal{P}_n(\mathbb{C})$ então $P_{\eta|\mathbb{Q}}(X) = P(X)$ sendo que $\partial P(X) = \varphi(n)$. Assim,

$$P(X) = \prod_{\eta \in \mathcal{P}_n(\mathbb{C})} (X - \eta)$$

Notação 1.3.5. *Chamaremos este polinômio de o n-ésimo polinômio ciclotômico, o qual será denotado por* Φ_n.

Exemplo 1.3.6. *É possível escrever* $X^4 - 1 = \Phi_1(X)\Phi_2(X)\Phi_4(X)$.

De fato, considerando $n = 2$, temos que -1 é a única raiz quadrada primitiva da unidade, então

$$\Phi_2(X) = X + 1$$

Da mesma forma, quando $n = 4$ temos que as raízes do polinômio $X^4 - 1$ são $1, -1, i$ e $-i$, sendo que i e $-i$ são as raízes primitivas da unidade, então

$$\Phi_4(X) = (X - i)(X + i) = X^2 + 1$$

Como $\Phi_1(X) = X - 1$, nós podemos escrever

$$X^4 - 1 = (X - 1)(X + 1)(X^2 + 1) = \Phi_1(X)\Phi_2(X)\Phi_4(X)$$

Esse exemplo nos leva à seguinte proposição:

Proposição 1.3.7. *Para todo $n \geq 1$, $\Phi_n(X)$ é um polinômio mônico e irredutível em $\mathbb{Z}[X]$. Além do mais,*

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Demonstração: $\Phi_n(X)$ é mônico, por definição. E ele tem grau $\varphi(n)$, como já foi mostrado anteriormente. Vamos mostrar, agora, que a igualdade enunciada acima é válida.

A ideia principal desta demonstração é o fato de que todo número $0 \leq i < n$ fornece um divisor d de n, sendo $d = mdc(i, n)$. Considerando $\zeta_n = e^{\frac{2\pi i}{n}}$, temos que

$$X^n - 1 = \prod_{0 \leq i < n} (X - {\zeta_n}^i)$$

Já mostramos que $\mathcal{W}_n(\mathbb{C}) = \cup_{d|n} \mathcal{P}_d(\mathcal{C})$, sendo que essa união é disjunta. Então,

$$X^n - 1 = \prod_{d|n} \left(\prod_{\eta \in \mathcal{P}_d(\mathbb{C})} (X - \eta) \right) = \prod_{d|n} \Phi_d(X)$$

Como $\Phi_n(X)$ é mônico, temos que $\Phi_n(X) \in \mathbb{Z}[X]$, pelo lema (1.3.3). E sendo irredutível em $\mathbb{Q}[X]$ (pois $\Phi_n(X) = \mathcal{P}_{\eta|\mathbb{Q}}(X)$) é também irredutível em $\mathbb{Z}[X]$. ■

Capítulo 2

Solubilidade de Equações Polinomiais por Radicais Reais

O objetivo deste capítulo é responder a seguinte questão:

Dado um polinômio $f(X) \in \mathbb{Q}[X]$ irredutível que é solúvel por radicais, podemos garantir que o mesmo seja solúvel por radicais reais?

Provamos neste capítulo que a resposta a esta questão é negativa e passamos então a procurar condições para garantir isso, tomando como referência ([6]). Lembre que, ao dizermos que o polinômio $f(X)$ é solúvel por radicais reais, estamos falando no sentido de que, além de ser solúvel por radicais, existe uma extensão radical K de $\mathbb{Q}$, totalmente contida em $\mathbb{R}$ tal que o corpo de raízes do polinômio $f(X)$ sobre $\mathbb{Q}$ esteja contido em K, isto é, $\Sigma_f(\mathbb{Q}) \subseteq K \subseteq \mathbb{R}$ (veja definição (1.2.8)). Adiante daremos um exemplo em que isto não acontece. Em particular, todas as raízes de f devem ser reais para que f possa ter chances de ser solúvel por radicais reais.

Equivalentemente, $f(X) \in \mathbb{Q}[X]$ é solúvel por radicais reais se todas as suas

raízes puderem ser expressas por radicais reais, ou seja, através de uma fórmula escrita apenas com operações aritméticas e de radiciação com números inteiros com uma quatidade finita dessas operações e que não haja radiciação de ordem par de número negativo.

2.1 Teorema de Solubilidade por Radicais Reais

Começamos por garantir que os expoentes $n(i)$ na definição (1.2.21) de extensão radical podem ser tomados primos.

Lema 2.1.1. *Se $L : K$ é uma extensão radical, então existem corpos*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{n-1} \subseteq K_n = L$$

onde para $i = 1, \ldots, n$, existe $\gamma_i \in K_i$ tal que $K_i = K_{i-1}(\gamma_i)$ e ${\gamma_i}^{m_i} \in K_{i-1}$ para algum primo m_i.

Demonstração: Primeiro, vamos mostrar que o lema é válido para uma extensão $K \subseteq K(\gamma)$ com $\gamma^m \in K$ para algum $m > 1$.

Se m é primo então nada há a mostrar. Se m não é primo, então seja p um primo que divide m e seja $\delta = \gamma^p$. Isso nos dá as seguintes extensões:

$$K \subseteq K(\delta) \subseteq K(\delta)(\gamma) = K(\gamma)$$

Assim, temos $\gamma^p = \delta \in K(\delta)$ e $\delta^{\frac{m}{p}} = (\gamma^p)^{\frac{m}{p}} = \gamma^m \in K$. Se $\frac{m}{p}$ é primo então acabamos de encontrar a cadeia procurada para essa extensão. Se $\frac{m}{p}$ não é primo então escolha um primo que divida $\frac{m}{p}$ e faça o mesmo processo como acima. Note que esse processo é finito, pois qualquer fatoração de m é finita.

Como toda extensão radical é uma sequência de extensões do tipo $K(\gamma) : K$ com $\gamma^m \in K$, o lema é válido para qualquer extensão radical. ■

Lema 2.1.2. *Sejam p um primo e K um corpo. Então $f(X) = X^p - a \in K[X]$ é irredutível sobre K se, e somente se, f não tem raízes em K.*

Demonstração: É claro que qualquer polinômio irredutível de $K[X]$ não tem raízes em K.

Mostraremos que se f é redutível sobre K então f tem alguma raiz em K.

Primeiramente, nós estudaremos as raízes de f em $\Sigma_f(K)$.

Suponhamos então que, em $\Sigma_f(K)[X]$,

$$X^p - a = (X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_p); \alpha_1, \dots, \alpha_p \in \Sigma_f(K)$$

Se $\alpha_1 = 0$ então f tem uma raiz em K e nada há a provar. Assim, nós suporemos que $\alpha_1 \neq 0$. Se nós definirmos

$$\xi_i = \frac{\alpha_i}{\alpha_1}$$

para $1 \leq i \leq p$ então

$$\xi_i{}^p = \frac{\alpha_i{}^p}{\alpha_1{}^p} = \frac{a}{a} = 1$$

isso implica que $\alpha_i = \xi_i\alpha_1$ onde ξ_i é uma raiz p-ésima da unidade em $\Sigma_f(K)$. Portanto, f pode ser escrito como:

$$f(X) = (X - \xi_1\alpha_1)(X - \xi_2\alpha_1)\dots(X - \xi_p\alpha_1) \tag{2.1}$$

Agora, suponha que $f(X) = g(X)h(X)$ onde $g(X), h(X) \in K[X]$ têm grau $r, s < p$, respectivamente. Nós podemos supor que $g(X)$ e $h(X)$ são mônicos, multiplicando-os por constantes adequadas, se necessário.

Como $f(X) = g(X)h(X)$ e a fatoração é única e g é mônico, g deve ser o produto de r dos fatores de f listados em (2.1). Renomeando, se for preciso, podemos supor que

$$g(X) = (X - \xi_1\alpha_1)(X - \xi_2\alpha_1)\dots(X - \xi_r\alpha_1)$$

Como $g(X) \in K[X]$ tem-se que o termo constante de $g(X)$ está em K, ou seja, $\xi {\alpha_1}^r \in K$, onde $\xi = \xi_1 \xi_2 \dots \xi_r$. Note que ξ é também uma raiz p-ésima da unidade em $\Sigma_f(K)$.

Como $0 < r < p$ e p é primo, temos que $mdc(r, p) = 1$ então existem inteiros m, n tais que $mr + np = 1$. Então,

$$\xi^m \alpha_1 = \xi^m {\alpha_1}^{mr+np} = \underbrace{(\xi {\alpha_1}^r)}_{\in K}{}^m \underbrace{({\alpha_1}^p)}_{=a}{}^n \in K$$

pois $\xi {\alpha_1}^r \in K$ e ${\alpha_1}^p = a \in K$.

Mas, $(\xi^m \alpha_1)^p = (\xi^p)^m {\alpha_1}^p = a$, o que mostra que $\xi^m \alpha_1$ é uma raiz de $f(X) = X^p - a$ que pertence a K. ■

Lema 2.1.3. *Seja E um subcorpo de $\mathbb{R}$ e suponhamos que $\gamma \in \mathbb{R}$ satisfaz $\gamma \notin E$ e $\gamma^p \in E$, onde p é um primo. Então, $g(X) = X^p - \gamma^p$ é irredutível em $E[X]$ e, portanto, $[E(\gamma) : E] = p$.*

Demonstração: Pelo lema (2.1.2), é suficiente mostrar que $g(X)$ não tem raízes em E. Se $\beta \in E$ é uma raiz de $g(X)$ então $\beta^p - \gamma^p = 0$. Logo, $\beta^p = \gamma^p$, ou seja, $\beta = \xi\gamma$ para alguma raiz ξ p-ésima complexa da unidade, pelo mesmo argumento feito na demonstração do lema (2.1.2).

Como β e γ são reais e não-nulos, ξ deve ser real, mas as únicas raízes reais da unidade são ± 1. Disso segue que $\gamma = \pm\beta \in E$, o que é um absurdo pois $\gamma \notin E$. Portanto, g é irredutível sobre E. ■

Exemplo 2.1.4. *O polinômio $X^5 - 2$ é irredutível em $\mathbb{Q}(\sqrt{3})[X]$.*

De fato, considerando $E = \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$ e $\gamma = \sqrt[5]{2} \in \mathbb{R}$, como $\gamma \notin \mathbb{Q}(\sqrt{3})$ e $\gamma^5 \in \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$, pelo lema acima, temos que o polinômio $X^5 - 2$ é irredutível em $\mathbb{Q}(\sqrt{3})[X]$.

Teorema 2.1.5. (Teorema de Solubilidade por Radicais Reais) *Seja $f(X) \in \mathbb{Q}[X]$ irredutível tal que todas as raízes de f são reais (mais precisamente, irracionais). Então f é solúvel por radicais reais se, e somente se, a ordem de $Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})$ é uma potência de 2. E, nesse caso, as raízes se escrevem usando somente raízes quadradas.*

Demonstração: Seja $\Sigma_f(\mathbb{Q}) \subseteq \mathbb{R}$ o corpo de raízes de f sobre $\mathbb{Q}$ e denote $G = Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})$.

($\Longleftarrow$) : Por hipótese, temos que a ordem de G é uma potência de 2, logo G é um 2-grupo. Então, pelo corolário (1.1.7), temos que G é um grupo solúvel. Mais precisamente, existe uma cadeia

$$id_{\mathbb{Q}} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_k = G \tag{2.2}$$

onde $|G_i| = 2^i$ e $(G_{i+1} : G_i) = \frac{|G_{i+1}|}{|G_i|} = 2$. E isso nos dá a seguinte cadeia de subcorpos de $\mathbb{R}$:

$$\begin{array}{c} L_k = \Sigma_f(\mathbb{Q}) \subseteq \mathbb{R} \\ | \\ \vdots \\ | \\ L_1 \\ | \\ L_0 \end{array}$$

onde L_i é a parte fixa do grupo G_{k-i}, isto é, $L_i = \{x \in \Sigma_f(\mathbb{Q}); \sigma(x) = x, \forall \sigma \in G_{k-1}\} = Fix(G_{k-i})$. Assim, $L_k = Fix(G_0) = Fix(id_{\mathbb{Q}}) = \Sigma_f(\mathbb{Q}) \subseteq \mathbb{R}$. E $L_0 =$

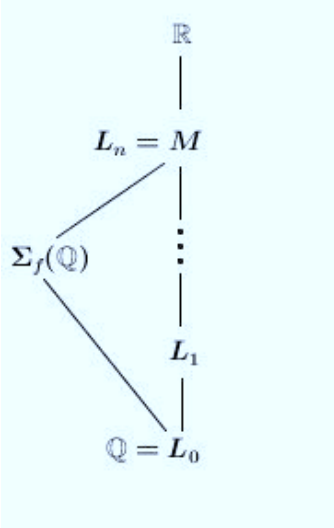
$Fix(G_k) = Fix(G) = \mathbb{Q}$, pelo teorema (1.2.17), já que $L : \mathbb{Q}$ é uma extensão finita, normal e separável.

Como a extensão $\Sigma_f(\mathbb{Q}) : \mathbb{Q}$ é uma extensão finita, normal e separável, podemos aplicar o Teorema Fundamental da Teoria de Galois para essa extensão. Assim, sabemos que existe uma correspondência biunívoca entre os subgrupos do grupo de Galois descritos em (2.2) com os corpos intermediários L_i. Além disso, como $(G_{i+1} : G_i) = 2$ temos que $[L_{i+1} : L_i] = 2$. Pelo lema (1.2.5), temos que existe $\alpha_{i+1} \in L_{i+1}$, $L_{i+1} = L_i(\alpha_{i+1})$ com ${\alpha_{i+1}}^2 \in L_i$.

Denotando $\beta = {\alpha_{i+1}}^2 \in L_i$, nós podemos escrever sem perda de generalidade $\sqrt{\beta} = \alpha_{i+1}$, o que nos mostra que toda extensão de grau 2 de L_i é obtida adjuntando uma raiz quadrada.

Esses resultados implicam que as extensões $L_{i+1} : L_i$ são radicais para todo i. Portanto, a extensão $\Sigma_f(\mathbb{Q}) : \mathbb{Q}$ é radical e como $\Sigma_f(\mathbb{Q}) \subseteq \mathbb{R}$, $L_i \subseteq \mathbb{R}, \forall i$, f é solúvel por radicais reais.

($\Longrightarrow$) : Suponhamos, agora, que f é solúvel por radicais reais. Então, existe um corpo M contendo $\Sigma_f(\mathbb{Q})$, tal que a extensão $M : \mathbb{Q}$ é radical e $M \subseteq \mathbb{R}$. Logo, podemos aplicar o lema (2.1.1) para a extensão $M : \mathbb{Q}$, obtendo a seguinte cadeia de corpos:



que é tal que existem n_i primos e $\alpha_i \in L_i$ tais que $L_i = L_{i-1}(\alpha_i)$ e ${\alpha_i}^{n_i} \in L_{i-1}$. Note que como $\Sigma_f(\mathbb{Q}) : \mathbb{Q}$ é finita, normal e separável, pelo teorema (1.2.18), temos que $|Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})| = [\Sigma_f(\mathbb{Q}) : \mathbb{Q}]$.

Se $|Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})| = 1 = 2^0$ então nada mais há a fazer.

Caso contrário, seja p primo tal que

$$p||Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})| = [\Sigma_f(\mathbb{Q}) : \mathbb{Q}]$$

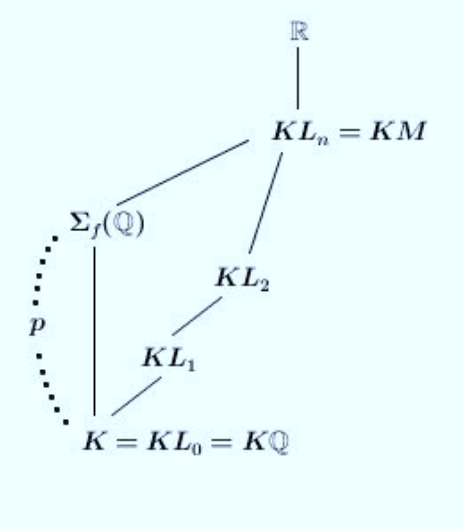
Pelo 1º teorema de Sylov existe subgrupo H de $G = Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})$ com $|H| = p$. Seja K o corpo fixo de H, isto é, $K = Fix(H)$, logo K é um corpo intermediário da extensão $\Sigma_f(\mathbb{Q}) : \mathbb{Q}$.

Como $\Sigma_f(\mathbb{Q}) : \mathbb{Q}$ é finita, normal e separável, pela proposição (1.2.15), temos que $\Sigma_f(\mathbb{Q}) : K$ é finita, normal e separável. Logo, $\Sigma_f(\mathbb{Q}) : K$ é uma extensão de Galois, então pela correspondência de Galois, Teorema (1.2.18), temos

$$[\Sigma_f(\mathbb{Q}) : K] = |Gal(\Sigma_f(\mathbb{Q}) : K)| = |Gal(\Sigma_f(\mathbb{Q}) : Fix(H))| =$$

$$|Fix(H)^*| \overset{(1.2.18)}{=} |H| = p$$

Em particular, $\Sigma_f(\mathbb{Q}) \nsubseteq K$. Consideramos agora as seguintes extensões de corpos:



Temos que $KL_i = KL_{i-1}(\alpha_i)$, onde ${\alpha_i}^{n_i} \in L_{i-1} \subseteq KL_{i-1}$.

Assim, como $\Sigma_f(\mathbb{Q}) \subseteq KL_n$ (pois $\Sigma_f(\mathbb{Q}) \subseteq L_n \subseteq KL_n$), mas $\Sigma_f(\mathbb{Q}) \nsubseteq K = KL_0$, existe $i \in \{1, 2, \ldots, n\}$ tal que $\Sigma_f(\mathbb{Q}) \subseteq KL_i$ e $\Sigma_f(\mathbb{Q}) \nsubseteq KL_{i-1}$ (isto é, i é o menor elemento do conjunto $\{1, 2, \ldots, n\}$ tal que $\Sigma_f(\mathbb{Q}) \subseteq KL_i$).

Seja, agora, β_1 tal que $\Sigma_f(\mathbb{Q}) = K(\beta_1)$, que existe devido ao lema (1.2.5). Como $\Sigma_f(\mathbb{Q}) : K$ é normal, separável e de grau p temos

$$P_{\beta_1|K}(X) = (X - \beta_1)(X - \beta_2)\ldots(X - \beta_p)$$

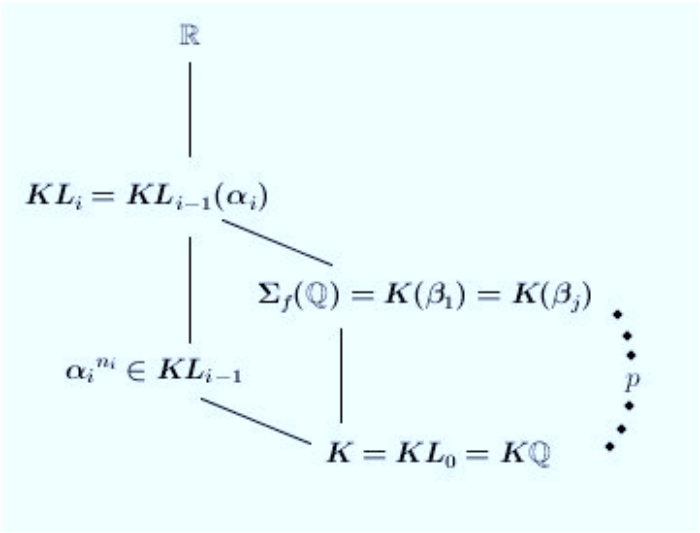
onde $\beta_1, \ldots, \beta_p \in \Sigma_f(\mathbb{Q})$ e $\beta_i \neq \beta_j$ para $i \neq j$.

Afirmação 1: Para todo $j \in \{1, 2, \ldots, p\}$, temos que $\Sigma_f(\mathbb{Q}) = K(\beta_j)$.

De fato, sabemos que $\Sigma_f(\mathbb{Q}) = K(\beta_1)$ e $[\Sigma_f(\mathbb{Q}) : K] = p$. Note que β_j anula $P_{\beta_1|K}(X)$,$\forall j \in \{1, 2, \ldots, p\}$ e esse polinômio é irredutível sobre K. Logo, $P_{\beta_j|K}(X) = P_{\beta_1|K}(X), \forall j \in \{1, 2, \ldots, p\}$.

Assim, $[K(\beta_j) : K] = p = [\Sigma_f(\mathbb{Q}) : K]$. Mas como $K \subseteq \Sigma_f(\mathbb{Q})$ e $\beta_j \in \Sigma_f(\mathbb{Q})$ temos que $K(\beta_j) \subseteq \Sigma_f(\mathbb{Q})$ e, portanto, $K(\beta_j) = \Sigma_f(\mathbb{Q})$.

Resumindo, temos a seguinte situação:



Por outro lado,

$$P_{\alpha_i|KL_{i-1}}(X)|X^{n_i} - {\alpha_i}^{n_i} \text{ em } KL_{i-1}[X]$$

Além disso, temos que $KL_i \nsubseteq KL_{i-1}$, uma vez que $\Sigma_f(\mathbb{Q}) \subseteq KL_i$ e $\Sigma_f(\mathbb{Q}) \nsubseteq KL_{i-1}$. Note que

$$KL_i = KL_{i-1}(\alpha_i) \nsubseteq KL_{i-1} \Longrightarrow \alpha_i \notin KL_{i-1}$$

Assim, temos que $KL_{i-1} \subseteq \mathbb{R}$, $\alpha_i \in \mathbb{R}$, $\alpha_i \notin KL_{i-1}$ e ${\alpha_i}^{n_i} \in KL_{i-1}$, onde n_i é primo. Desse modo, pelo Lema (2.1.3), temos que o polinômio $X^{n_i} - {\alpha_i}^{n_i} \in KL_{i-1}[X]$ é irredutível sobre $KL_{i-1}[X]$.

Então, $X^{n_i} - {\alpha_i}^{n_i} = P_{\alpha_i|KL_{i-1}}(X)$ e

$$[KL_i : KL_{i-1}] = [KL_{i-1}(\alpha_i) : KL_{i-1}] = n_i \tag{2.3}$$

Disso segue que não existe corpo propriamente contido entre KL_{i-1} e KL_i, já que n_i é primo.

Afirmação 1: Para todo $j \in \{1, 2, \ldots, p\}$, temos que $\Sigma_f(\mathbb{Q}) = K(\beta_j)$.

De fato, sabemos que $\Sigma_f(\mathbb{Q}) = K(\beta_1)$ e $[\Sigma_f(\mathbb{Q}) : K] = p$. Note que β_j anula $P_{\beta_1|K}(X)$,$\forall j \in \{1, 2, \ldots, p\}$ e esse polinômio é irredutível sobre K. Logo, $P_{\beta_j|K}(X) = P_{\beta_1|K}(X), \forall j \in \{1, 2, \ldots, p\}$.

Assim, $[K(\beta_j) : K] = p = [\Sigma_f(\mathbb{Q}) : K]$. Mas como $K \subseteq \Sigma_f(\mathbb{Q})$ e $\beta_j \in \Sigma_f(\mathbb{Q})$ temos que $K(\beta_j) \subseteq \Sigma_f(\mathbb{Q})$ e, portanto, $K(\beta_j) = \Sigma_f(\mathbb{Q})$.

Afirmação 2: Para todo $j \in \{1, 2, \ldots, p\}$, temos que $KL_i = KL_{i-1}(\beta_j)$.

De fato, temos que

$$KL_{i-1} \subseteq KL_{i-1}(\beta_j) \overset{\mathrm{KL_{i-1}=L_{i-1}K}}{=} L_{i-1}K(\beta_j) \overset{\Sigma_f(\mathbb{Q})=K(\beta_j)}{=}$$

$$L_{i-1}\Sigma_f(\mathbb{Q}) \overset{\Sigma_f(\mathbb{Q})\subseteq KL_i}{\subseteq} L_{i-1}KL_i \overset{L_{i-1}\subseteq L_i}{=} KL_i$$

Como não existe corpo propriamente contido entre KL_{i-1} e KL_i temos que $KL_{i-1}(\beta_j) = KL_{i-1}$ ou $KL_{i-1}(\beta_j) = KL_i$. Mas como $\beta_j \notin KL_{i-1}$, para todo $p \in \{1, \ldots, p\}$, pois $K(\beta_j) = \Sigma_f(\mathbb{Q}) \nsubseteq KL_{i-1}$, segue que $KL_{i-1}(\beta_j) = KL_i$, para todo $j \in \{1, 2, \ldots, p\}$.

Como todos os conjugados de β_1 estão em $\Sigma_f(\mathbb{Q})$ e $\Sigma_f(\mathbb{Q}) \subseteq KL_i$, todos os conjugados de β_1 estão em KL_i. Portanto a extensão $KL_i : KL_{i-1} = KL_{i-1}(\beta_j) : KL_{i-1}$ é uma extensão normal.

Como $KL_i = KL_{i-1}(\alpha_i)$, segue pela definição de extensão normal, que todas as raízes de $P_{\alpha_i|KL_{i-1}}(X) = X^{n_i} - {\alpha_i}^{n_i}$ estão em KL_i. Então, $\xi\alpha_i \in KL_i \subseteq \mathbb{R}$, onde ξ percorre todas as raízes n_i-ésima da unidade. Como $\xi\alpha_i \in \mathbb{R}$ e $\alpha_i \in L_i \subseteq \mathbb{R}$, ξ deve ser um número real. Mas as únicas raízes n_i-ésimas reais da unidade são ± 1. Logo $\xi = \pm 1$ e isso implica que todas as raízes de $X^{n_i} - {\alpha_i}^{n_i}$ resumem-se a α_i e $-\alpha_i$. Portanto, $n_i = 2$.

Como $P_{\beta_j|KL_{i-1}}(X)|P_{\beta_j|K}(X) = (X - \beta_1)\ldots(X - \beta_p)$ e

$$\partial P_{\beta_j|KL_{i-1}}(X) = [KL_{i-1}(\beta_j) : KL_{i-1}] = [KL_i : KL_{i-1}] \overset{2.3}{=} n_i = 2$$

segue que para todo $j \in \{1, 2, \ldots, p\}$, existe $r_j \in \{1, 2, \ldots, p\} - \{j\}$ tal que

$$P_{\beta_j|KL_{i-1}}(X) = (X - \beta_j)(X - \beta_{r_j})$$

Para todo $i, j \in \mathbb{N}$, temos que

$$P_{\beta_i|KL_{i-1}}(X) = P_{\beta_j|KL_{i-1}}(X) \iff (X - \beta_i)(X - \beta_{r_i}) = (X - \beta_j)(X - \beta_{r_j})$$

$$\iff i \in \{j, r_j\} \iff j \in \{i, r_i\}$$

Assim, a família $\{j, r_j\}$ para $j = \{1, \ldots, p\}$ define uma partição no conjunto $\{1, 2, \ldots, p\}$ e como $\#\{j, r_j\} = 2$, $\forall j = \{1, \ldots, p\}$, segue que p é um número par, ou seja, $p = 2$. Portanto, $|Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})|$ é uma potência de 2. ■

2.2 Aplicações

Veremos, agora, algumas aplicações do Teorema de Solubilidade por Radicais Reais.

Corolário 2.2.1. *Se $f(X) \in \mathbb{Q}[X]$ é irredutível, tem grau que não é potência de 2 e tem todas as raízes reais, então a equação $f(X) = 0$ não é solúvel por radicais reais.*

Demonstração: Como todas as raízes de f são reais, temos que $\mathbb{Q} \subseteq \Sigma_f(\mathbb{Q}) \subseteq \mathbb{R}$. Seja $\alpha \in \Sigma_f(\mathbb{Q})$ uma raiz de f. Então

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \Sigma_f(\mathbb{Q})$$

o que implica que $[\Sigma_f(\mathbb{Q}) : \mathbb{Q}] = [\Sigma_f(\mathbb{Q}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Mas note que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é igual ao grau do polinômio minimal de α sobre $\mathbb{Q}$ que é f, uma vez que α é uma raiz de f e f é irredutível sobre $\mathbb{Q}$ (se f não for um polinômio mônico basta dividir pelo coeficiente do termo de mais alto grau).

Então, $[\Sigma_f(\mathbb{Q}) : \mathbb{Q}]$ é múltiplo do grau de f. Já que o grau de f não é uma potência de 2, temos que $[\Sigma_f(\mathbb{Q}) : \mathbb{Q}]$ não é igual a uma potência de 2.

Como a extensão $\Sigma_f(\mathbb{Q}) : \mathbb{Q}$ é finita, normal e separável, por (1.2.18), temos que $[\Sigma_f(\mathbb{Q}) : \mathbb{Q}] = |Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})|$. Logo, a ordem do grupo $Gal(f)$ não é uma potência de 2, então, por (2.1.5), f não é solúvel por radicais reais. ■

O corolário acima diz que se um polinômio com todas as raízes reais é irredutível sobre $\mathbb{Q}$ e tem grau diferente de uma potência de 2, então é impossível expressar todas as suas raízes usando radicais reais sobre $\mathbb{Q}$. Particularmente, isso é válido para qualquer polinômio cúbico irredutível com todas as raízes reais.

Exemplo 2.2.2. *O polinômio $f(X) = X^3 - 3X + 1$ não é solúvel por radicais reais.*

Foi mostrado na introdução que o polinômio $f(X) = X^3 - 3X + 1$ tem todas as raízes reais. Além disso, ele é irredutível sobre $\mathbb{Q}$, uma vez que se $f(X)$ fosse redutível em $\mathbb{Q}$ ele teria, pelo menos, um fator irredutível de grau 1, o que não ocorre pois $f(X)$ não tem raízes racionais, por Briot-Ruffini. Assim, pelo corolário acima, f não pode ser solúvel por radicais reais.

Corolário 2.2.3. *Seja $f(X) \in \mathbb{Q}[X]$ com todas as raízes reais. Então todas as raízes de f são exprimíveis por radicais reais se, e somente se, todas as raízes de f são construtíveis com régua e compasso.*

Demonstração: Note que basta provar o resultado para cada fator irredutível de f. Então, vamos supor f irredutível. Pelo teorema (2.1.5), basta provar a seguinte afirmação:

Afirmação: A ordem do grupo $Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})$ é uma potência de 2 se, e somente se, todas as raízes de f são construtíveis com régua e compasso.

Antes de demonstrarmos a afirmação, vamos relembrar que $\mathcal{M}$ foi denotado como o conjunto de pontos iniciais tal que $\{0, 1\} \subseteq \mathcal{M}$ e que não estamos preocu-

pados com a cardinalidade de $\mathcal{M}$, por isso, no que segue, podemos tomar $\mathcal{M}$ como o conjunto mais conveniente a cada momento.

($\Longrightarrow$) Suponhamos que a ordem do grupo $Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})$ é uma potência de 2. Considerando $\mathcal{M} = \{0, 1\}$, temos que $\mathcal{K}_{\mathcal{M}} \overset{(.2.8)}{=} \mathbb{Q}$. Temos que a extensão $\Sigma_f(\mathbb{Q}) : \mathbb{Q}$ é finita, normal e separável. Então, pelo teorema (1.2.18) temos que $[\Sigma_f(\mathbb{Q}) : \mathbb{Q}] = |Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})|$ que é uma potência de 2.

Pelo teorema (.2.12), temos que $\Sigma_f(\mathbb{Q})$ está contido no conjunto dos pontos construtíveis $\mathcal{M}^{(\infty)}$. Como $\Sigma_f(\mathbb{Q})$ denota o corpo de raízes de f sobre $\mathbb{Q}$, temos que todas as raízes de f são construtíveis com régua e compasso.

($\Longleftarrow$) Suponhamos que todas as raízes de f são construtíveis com régua e compasso. Logo,

$$\Sigma_f(\mathbb{Q}) \subseteq \mathcal{M}^{(\infty)}$$

Sejam $z_1, z_2, \ldots, z_s$ as raízes de f. Então, se tomarmos $\mathcal{M} = \{0, 1\}$ temos que $\mathcal{K}_{\mathcal{M}} = \mathbb{Q}$ e, então, pelo teorema (.2.11),

$$[\mathbb{Q}(z_1) : \mathbb{Q}] \text{ é uma potência de 2}$$

Se tomarmos, agora, $\mathcal{M} = \{0, 1, z_1\}$ temos que $\mathcal{K}_{\mathcal{M}} = \mathbb{Q}(z_1)$, pois $z_1 = \overline{z_1}$ já que todas as raízes de f são reais. Então, analogamente, temos que

$$[\mathbb{Q}(z_1)(z_2) : \mathbb{Q}(z_1)] \text{ é uma potência de 2}$$

Fazendo esse mesmo processo, temos que

$$[\Sigma_f(\mathbb{Q}) : \mathbb{Q}] = [\mathbb{Q}(z_1, z_2, \ldots, z_s) : \mathbb{Q}] =$$
$$[\mathbb{Q}(z_1, \ldots, z_s) : \mathbb{Q}(z_1, \ldots, z_{s-1})] \ldots [\mathbb{Q}(z_1, z_2) : \mathbb{Q}(z_1)][\mathbb{Q}(z_1) : \mathbb{Q}]$$

que é uma potência de 2, uma vez que cada fator acima é uma potência de 2. Logo, $|Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})| = [\Sigma_f(\mathbb{Q}) : \mathbb{Q}]$ é uma potência de 2, o que completa a prova da afirmação. ■

Para a próxima aplicação precisamos do seguinte lema:

Lema 2.2.4. *Existem polinômios $P_n(X)$ e $Q_n(X)$ pertencentes a $\mathbb{Q}[X]$ tais que*

$$cos(nX) = P_n(cosX)$$

$$sen(nX) = senXQ_n(cosX)$$

tal que $\partial P_n(X) \leq n$ e $\partial Q_n(X) \leq n-1$.

Demonstração: A prova será feita por indução em n. Mas note que a base de indução para $P_n(X)$ será tomando $n = 0$ e a base de indução para $Q_n(X)$ será tomando $n = 1$, já que queremos que $\partial P_n(X) \leq n$ e $\partial Q_n(X) \leq n-1$.

Base de indução para $P_n(X) : n = 0$

Tomando $P_0(X) = 1$ temos que $cos(0X) = 1 = P_0(cosX)$ e $\partial P_0(X) = 0$.

Base de indução para $Q_n(X) : n = 1$

Tomando $Q_1(X) = 1$ temos que $senX = senXQ_1(cosX)$ e $\partial Q_1(X) = 0$.

Seja $n \geq 0$ (para o caso $cosX$), $n \geq 1$ (para o caso $senX$) e suponhamos que a afirmação seja válido para n, isto é, existem $P_n(X), Q_n(X) \in \mathbb{Q}[X]$ tais que $cos(nX) = P_n(cosX)$ e $sen(nX) = senXQ_n(cosX)$ com $\partial P_n(X) \leq n$ e $\partial Q_n(X) \leq n-1$.

Note que

$$cos((n+1)X) = cos(nX + X) = cos(nX)cosX - sen(nX)senX \overset{\text{H.I.}}{=}$$

$$cosXP_n(cosX) - sen^2XQ_n(cosX) = P_{n+1}(cosX)$$

onde $P_{n+1}(X) = XP_n(X) - (1-X^2)Q_n(X)$. Note que $\partial P_{n+1}(X) \leq n+1$, uma vez que $\partial XP_n(X) \leq n+1$ e $\partial(1-X^2)Q_n(X) \leq n+1$.

Da mesma forma,

$$sen((n+1)X) = sen(nX+X) = sen(nX)cosX + senXcos(nX) \overset{\text{H.I.}}{=}$$

$$senXQ_n(cosX)cosX + senXP_n(cosX) = senX(Q_n(cosX)cosX + P_n(cosX)) =$$

$$senXQ_{n+1}(cosX)$$

onde $Q_{n+1}(X) = XQ_n(X) + P_n(X) \in \mathbb{Q}[X]$. Note que $\partial Q_{n+1}(X) \leq n$, já que $\partial XQ_n(X) \leq n$ e $\partial P_n(X) \leq n$. ■

Corolário 2.2.5. *As seguintes afirmações são equivalentes:*

(i) $cos\left(\frac{2\pi}{n}\right)$ *é exprimível por radicais reais;*

(ii) O polígono regular de n lados é construtível com régua e compasso;

(iii) $n = 2^k p_1 p_2 \dots p_r$*, onde* $k \in \mathbb{N}$ *e* $p_1, p_2, \dots, p_r$ *são primos de Fermat distintos da forma* $p_i = 2^{2^{l_i}} + 1$*, onde* $i = \{1, \dots, r\}$.

Demonstração: $(ii) \iff (iii)$

Pelo corolário (.2.13), temos que o n-polígono regular poderá ser construído com régua e compasso se, e somente se, $\varphi(n)$ for uma potência de 2. Além disso, pela proposição (.2.15) $\varphi(n)$ é uma potência de 2 se, e somente se, $n = 2^k p_1 \dots p_r$ sendo $p_1, \dots, p_r$ primos de Fermat distintos. E, por fim, pela proposição (.2.16), para todo primo de Fermat p existe um $t \in \mathbb{N}$ tal que $p = 2^{2^t} + 1$.

$(i) \implies (ii)$

Pelo lema (2.2.4), existe $P_n(X) \in \mathbb{Q}[X]$ tal que $cos(nX) = P_n(cosX)$.

Como $cos\left(n\frac{2\pi}{n}\right) = cos(2\pi) = 1$, temos que $cos\left(\frac{2\pi}{n}\right)$ é raiz de

$$P_n(x) - 1$$

pois $P_n\left(cos\left(\frac{2\pi}{n}\right)\right) - 1 \overset{\text{lema(2.2.4)}}{=} cos\left(n\frac{2\pi}{n}\right) - 1 = 0$.

Afirmamos que, para cada $k \in \{1, \ldots, n-1, n\}$, $cos\left(\frac{2k\pi}{n}\right)$ é também raiz de $P_n(X) - 1$. De fato,

$$P_n\left(cos\left(\frac{2k\pi}{n}\right)\right) - 1 = cos\left(n\frac{2k\pi}{n}\right) - 1 = 0$$

O que implica que

$$\left(X - cos\left(\frac{2\pi}{n}\right)\right) \Big| P_n(X) - 1$$

$$\left(X - cos\left(\frac{4\pi}{n}\right)\right) \Big| P_n(X) - 1$$

$$\vdots$$

$$\left(X - cos\left(\frac{2(n-2)\pi}{n}\right)\right) \Big| P_n(X) - 1$$

$$\left(X - cos\left(\frac{2(n-1)\pi}{n}\right)\right) \Big| P_n(X) - 1$$

$$\left(X - cos\left(\frac{2n\pi}{n}\right)\right) \Big| P_n(X) - 1$$

No entanto, muitos destes divisores são iguais, como veremos a seguir.

Afirmação 1: $cos\left(\frac{2k\pi}{n}\right) = cos\left(\frac{2l\pi}{n}\right)$, $k \neq l$, $\{l, k\} \subseteq \{1, \ldots, n-1, n\}$ se, e somente se, $k + l = n$

Suponhamos que $k + l = n$ então

$$cos\left(\frac{2k\pi}{n}\right) = cos\left(\frac{2n\pi - 2l\pi}{n}\right) = cos\left(2\pi - \frac{2l\pi}{n}\right) = cos\left(\frac{2l\pi}{n}\right)$$

Por outro lado, suponhamos que

$$cos\left(\frac{2k\pi}{n}\right) = cos\left(\frac{2l\pi}{n}\right), k \neq l, \{l, k\} \subseteq \{0, 1, \ldots, n-1\}$$

Como $\{l, k\} \subseteq \{0, 1, \ldots, n-1\}$, $\frac{k}{n}, \frac{l}{n} < 1$. Então, $\frac{2k\pi}{n}$ e $\frac{2l\pi}{n}$ são ângulos que não completam nem uma volta na circunferência. Logo, $\frac{2k\pi}{n}$ e $\frac{2l\pi}{n}$ são ângulos entre 0 e

2π. Portanto,

$$\frac{2k\pi}{n} = 2\pi - \frac{2l\pi}{n}$$

Desse modo,

$$\frac{2k\pi}{n} + \frac{2l\pi}{n} = 2\pi \Longrightarrow \frac{k}{n} + \frac{l}{n} = 1 \Longrightarrow k + l = n$$

Afirmação 2: Se $k \neq n$ e $k \neq \frac{n}{2}$ então $cos\left(\frac{2k\pi}{n}\right)$ é raiz múltipla de $P_n(X) - 1$.

$$P_n(cosX) = cos(nX) \Longrightarrow -P_n'(cosX)senX = -nsen(nX)$$

Temos que se $X = \frac{2k\pi}{n}$, $k \neq n$, $k \neq \frac{n}{2}$ então $senX \neq 0$ enquanto $sen(nX) = 0$. Logo,

$$P_n'(cosX) = \frac{nsen(nX)}{senX} = 0$$

Como $P_n(cosX) - 1 = 0$ e $(P_n - 1)'(cosX) = P_n'(cosX) = 0$ concluimos que $cosX$ é (pelo menos) raiz dupla de $P_n(X) - 1$. Então,

$$\left(X - cos\left(\frac{2k\pi}{n}\right)\right)\left(X - cos\left(\frac{2l\pi}{n}\right)\right) \Bigg| (P_n(X) - 1)$$

se $k + l = n$, $k \neq l$, $\{k, l\} \subseteq \{0, 1, \ldots, n-1\}$.

Então, quando mostramos que cada fator $\left(X - cos\left(\frac{2k\pi}{n}\right)\right)$ para $k \in \{1, \ldots, n\}$ dividia $P_n(X) - 1$ e que para $k \neq n$ e $k \neq \frac{n}{2}$ as raízes são duplas, não precisamos descontar nenhum fator para $k \in \{1, \ldots, n\}$. Assim, obtemos

$$\prod_{k=1}^{n}\left(X - cos\left(\frac{2k\pi}{n}\right)\right) \Bigg| P_n(X) - 1$$

Como $\partial(P_n(X) - 1) \leq n$ concluimos que $\partial(P_n(x) - 1) = n$ e esses polinômios diferem por um fator constante, sendo que suas raízes são as mesmas. Em particular, todas as raízes de $P_n(X) - 1$ são reais.

Lembre que, pelo lema anterior, $P_n(X) \in \mathbb{Q}[x]$. Logo, o polinômio $P_n(X) - 1 \in \mathbb{Q}[X]$. Além disso, note que se $cos\left(\frac{2\pi}{n}\right)$ é exprimível por radicais reais então $cos\left(\frac{2k\pi}{n}\right), \forall k$ também é já que

$$cos\left(\frac{2k\pi}{n}\right) = \left(cos\left(\frac{2\pi}{n}\right)\right)^k$$

Ou seja, todas as raízes de $P_n(X) - 1$ são exprimíveis por radicais reais. Como $P_n(X) - 1 \in \mathbb{Q}[X]$ e tem todas as suas raízes reais, pelo corolário (2.2.3), todas as raízes de $P_n(X) - 1$ são construtíveis com régua e compasso.

Para mostrar que o polígono regular de n lados é construtível com régua e compasso precisamos provar que uma raiz n-ésima primitiva da unidade, digamos

$$e^{\frac{2\pi i}{n}} = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$$

é construtível com régua e compasso, uma vez que as demais raízes são potências dessa e produto de construtíveis continua sendo construtível.

Como $senX = \sqrt{1 - cosX^2}$ e $1 - cosX^2$ é construtível, pela proposição (.2.7), temos que $sen\left(\frac{2k\pi}{n}\right)$ também é construtível para todo k. Logo, como i é construtível também, temos que $e^{\frac{2\pi i}{n}}$ é construtível, ou seja, o polígono regular de n lados é construtível com régua e compasso.

$(ii) \Longrightarrow (i)$

Suponhamos que o polígono regular de n lados é construtível com régua e compasso. Então, pelo corolário (.2.13), temos que $\varphi(n)$ é uma potência de 2. Lembremos que o polinômio $\Phi_n(X)$ foi definido da seguinte forma (veja notação (1.3.5)):

$$\Phi_n(X) = \prod_{\eta \in \mathcal{P}_n(\mathbb{C})} (X - \eta)$$

Assim, o n-ésimo corpo ciclotômico é $\mathbb{Q}(\mathcal{R}_{X^n-1}) = \Sigma_{\Phi_n}(\mathbb{Q})$, pois basta adjuntarmos a $\mathbb{Q}$ as raízes n-ésimas primitivas da unidade.

Dessa forma, como a extensão $\Sigma_{\phi_n}(\mathbb{Q}) : \mathbb{Q}$ é finita, normal e separável, pelos teoremas (1.2.18) e (1.3.4), temos que

$$|Gal(\Sigma_{\phi_n}(\mathbb{Q}) : \mathbb{Q})| = [\Sigma_{\phi_n}(\mathbb{Q}) : \mathbb{Q}] = \varphi(n)$$

que é uma potência de 2. Como $\Sigma_{\phi_n}(\mathbb{Q}) = \mathbb{Q}(e^{\frac{2\pi i}{n}})$ e

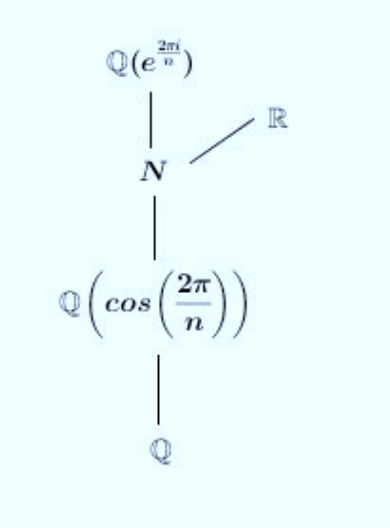
$$cos\left(\frac{2\pi}{n}\right) = \frac{1}{2}\left(e^{\frac{2\pi i}{n}} + e^{\frac{-2\pi i}{n}}\right)$$

temos as seguintes extensão de corpos:

$$\begin{array}{c} \mathbb{Q}(e^{\frac{2\pi i}{n}}) \\ | \\ \mathbb{Q}\left(cos\left(\frac{2\pi}{n}\right)\right) \\ | \\ \mathbb{Q} \end{array}$$

Como $[\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}]$ é uma potência de 2, temos que $[\mathbb{Q}(cos\left(\frac{2\pi}{n}\right)) : \mathbb{Q}]$ também é uma potência de 2.

Seja N o corpo de raízes de $P_{(cos\left(\frac{2\pi}{n}\right))|\mathbb{Q}}(X)$. Na demonstração do item anterior mostramos que $cos\left(\frac{2\pi}{n}\right)$ é raiz de $P_n(X)-1$, o que implica que $P_{(cos\left(\frac{2\pi}{n}\right))|\mathbb{Q}}(X)$ divide $P_n(X) - 1 \in \mathbb{Q}[X]$. Além disso, mostramos também que o polinômio $P_n(X) - 1$ possuia todas as suas raízes reais, consequentemente, $P_{cos\left(\frac{2\pi}{n}\right)|\mathbb{Q}}(X)$ também tem todas as raízes reais. Logo, $N \subseteq \mathbb{R}$. Assim, temos:



Então $|Gal(N:\mathbb{Q})| = [N:\mathbb{Q}]$ é uma potência de 2. Então, pelo teorema (2.1.5), $P_{(cos\left(\frac{2\pi}{n}\right))|\mathbb{Q}}(X)$ é solúvel por radicais reais, o que implica que $(cos\left(\frac{2\pi}{n}\right))$ é exprimível por radicais reais. ■

Corolário 2.2.6. *Se* $mdc(p,q) = 1$ *então* $cos\left(\frac{p\pi}{q}\right)$ *é exprimível por radicais reais se, e somente se, o polígono regular de* q *lados é construtível com régua e compasso.*

Demonstração: $(\Longleftarrow)$: Suponhamos que o polígono regular de q lados é construtível com régua e compasso. Então, pelo corolário (2.2.5), $q = 2^k p_1 p_2 \dots p_r$, onde $k \in \mathbb{N}$ e $p_1, p_2, \dots, p_r$ são primos de Fermat distintos. Consequentemente, $2q = 2^{k+1} p_1 p_2 \dots p_r$, onde $k \in \mathbb{N}$ e $p_1, p_2, \dots, p_r$ são primos de Fermat distintos.

Então, o polígono regular de $2q$ lados é construtível com régua e compasso. Novamente, pelo corolário (2.2.5), $cos\left(\frac{2\pi}{2q}\right) = cos\left(\frac{\pi}{q}\right)$ é exprimível por radicais reais. Dessa forma, $\left(cos\left(\frac{\pi}{q}\right)\right)^p = cos\left(\frac{p\pi}{q}\right)$ é exprimível por radicais reais.

$(\Longrightarrow)$: Suponhamos que $cos\left(\frac{p\pi}{q}\right)$ é exprimível por radicais reais.

1) p ímpar

Neste caso, $mdc(p, 2q) = 1$.

Afirmação: $cos\left(\frac{p\pi}{q}\right)$ é uma raiz $2q$-ésima primitiva da unidade.

Já vimos que $\mathcal{P}_n(K) = \{z^l; 1 \leq l \leq n; mdc(l,n) = 1\}$ com $z \in \mathcal{P}_n(K)$. Temos que

$$cos\left(\frac{p\pi}{q}\right) = cos\left(p\frac{2\pi}{2q}\right)$$

Denotando $z = cos\left(\frac{2\pi}{2q}\right)$ temos

$$z^{2q} - 1 = (cos2\pi) - 1 = 0$$

Então, z é uma raiz de $X^{2q} - 1$. Como $mdc(p, 2q) = 1$, $z^p \in \mathcal{P}_{2q}(K)$ e $z^p = cos\left(\frac{2p\pi}{2q}\right)$. Ou seja, $cos\left(\frac{p\pi}{q}\right)$ é uma raiz $2q$-ésima primitiva da unidade.

Então, por definição de raiz primitiva, temos que $cos\left(\frac{2\pi}{2q}\right)$ é uma potência de $cos\left(\frac{p\pi}{q}\right)$ que é exprimível por radicais reais. Logo, $cos\left(\frac{2\pi}{2q}\right)$ é exprimível por radicais reais. Dessa maneira, pelo corolário (2.2.5), o polígono de $2q$ lados é construtível com régua e compasso. Novamente, o corolário nos diz que $2q = 2^k p_1 p_2 \dots p_r$, onde $k \geq 1$ e $p_1, p_2, \dots, p_r$ são primos de Fermat distintos. Assim, $q = 2^k p_1 p_2 \dots p_r$, onde $k \geq 0$ e $p_1, p_2, \dots, p_r$ são primos de Fermat distintos. Então, o polígono regular de q lados é construtível com régua e compasso.

2) p par

Como p é par, $p = 2k$ com $k \in \mathbb{N}$. Então, $mdc(k, q) = 1$. Temos que

$$cos\left(\frac{p\pi}{q}\right) = cos\left(k\frac{2\pi}{q}\right)$$

E, pelo mesmo argumento dado acima, temos que $cos\left(k\frac{2\pi}{q}\right)$ é uma raiz q-ésima primitiva da unidade. Então $cos\left(\frac{2\pi}{q}\right)$ é potência de $cos\left(\frac{2k\pi}{q}\right)$ que é exprimível por radicais reais. Assim, $cos\left(\frac{2\pi}{q}\right)$ é exprimível por radicais reais. Pelo corolário (2.2.5), o polígono regular de q lados é construtível com régua e compasso. ■

Capítulo 3

O Cálculo do Grupo de Galois em $\mathbb{Q}[X]$

O objetivo deste capítulo será mostrar que dado $f(X) \in \mathbb{Q}[X]$ é sempre possível encontrar o grupo $Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})$. Para tal nos baseamos em ([4]).

3.1 Fatoração Efetiva

Antes de demonstrarmos o que foi afirmado acima, trataremos de alguns aspectos sobre fatoração efetiva.

Definição 3.1.1. *Seja D um domínio de fatoração única e $f(X) \in D[X]$. O conteúdo de $f(X)$ é o máximo divisor comum dos coeficientes de f e será denotado por $c(f(X))$. Além disso, f é dito polinômio primitivo quando o $c(f(X))$ é um elemento invertível de D.*

É claro que se D é um domínio de fatoração única então $f(X) = c(f(X))g(X)$ com $g(X) \in D[X]$ agora um polinômio primitivo.

Lema 3.1.2. *Sejam D um domínio e $f(X), g(X) \in D[X]$ polinômios de grau menor ou igual a n tais que $f(\alpha) = g(\alpha)$ para $n+1$ elementos distintos $\alpha \in D$. Então $f(X) = g(X)$.*

Teorema 3.1.3. (Fórmula de Interpolação de Lagrange) *Sejam K um corpo, $a_1, \ldots, a_{n+1}$ distintos elementos de K e $b_1, \ldots, b_{n+1}$ elementos quaisquer de K.Então,*

$$f(X) = \sum_{i=1}^{n+1} b_i \frac{(X-a_1)\ldots\widehat{(X-a_i)}\ldots(X-a_{n+1})}{(a_i-a_1)\ldots\widehat{(a_i-a_i)}\ldots(a_i-a_{n+1})}$$

é o único polinômio em $K[X]$ de grau menor ou igual a n tal que $f(a_i) = b_i, \forall i \in \{1, \ldots, n+1\}$. O símbolo $\widehat{a}$ significa que omitimos o fator a.

Definição 3.1.4. *Dado D um domínio de fatoração única, a fatoração em D é dita efetiva quando existir algum algoritmo capaz de efetivamente encontrar a fatoração de todo elemento de D como um produto de fatores irredutíveis.*

Notação 3.1.5. *No restante deste texto, o símbolo $p(a_1, \ldots, a_n) \in D[a_1, \ldots, a_n]$ significará que estamos avaliando o polinômio $p(X_1, \ldots, X_n) \in D[X_1, \ldots, X_n]$ em $a_1, \ldots, a_n$.*

Teorema 3.1.6. *A fatoração em $\mathbb{Q}[X]$ é efetiva.*

Demonstração: Nessa demonstração, utilizaremos o fato de que $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, que, por sua vez, é um domínio de fatoração única com um número finito de elementos invertíveis no qual a fatoração é efetiva*, pelo Teorema Fundamental da Aritmética.

Seja $g(X) \in \mathbb{Q}[X]$ o polinômio cuja fatoração queremos determinar. Então,

$$g(X) = \frac{1}{\alpha'} h(X)$$

*Por exemplo, o crivo de Eratóstenes nos permite não só decidir se um dado número n é ou não primo como também, no caso de n não ser primo, nos leva a uma fatoração em primos para n. Não estamos aqui tratando do problema "algoritmo computacionalmente viável".

onde α' é o mínimo múltiplo comum dos denominadores dos coeficientes de $g(X)$. Então $h(X) \in \mathbb{Z}[X]$ e, portanto, podemos ainda escrever

$$g(X) = \underbrace{\frac{\alpha''}{\alpha'}}_{=\alpha \in \mathbb{Q}} g_1(X) \tag{3.1}$$

sendo $\alpha'' = c(h(X))$ de modo que, agora, $g_1(X) \in \mathbb{Z}[X]$ é também um polinômio primitivo[†].

Ora, sendo $g(X)$ e $g_1(X)$ associados em $\mathbb{Q}[X]$, encontrar uma fatoração em irredutíveis para $g(X)$ em $\mathbb{Q}[X]$ equivale a encontrar uma fatoração em irredutíveis para $g_1(X)$ em $\mathbb{Q}[X]$. Como $g_1(X) \in \mathbb{Z}[X]$, pelo Lema de Gauss, procurar fatores irredutíveis de $g_1(X)$ em $\mathbb{Q}[X]$ equivale a procurar fatores irredutíveis para $g_1(X)$ em $\mathbb{Z}[X]$ e de grau maior ou igual a um.

Assim, vamos reduzir nossa demonstração a $\mathbb{Z}[X]$. Seja $g_1(X) \in \mathbb{Z}[X]$ um polinômio de grau r. Iremos analisar os fatores de $g_1(X)$ com grau maior ou igual a 1 e menor ou igual a $r-1$. Considere r elementos distintos em $\mathbb{Z}$, digamos $a_1, \ldots, a_r$ e defina os seguintes conjuntos:

$$D_i = \{a \in \mathbb{Z}; a \text{ é um divisor de } g_1(a_i)\}, \forall i \in \{1, \ldots, r\}$$

Note que cada D_i é conhecido, já que em $\mathbb{Z}$ a fatoração é efetiva e também é finito, pois em $\mathbb{Z}$ temos finitos elementos invertíveis.

Seja $G(X) \in \mathbb{Z}[X]$ um polinômio de grau menor ou igual a $r-1$ que divide $g_1(X) \in \mathbb{Z}[X]$, digamos $g_1(X) = G(X)L(X)$ com $G(X), L(X) \in \mathbb{Z}[X]$. Assim,

$$g_1(a_i) = G(a_i)L(a_i), \forall i \in \{1, \ldots, r\}$$

o que implica que $(G(a_1), \ldots, G(a_r)) \in D_1 \times \ldots \times D_r$.

[†]É importante mencionar que isso somente foi possível, pois em $\mathbb{Z}$ a fatoração é efetiva, assim podemos calcular tanto o mínimo múltiplo comum quanto o máximo divisor comum de inteiros.

Ora, dado um elemento qualquer $(\alpha_1, \ldots, \alpha_r) \in D_1 \times \ldots \times D_r$, pelo teorema (3.1.3), existe um um único polinômio $M_{\alpha_1,\ldots,\alpha_r}(X) \in \mathbb{Q}[X]$ de grau menor ou igual a $r-1$ tal que $M_{\alpha_1,\ldots,\alpha_r}(a_i) = \alpha_i, \forall i \in \{1, \ldots, r\}$.

Dessa forma, como $(G(a_1), \ldots, G(a_r)) \in D_1 \times \ldots \times D_r$, pelo o que dissemos acima, existe um único $M_{G(a_1),\ldots,G(a_r)}(X) \in \mathbb{Q}[X]$ de grau menor ou igual a $r-1$ tal que

$$M_{G(a_1),\ldots,G(a_r)}(a_i) = G(a_i), \forall i \in \{1, \ldots, r\}$$

o que, pela unicidade no lema (3.1.2), implica que $M_{\alpha_1,\ldots,\alpha_r}(X) = G(X) \in \mathbb{Z}(X)$. Consequentemente, $G(X)$ é um dos $M_{\alpha_1,\ldots,\alpha_r}(X)$ com $(\alpha_1, \ldots, \alpha_r) \in D_1 \times \ldots \times D_r$.

Como existem finitos $M_{\alpha_1,\ldots,\alpha_r}(X)$, já que todos os conjuntos D_i são finitos, basta listá-los todos e verificar quais deles são fatores de $g_1(X)$. Se nenhum dos $M_{\alpha_1,\ldots,\alpha_r}(X)$ dividir $g_1(X)$, então $g_1(X)$ é irredutível em $\mathbb{Z}[X]$.

Por outro lado, se conseguimos encontrar algum $M_{\alpha_1,\ldots,\alpha_r}(X)$ que divida $g_1(X)$, temos uma fatoração para $g_1(X)$, digamos

$$g_1(X) = M_{\alpha_1,\ldots,\alpha_r}(X) g_2(X)$$

com $1 \leq \partial M_{\alpha_1,\ldots,\alpha_r}(X) \leq r-1$ e $1 \leq \partial g_2(X) \leq r-1$. Então, continuamos o processo para encontrar fatores próprios tanto de $M_{\alpha_1,\ldots,\alpha_r}(X)$ quanto de $g_2(X)$. No entanto, é importante destacar que os fatores de $M_{\alpha_1,\ldots,\alpha_r}(X)$ e $g_2(X)$ são também fatores de $g_1(X)$, logo eles estão entre os $M_{\alpha_1,\ldots,\alpha_r}(X)$, assim, continuamos a procurá-los entre as possibilidades de $M_{\alpha_1,\ldots,\alpha_r}(X)$.

Esse processo é finito, porque a cada etapa baixamos o grau. ■

Resumindo, temos o seguinte algoritmo:

Dado $g(X) \in \mathbb{Q}[X]$ cuja fatoração queremos explicitar, os seguintes passos devem ser seguidos:

1º passo: Denotando por α' o mínimo múltiplo comum dos denominadores dos coeficientes de $g(X)$, escreva

$$g(X) = \alpha g_1(X)$$

tal que

$$\alpha = \frac{c(\alpha' g(X))}{\alpha'}$$

de modo que $g_1(X) \in \mathbb{Z}[X]$ é primitivo. Com isso, α é o fator de grau zero na fatoração de g.

Passamos, então, a analisar a fatoração de $g_1(X)$ em $\mathbb{Z}[X]$.

2º passo: Supondo $\partial g_1(X) = r$, escolha r inteiros distintos quaisquer $a_1, \ldots, a_r \in \mathbb{Z}$ e construa os conjuntos

$$D_i = \{a \in \mathbb{Z}; a \text{ é um divisor de } g_1(a_i)\}, \forall i \in \{1, \ldots, r\}$$

3º passo: Para cada $(\alpha_1, \ldots, \alpha_r) \in D_1 \times \ldots \times D_r$, determine o polinômio interpolador $M_{\alpha_1,\ldots,\alpha_r}(X)$ de grau menor ou igual a $r-1$ satisfazendo $M_{\alpha_1,\ldots,\alpha_r}(a_i) = \alpha_i, \forall i \in \{1, \ldots, r\}$.

4º passo: Verifique dentre a lista de todos os possíveis $M_{\alpha_1,\ldots,\alpha_r}(X)$ se algum $M_{\alpha_1,\ldots,\alpha_r}(X)$ divide $g_1(X)$ em $\mathbb{Z}[X]$.

Se nenhum $M_{\alpha_1,\ldots,\alpha_r}(X)$ dividir $g_1(X)$, então $g_1(X)$ é irredutível em $\mathbb{Z}[X]$ e a fatoração de $g(X)$ em $\mathbb{Q}[X]$ é simplesmente $g(X) = \alpha g_1(X)$. Caso contrário, $g_1(X) = M_{\alpha_1,\ldots,\alpha_r}(X) g_2(X)$ e, então, continuamos o processo procurando entre os interpoladores determinados no 3º passo e que não foram ainda testados, quais são divisores tanto de $M_{\alpha_1,\ldots,\alpha_r}(X)$ quanto de $g_2(X)$.

Exemplo 3.1.7. *Sem usar Baskhara, tentemos chegar à fatoração de*

$$g(X) = X^2 + \frac{4}{5}X - \frac{1}{5}$$

Aplicando o 1º passo chegamos a

$$g(X) = \underbrace{\frac{1}{5}}_{\alpha}\ (\underbrace{5X^2 + 4X - 1}_{g_1(X)})$$

já que $c(5X^2+4X-1) = 1$. Agora vamos encontrar os fatores não constantes $G(X)$ de $g_1(X)$ tais que $\partial G(X) \leq 2 - 1 = 1$. Pelo 2º passo, como $\partial g_1 = 2$, precisamos escolher dois valores inteiros quaisquer. Neste exemplo, escolhemos $a_1 = 0$ e $a_2 = 1$. Logo,

$$D_1 \overset{g_1(0)=-1}{=} \{ \text{ divisores de -1 } \} = \{-1, 1\}$$
$$D_2 \overset{g_1(1)=8}{=} \{ \text{ divisores de 8 } \} = \{-1, 1, -2, 2, -4, 4, -8, 8\}$$

Assim, temos 16 possibilidades para o interpolador de Lagrange. Para cada $\{b_1, b_2\} \in D_1 \times D_2$, por (3.1.3), temos que

$$M_{b_1,b_2}(X) = b_1(1 - X) + b_2(X)$$

é o único polinômio em $\mathbb{Q}[X]$ de grau um tal que $M_{b_1,b_2}(a_i) = b_i$, para $i \in \{1, 2\}$.

Ao testar o par $\{1, 2\} \in D_1 \times D_2$, temos que $M_{1,2}(X) = X + 1$ que é um fator de $g_1(X)$. Dessa forma, dividindo $g_1(X)$ por $M_{1,2}(X)$ encontramos o outro fator de $g_1(X)$, chegando à fatoração

$$g(X) = X^2 + \frac{4}{5}X - \frac{1}{5} = \frac{1}{5}(X + 1)(5X - 1)$$

Exemplo 3.1.8. *Seja*

$$g(X) = X^3 - 3X + 1$$

Já sabemos, pela Introdução, que este polinômio possui três raízes reais e, por (2.2.2), temos que $g(X)$ é irredutível em $\mathbb{Q}[X]$. Vamos verificar esta irredutibilidade pelo método da fatoração efetiva.

Neste caso, como $g(X) \in \mathbb{Z}[X]$ e é mônico, pelo 1º passo temos que $\alpha = 1$ e $g_1(X) = g(X)$.

Queremos agora encontrar os fatores de $g(X)$ não constantes e com grau menor ou igual a 3-1=2. Escolhemos $a_1 = -1$, $a_2 = 0$ e $a_3 = 1$ e construímos os conjuntos

$$D_1 \overset{\text{g}(-1)=3}{=} \{ \text{ divisores de 3 } \} = \{-1, 1, -3, 3\}$$
$$D_2 \overset{\text{g}(0)=1}{=} \{ \text{ divisores de 1 } \} = \{-1, 1\}$$
$$D_3 \overset{\text{g}(1)=-1}{=} \{ \text{ divisores de -1 } \} = \{-1, 1\}$$

Dado $\{b_1, b_2, b_3\} \in D_1 \times D_2 \times D_3$, por (3.1.3), temos que o polinômio interpolador de $M_{b_1,b_2,b_3}(a_i) = b_i$, para $i \in \{1, 2, 3\}$ é dado por

$$M_{b_1,b_2,b_3}(X) = b_1 \frac{X(X-1)}{2} + b_2(X+1)(X-1) + b_3 \frac{X(X+1)}{2}$$

Assim, temos 16 possibilidades para o interpolador de Lagrange.

$$M_{1,1,1}(X) = 2X^2 - 1$$
$$M_{1,-1-1}(X) = -X^2 - X + 1$$
$$M_{1,1,-1}(X) = X^2 - X - 1$$
$$M_{1,-1,1}(X) = 1$$
$$M_{-1,1,1}(X) = X^2 + X - 1$$
$$M_{-1,-1,-1}(X) = -2X^2 + 1$$
$$M_{-1,1,-1}(X) = -1$$
$$M_{-1,-1,1}(X) = -X^2 + X + 1$$
$$M_{3,1,1}(X) = 3X^2 - X - 1$$
$$M_{3,-1,-1}(X) = -2X + 1$$
$$M_{3,1,-1}(X) = 2X^2 - 2X - 1$$
$$M_{3,-1,1}(X) = X^2 - X + 1$$
$$M_{-3,1,1}(X) = 2X - 1$$

$$M_{-3,-1,-1}(X) = -3X^2 + X + 1$$
$$M_{-3,1,-1}(X) = -X^2 + X - 1$$
$$M_{-3,-1,1}(X) = -2X^2 + 2X + 1$$

Ao testarmos todos polinômios $M_{b_1,b_2,b_3}(X)$ vemos que nenhum $M_{b_1,b_2,b_3}(X)$ é fator de $g(X)$. Dessa forma, $g(X)$ é, de fato, irredutível em $\mathbb{Q}[X]$.

Teorema 3.1.9. *Se K é um corpo tal que a fatoração em $K[X]$ é efetiva então a fatoração em $K[X_1, \ldots, X_n]$ também é efetiva.*

Demonstração: Seja $h(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ e $m > \partial h(X_1, \ldots, X_n)$. Vamos substituir X_i por $T^{m^{i-1}}$ para todo $i \in \{1, \ldots, n\}$. Assim,

$$X_1 \longmapsto T \tag{3.2}$$

$$X_2 \longmapsto T^m$$
$$\vdots$$
$$X_n \longmapsto T^{m^{n-1}}$$

Consequentemente,

$$aX_1{}^{\alpha_1} \ldots X_n{}^{\alpha_n} \longmapsto aT^{\alpha_1} \ldots T^{m^{n-1}\alpha_n} = aT^{\alpha_1+\alpha_2 m+\ldots+\alpha_n m^{n-1}} \tag{3.3}$$

Como $m > \partial h(X_1, \ldots, X_n)$, temos que cada parcela de $h(X_1, \ldots, X_n)$ tem grau menor do que m; em particular, $m > \alpha_i, \forall i \in \{1, \ldots, n\}$. Assim, o expoente de T em (3.3) está expresso em base m (sabemos que todo número natural pode ser expresso em base m, isto é, se escreve unicamente da forma $y_1 + y_2 m + \ldots + y_n m^{n-1}$ com $0 \leq y_i \leq m-1$ para todo $i \in \{1, \ldots, n\}$ para algum $n \in \mathbb{N}^*$).

Logo, dois monômios distintos do tipo $X_1{}^{\alpha_1} \ldots X_n{}^{\alpha_n}$ e $X_1{}^{\beta_1} \ldots X_n{}^{\beta_n}$ darão origem a $T^{\alpha_1+\alpha_2 m+\ldots+\alpha_n m^{n-1}}$ e $T^{\beta_1+\beta_2 m+\ldots+\beta_n m^{n-1}}$, os quais têm necessariamente graus distintos, devido à unicidade da representação de um número em base m.

Com tais considerações, denotando por $h^*(T)$ o polinîmio obtido a partir de $h(X_1, \ldots, X_n)$ pela substituição (3.2), vemos que toda fatoração não trivial

$$h(X_1, \ldots, X_n) = g_1(X_1, \ldots, X_n)g_2(X_1, \ldots, X_n)$$

(isto é, $\partial g_1(X) \geq 1$ e $\partial g_2(X) \geq 1$) para $h(X_1, \ldots, X_n)$ dá origem a uma fatoração não trivial de $h^*(T)$, digamos, $h^*(T) = g_1^*(T)g_2^*(T)$.

Mas, por hipótese, $h^*(T)$ pode ser efetivamente fatorado em fatores irredutíveis. Reciprocamente, uma vez fixado $m > \partial h(X_1, \ldots, X_n)$, todo polinômio $g^*(T)$ pode ser visto como o transformado de um único polinômio $g(X_1, \ldots, X_n)$.

Passamos então a considerar todas as possíveis fatorações não triviais de $h^*(T)$ em dois fatores $h^*(T) = h_1(T)h_2(T)$ que é, por hipótese, um processo finito. Note que $\partial h_1(T), \partial h_2(T) < m^n$ e, assim, $h_1(T)$ e $h_2(T)$ correspondem a dois polinômios $g_1(X_1, \ldots, X_n)$ e $g_2(X_1, \ldots, X_n)$, respectivamente, univocamente determinados devido à substituição anterior. Ou seja, $h_1(T) = {g_1}^*(T)$ e $h_2(T) = {g_2}^*(T)$.

Uma vez obtida a fatoração $h^*(T) = h_1(T)h_2(T) = {g_1}^*(T){g_2}^*(T)$, vamos verificar se

$$h(X_1, \ldots, X_n) = g_1(X_1, \ldots, X_n)g_2(X_1, \ldots, X_n) \tag{3.4}$$

ou não. Uma pergunta que surge é: fazendo esse processo, não segue diretamente que $g_1(X_1, \ldots, X_n)$ e $g_2(X_1, \ldots, X_n)$ são fatores de $h(X_1, \ldots, X_n)$? A resposta é *não* e será dado um exemplo disso no final da demonstração. Se a igualdade não ocorrer para nenhuma fatoração de $h^*(T)$ então podemos concluir que $h(X_1, \ldots, X_n)$ é irredutível, uma vez que, se existisse outra fatoração para $h(X_1, \ldots, X_n)$, essa fatoração geraria uma nova fatoração para $h^*(T)$ então ocorreria a igualdade (3.4) para alguma fatoração de $h^*(T)$.

Por outro lado, se $h(X_1, \ldots, X_n) = g_1(X_1, \ldots, X_n)g_2(X_1, \ldots, X_n)$ basta repetirmos o mesmo processo, agora trabalhando com $g_1(X_1, \ldots, X_n)$ e $g_2(X_1, \ldots, X_n)$.

Logo, após um número finito de etapas, teremos efetivamente encontrado uma fatoração de $h(X_1, \ldots, X_n)$ em fatores irredutíveis, o que mostra que a fatoração em $K[X_1, \ldots, X_n]$ é efetiva. ■

Exemplo 3.1.10. *Uma vez encontrada uma fatoração* $h^*(T) = h_1(T)h_2(T) = {g_1}^*(T){g_2}^*(T)$ *onde* $h_1(T)$ *e* $h_2(T)$ *são, respectivamente, os transformados de* $g_1(X_1, \ldots, X_n)$ *e* $g_2(X_1, \ldots, X_n)$ *não temos necessariamente que* $g_1(X_1, \ldots, X_n)$ *e* $g_2(X_1, \ldots, X_n)$ *são fatores de* $h(X_1, \ldots, X_n)$.

De fato, tomemos $h(X_1, X_2) = X_1{X_2}^3$ e $m = 10$. Então,

$$h^*(T) = T^{1+3m} \overset{\text{m=10}}{=} T^{3+m}T^{8+m} = g_1^*(T)g_2^*(T)$$

onde $g_1(X_1, X_2) = {X_1}^3X_2$ e $g_2(X_1, X_2) = {X_1}^8X_2$, que claramente não nos fornecem uma fatoração para $h(X_1, X_2) = X_1{X_2}^3$.

3.2 Cálculo do Grupo de Galois

Para o cálculo do grupo de Galois de um polinômio $f(X) \in \mathbb{Q}[X]$, precisamos do Teorema Fundamental sobre Polinômios Simétricos, pois ele será útil para podermos garantir o cálculo efetivo de alguns polinômios.

Definição 3.2.1. *Seja* $L : K$ *uma extensão e* $u_1, \ldots, u_n \in L$. *Dizemos que* $u_1, \ldots, u_n$ *são algebricamente independentes sobre* K *se para qualquer polinômio* $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ *a igualdade* $f(u_1, \ldots, u_n) = 0$ *só ocorre se todos os coeficientes de* f *são nulos, ou seja, se* f *é o polinômio identicamente nulo.*

Definição 3.2.2. *Seja* K *um corpo. Um polinômio em* n *indeterminadas* $p(T_1, \ldots, T_n) \in K[T_1, \ldots, T_n]$ *é dito simétrico se qualquer permutação de suas indeterminadas o mantém inalterado:*

$$p(T_{\sigma(1)}, \ldots, T_{\sigma(n)}) = p(T_1, \ldots, T_n), \forall \sigma \in S_n$$

Lema 3.2.3. *Seja K um corpo e $T_1, \ldots, T_n$ indeterminadas algebricamente independentes sobre K. Todo polinômio $p(T_1, \ldots, T_n) \in K[T_1, \ldots, T_n]$ simétrico de grau um é necessariamente da forma $a(T_1 + \ldots + T_n) + b$.*

Demonstração: É claro que $p(T_1, \ldots, T_n) = a(T_1 + \ldots + T_n) + b$ é um polinômio simétrico de grau um.

Reciprocamente, dado um polinômio simétrico $p(T_1, \ldots, T_n)$ de grau um, temos que

$$p(T_1, \ldots, T_n) = a_1T_1 + \ldots + a_nT_n + b$$

Seja $i \neq j$ com $i, j \in \{1, \ldots, n\}$, então tomemos a permutação que troca T_i por T_j e as demais indeterminadas continuam inalteradas. Então, como $p(T_1, \ldots, T_n)$ é simétrico, temos que

$$p(T_1, \ldots, T_i, \ldots, T_j, \ldots, T_n) = p(T_1, \ldots, T_j, \ldots, T_i, \ldots, T_n)$$

Logo, $(a_i - a_j)T_i + (a_j - a_i)T_j = 0$, o que implica que $a_i = a_j = a, \forall i \neq j$. Portanto,

$$p(T_1, \ldots, T_n) = a(T_1 + \ldots T_n) + b$$

■

Definição 3.2.4. *Sejam K um corpo e $T_1, \ldots, T_n$ indeterminadas sobre K. Os polinômios*

$$S_1 = T_1 + \ldots + T_n$$

$$S_2 = \sum_{1 \leq i \leq j \leq n} T_iT_j$$

$$\vdots$$

$$S_n = \prod_{1 \leq i \leq n} T_i$$

são ditos polinômios simétricos elementares de $T_1, \ldots, T_n$.

Como motivação para o Teorema Sobre Polinômios Simétricos, observe o seguinte exemplo: seja

$$p(T_1, T_2, T_3) = {T_1}^2 T_2 T_3 + T_1 {T_2}^2 T_3 + T_1 T_2 {T_3}^2$$

que é simétrico em T_1, T_2, T_3. Então,

$${T_1}^2 T_2 T_3 + T_1 {T_2}^2 T_3 + T_1 T_2 {T_3}^2 = (T_1 + T_2 + T_3) T_1 T_2 T_3 = S_1 S_3$$

Note que o polinômio acima, quando analisado como um polinômio em T_3, ou seja,

$$p(T_1, T_2, T_3) = ({T_1}^2 T_2 + T_1 {T_2}^2) T_3 + (T_1 T_2) {T_3}^2$$

tem como coeficientes polinômios simétricos de $K[T_1, T_2]$. De fato, isso ocorre sempre, como nos mostra o lema a seguir.

Lema 3.2.5. *Seja K um corpo e $p(T_1, \ldots, T_n) \in K[T_1, \ldots, T_n]$ simétrico. Então os coeficientes de $p(T_1, \ldots, T_n) \in K[T_1, \ldots, T_{n-1}][T_n]$ são polinômios simétricos de $K[T_1, \ldots, T_{n-1}]$.*

Demonstração: Considere $p(T_1, \ldots, T_n)$ como um polinômio pertencente a $K[T_1, \ldots, T_{n-1}][T_n]$ de grau r. Então,

$$p(T_1, \ldots, T_n) = \varphi_0(T_1, \ldots, T_{n-1}) {T_n}^r + \varphi_1(T_1, \ldots, T_{n-1}) {T_n}^{r-1} + \ldots + \varphi_r(T_1, \ldots, T_{n-1})$$

sendo que $\partial\varphi_j(T_1, \ldots, T_{n-1}) \leq j$ ou $\varphi_j(T_1, \ldots, T_{n-1}) = 0$ para todo $j \in \{0, 1, \ldots, r\}$.

Suponhamos que exista um $j \in \{0, 1, \ldots, r\}$ tal que $\varphi_j(T_1, \ldots, T_{n-1})$ não é simétrico em $K[T_1, \ldots, T_{n-1}]$, isto é, existe uma permutação das indeterminadas $T_1, \ldots, T_{n-1}$ que não mantém $\varphi_j(T_1, \ldots, T_{n-1})$ inalterado.

Ora, toda permutação σ de $T_1, \ldots, T_{n-1}$ pode ser estendida a uma permutação τ de $T_1, \ldots, T_{n-1}, T_n$ de forma que $\tau(T_i) = \sigma(T_i)$ para $i \in \{1, \ldots, n-1\}$ e $\tau(T_n) = T_n$.

Dessa forma, se τ denota a extensão de φ_j então é uma permutação de $K[T_1, \ldots, T_n]$ que não mantém $p(T_1, \ldots, T_n)$ inalterado, o que contraria o fato de $p(T_1, \ldots, T_n)$ ser simétrico.

Portanto, os coeficientes de $p(T_1, \ldots, T_n) \in K[T_1, \ldots, T_n][T_n]$ são polinômios simétricos de $K[T_1, \ldots, T_{n-1}]$. ■

Outra propriedade a ser utilizada sobre polinômios simétricos e de fácil constatação é que a soma de polinômios simétricos é um polinômio simétrico.

Apresentamos a seguir a relação entre as raízes de um polinômio e os polinômios simétricos.

Lema 3.2.6. (Relações de Newton-Viète) *Seja* $f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$ *e* $x_1, \ldots, x_n$ *suas raízes. Então*

$$-\frac{a_1}{a_0} = S_1 = x_1 + \ldots + x_n$$

$$\frac{a_2}{a_0} = S_2 = \sum_{1 \leq i \leq j \leq n} x_i x_j$$

$$\vdots$$

$$(-1)^k \frac{a_k}{a_0} = S_k = \sum_{1 \leq i_1 \leq \ldots \leq i_k \leq n} x_{i_1} \ldots x_{i_k}$$

$$\vdots$$

$$(-1)^n \frac{a_n}{a_0} = S_n = x_1 \ldots x_n$$

onde $S_1, \ldots, S_n$ *são os polinômios simétricos elementares de* $x_1, \ldots, x_n$.

Teorema 3.2.7. (Teorema sobre Polinômios Simétricos- Parte I) *Seja* A *um anel comutativo e sejam* $T_1, \ldots, T_n$ *indeterminadas sobre* A. *Seja*

$$g(T_1, \ldots, T_n) = \sum_{j_1, \ldots, j_n} b_{j_1 \ldots j_n} {T_1}^{j_1} \ldots {T_n}^{j_n} \in A[T_1, \ldots, T_n]$$

um polinômio simétrico em $T_i, \forall i \in \{1, \ldots n\}$.

Então existe um polinômio que pode ser efetivamente encontrado,

$$h(S_1, \ldots, S_n) \in A[S_1, \ldots, S_n]$$

cujos coeficientes são combinações lineares inteiras dos coeficientes de $g(T_1, \ldots, T_n)$ *(ou seja, os coeficientes de* $h(S_1, \ldots, S_n)$ *são da forma* $\sum a_{j_1 \ldots j_n} b_{j_1 \ldots j_n}$ *com* $a_{j_1 \ldots j_n} \in \mathbb{Z}$*) e tal que* $g(T_1, \ldots, T_n) = h(S_1, \ldots, S_n)$.

Demonstração: A prova fará uso de indução tanto no número n de variáveis quanto no grau k de $g(T_1, \ldots, T_n)$.

Para $n = 1$, basta tomar $h(T_1) = g(T_1)$, pois $S_1 = T_1$ e já teremos $g(T_1) = h(T_1) = h(S_1)$ e, mais, $h(S_1)$ possui os mesmos coeficientes de $g(T_1)$.

Suponhamos que o teorema seja válido para qualquer polinômio simétrico em $n - 1$ variáveis. Vamos mostrar o resultado para um polinômio simétrico em n variáveis. Para tal, usamos agora indução sobre o grau de $g(T_1, \ldots, T_n)$.

Note que se $g(T_1, \ldots, T_n)$ é simétrico e tem grau menor ou igual a 1 então pelo lema (3.2.3) necessariamente ele é da forma

$$g(T_1, \ldots, T_n) = a_1(T_1 + \ldots + T_n) + a_0$$

com $a_1, a_0 \in A$ (pois $g(T_1, \ldots, T_n)$ é simétrico em $T_i, \forall i \in \{1, \ldots, n\}$). Assim, tomando $h(T_1, \ldots, T_n) = a_1 T_1 + a_0$ temos que $g(T_1, \ldots, T_n) = h(S_1, \ldots, S_n)$ e, note que, $h(S_1, \ldots, S_n)$ tem os mesmos coeficientes de $g(T_1, \ldots, T_n)$.

Suponhamos que o teorema seja válido para todos os polinômios simétricos em n variáveis que têm grau menor que k. Vamos mostrar que ele é válido também para polinômios simétricos a n indeterminadas e de grau k.

Seja $g(T_1, \ldots, T_n)$ um tal polinômio. Consideremos $g(T_1, \ldots, T_n)$ como um po-

linômio de $A[T_1, \ldots, T_{n-1}][T_n]$:

$$g(T_1, \ldots, T_n) = \phi_0(T_1, \ldots, T_{n-1}){T_n}^k + \phi_1(T_1, \ldots, T_{n-1}){T_n}^{k-1} + \ldots + \phi_k(T_1, \ldots, T_{n-1}) \tag{3.5}$$

sendo que $\partial\phi_j(T_1, \ldots, T_{n-1}) \leq j$ ou $\phi_j(T_1, \ldots, T_{n-1}) = 0$ para todo $j \in \{0, 1, \ldots, k\}$. Como $g(T_1, \ldots, T_n)$ é um polinômio simétrico em $T_i, \forall i \in \{1, \ldots, n\}$, pelo lema (3.2.5) temos que $\phi_j(T_1, \ldots, T_{n-1}), \forall j \in \{0, 1, \ldots, k\}$ é também simétrico em $T_i, \forall i \in \{1, \ldots, n-1\}$.

Para cada $1 \leq j \leq n-1$, defina $(S_j)_0 = (S_j)_0(T_1, \ldots, T_n) := S_j(T_1, \ldots, T_{n-1}, 0)$, que, portanto, são exatamente os polinômios simétricos elementares das variáveis $T_1, \ldots, T_{n-1}$.

Se $\phi_k(T_1, \ldots, T_{n-1}) = 0$ então T_n divide $g(T_1, \ldots, T_n)$ e como $g(T_1, \ldots, T_n)$ é simétrico em $T_1, \ldots, T_n$ temos que T_i divide $g(T_1, \ldots, T_n)$ para todo $i \in \{1, \ldots, n\}$, ou seja,

$$g(T_1, \ldots, T_n) = S_n\overline{g}(T_1, \ldots, T_n)$$

com $\overline{g}(T_1, \ldots, T_n) \in A[T_1, \ldots, T_n]$ simétrico e de grau menor ou igual a $k - n$. Assim, usando a hipótese de indução sobre k, podemos efetivamente encontrar um polinômio $h_2(T_1, \ldots, T_n) \in A[T_1, \ldots, T_n]$ tal que

$$\overline{g}(T_1, \ldots, T_n) = h_2(S_1, \ldots, S_n) \tag{3.6}$$

com grau menor ou igual a $k-n$ e cujos coeficientes são combinações lineares inteiras dos coeficientes de $\overline{g}(T_1, \ldots, T_n)$.

Assim, $g(T_1, \ldots, T_n) = S_n h_2(S_1, \ldots, S_n)$. E, portanto, o polinômio

$$h(T_1, \ldots, T_n) = T_n h_2(T_1, \ldots, T_n)$$

satisfaz as condições do teorema.

Se $\phi_k(T_1, \ldots, T_{n-1}) \neq 0$ então pela indução feita no número de geradores podemos encontrar efetivamente um polinômio $h_1(T_1, \ldots, T_{n-1}) \in A[T_1, \ldots, T_{n-1}]$ tal

que

$$\phi_k(T_1, \ldots, T_{n-1}) = h_1((S_1)_0, \ldots, (S_{n-1})_0) \tag{3.7}$$

com grau menor ou igual a k e cujos coeficientes são combinações lineares inteiras dos coeficientes de $\phi_k(T_1, \ldots, T_{n-1})$.

Definido o polinômio $h_1(T_1, \ldots, T_{n-1})$, consideramos a seguir polinômio

$$g_1(T_1, \ldots, T_n) = g(T_1, \ldots, T_n) - h_1(S_1, \ldots, S_{n-1}) \tag{3.8}$$

Assim, $\partial g_1(T_1, \ldots, T_n) \leq k$ e é simétrico em $T_1, \ldots, T_n$. E, não obstante a isso, utilizando as equações (3.5),(3.7) e (3.8),temos que T_n divide $g_1(T_1, \ldots, T_n)$, já que $g_1(T_1, \ldots, T_{n-1}, 0) = 0$.

Utilizando o mesmo raciocínio, devido ao fato que $g_1(T_1, \ldots, T_n)$ é simétrico em $T_1, \ldots, T_n$, temos que T_i divide $g_1(T_1, \ldots, T_n)$ para todo $i \in \{1, \ldots, n\}$, ou seja, S_n é um fator de $g_1(T_1, \ldots, T_n)$. Então,

$$g_1(T_1, \ldots, T_n) = S_n \overline{g}(T_1, \ldots, T_n) \tag{3.9}$$

com $\overline{g}(T_1, \ldots, T_n) \in A[T_1, \ldots, T_n]$ simétrico e de grau menor ou igual a $k - n$. Assim, usando a hipótese de indução sobre k, podemos efetivamente encontrar um polinômio $h_2(T_1, \ldots, T_n) \in A[T_1, \ldots, T_n]$ tal que

$$\overline{g}(T_1, \ldots, T_n) = h_2(S_1, \ldots, S_n) \tag{3.10}$$

com grau menor ou igual a $k-n$ e cujos coeficientes são combinações lineares inteiras dos coeficientes de $\overline{g}(T_1, \ldots, T_n)$.

Assim, temos:

$$g(T_1, \ldots, T_n) \overset{(3.8)}{=} g_1(T_1, \ldots, T_n) + h_1(S_1, \ldots, S_{n-1}) \overset{(3.9)}{=}$$

$$S_n \overline{g}(T_1, \ldots, T_n) + h_1(S_1, \ldots, S_{n-1}) \overset{(3.10)}{=}$$

$$S_n h_2(S_1, \ldots, S_n) + h_1(S_1, \ldots, S_{n-1})$$

cujos coeficientes, por construção, são combinações lineares inteiras dos coeficientes de $g(T_1, \ldots, T_n)$.

Portanto, o polinômio

$$h(T_1, \ldots, T_n) = h_1(T_1, \ldots, T_{n-1}) + T_n h_2(T_1, \ldots, T_n)$$

satisfaz as condições do teorema. ■

A demonstração acima nos garante um algoritmo para encontrar uma representação de um polinômio simétrico, como veremos a seguir.

Resumindo, temos o seguinte algoritmo:

Consideremos n o número de variáveis e k o grau total do polinômio simétrico $g(T_1, \ldots, T_n)$ que queremos expressar em função dos polinômios simétricos elementares.

1º passo: Se $n = 1$ então $S_1 = T_1$ e teremos $g(T_1) = g(S_1)$.

2º passo: Se $n > 1$, olhamos $g(T_1, \ldots, T_n)$ como um elemento de $A[T_1, \ldots, T_{n-1}][T_n]$:

$$g(T_1, \ldots, T_n) = \phi_0(T_1, \ldots, T_{n-1}){T_n}^k + \phi_1(T_1, \ldots, T_{n-1}){T_n}^{k-1} + \ldots + \phi_k(T_1, \ldots, T_{n-1})$$

Se $\phi_k(T_1, \ldots, T_{n-1}) = 0$ então $T_1, \ldots, T_n$ é fator de $g(T_1, \ldots, T_n)$. Logo,

$$g(T_1, \ldots, T_n) = \underbrace{T_1 \ldots T_n}_{S_n} \overline{g}(T_1, \ldots, T_n)$$

e repetimos o processo para $\overline{g}(T_1, \ldots, T_n)$, que é também um polinômio simétrico.

Defina $(S_j)_0 = (S_j)_0(T_1, \ldots, T_n) := S_j(T_1, \ldots, T_{n-1}, 0)$.

Se $\phi_k(T_1, \ldots, T_{n-1}) \neq 0$ escreva $\phi_k(T_1, \ldots, T_{n-1})$, que pelo lema (3.2.5) é um polinômio simétrico em $n-1$ indeterminadas, como um polinômio nos polinômios simétricos elementares, encontrando efetivamente um polinômio $h_1(T_1, \ldots, T_{n-1}) \in A[T_1, \ldots, T_{n-1}]$ tal que

$$\phi_k(T_1, \ldots, T_{n-1}) = h_1((S_1)_0, \ldots, (S_{n-1})_0)$$

com grau menor ou igual a k e cujos coeficientes são combinações lineares inteiras dos coeficientes de $\phi_k(T_1, \ldots, T_{n-1})$.

3º passo: Considere

$$g_1(T_1, \ldots, T_n) = g(T_1, \ldots, T_n) - h_1(S_1, \ldots, S_{n-1})$$

que certamente é divisível por $T_1 \ldots T_n = S_n$.

Escreva $g_1(T_1, \ldots, T_n) = S_n \overline{g}(T_1, \ldots, T_n)$ e repita o processo para $\overline{g}(T_1, \ldots, T_n)$ que continua sendo simétrico e tem grau menor do que o grau de $g_1(T_1, \ldots, T_n)$. Vamos, assim, encontrar $h_2(T_1, \ldots, T_n) \in A[T_1, \ldots, T_n]$ tal que

$$\overline{g}(T_1, \ldots, T_n) = h_2(S_1, \ldots, S_n)$$

com grau menor ou igual a $k-n$ e cujos coeficientes são combinações lineares inteiras dos coeficientes de $\overline{g}(T_1, \ldots, T_n)$.

4º passo: O polinômio

$$h(T_1, \ldots, T_n) = h_1(T_1, \ldots, T_{n-1}) + T_n h_2(T_1, \ldots, T_n)$$

é tal que $g(T_1, \ldots, T_n) = h(S_1, \ldots, S_n)$.

Exemplo 3.2.8. *Vamos aplicar o algoritmo acima para o polinômio*

$$g(T_1, T_2, T_3) = (T_1 - T_2)^2 + (T_2 - T_3)^2 + (T_3 - T_1)^2$$

$$= 2({T_1}^2 + {T_2}^2 + {T_3}^2 - T_1T_2 - T_2T_3 - T_3T_1)$$

Claramente $g(T_1, T_2, T_3)$ é simétrico em T_1, T_2, T_3. Olhando $g(T_1, T_2, T_3)$ como um polinômio em T_3, temos

$$g(T_1, T_2, T_3) = 2{T_3}^2 - 2(T_2 + T_1)T_3 + \underbrace{(2{T_1}^2 + 2{T_2}^2 - 2T_1T_2)}_{\phi_2(T_1, T_2)} \tag{3.11}$$

O próximo passo então é expressar o polinômio (simétrico) $\phi_2(T_1, T_2)$ em termos dos polinômios simétricos elementares a duas indeterminadas. Dessa forma, olhando-o como um polinômio em T_2, temos

$$\phi_2(T_1, T_2) = 2{T_2}^2 - (2T_1)T_2 + \underbrace{(2{T_1}^2)}_{\varphi_2(T_1)}$$

E $\varphi_2(T_1) = \varphi_2(S_1)$ com S_1 o polinômio simétrico elementar da indeterminada T_1 (ou seja, $S_1 = T_1$). Agora, considerando S_1, S_2 os polinômios simétricos elementares de T_1, T_2, temos

$$g_1(T_1, T_2) = \phi_2(T_1, T_2) - \varphi_2(S_1)$$

$$= 2{T_1}^2 + 2{T_2}^2 - 2T_1T_2 - 2(T_1 + T_2)^2 = -6T_1T_2 = -6S_2$$

De modo que $\phi_2(T_1, T_2) = 2{S_1}^2 - 6S_2$.

Repetimos agora este último passo para (3.11), considerando S_1, S_2 como os polinômios simétricos elementares de T_1, T_2, T_3.

$$g'(T_1, T_2, T_3) = g(T_1, T_2, T_3) - 2{S_1}^2 + 6S_2 =$$

$$2{T_3}^2 - 2T_2T_3 - 2T_1T_3 + 2{T_1}^2 + 2{T_2}^2 - 2T_1T_2 - 2(T_1+T_2+T_3)^2 + 6(T_1T_2+T_2T_3+T_1T_3) = 0$$

Logo, $g(T_1, T_2, T_3) = 2{S_1}^2 + 6S_2$.

Teorema 3.2.9. (Teorema sobre Polinômios Simétricos- Parte II) *Seja D um domínio e sejam $X, Z_1, \ldots, Z_m, T_1, \ldots, T_n$ indeterminadas sobre D. Seja*

$$f(X) = a_0X^n - a_1X^{n-1} + \ldots + (-1)^n a_n \in D[X]$$

com a_0 invertível em D, um polinômio com raízes $x_1, \ldots, x_n$ no fecho algébrico do corpo de frações de D. Seja

$$G(Z_1, \ldots, Z_m, T_1, \ldots, T_n) = \sum \beta_{i_1,\ldots,i_m,j_1,\ldots,j_n} {Z_1}^{i_1} \ldots {Z_m}^{i_m} {T_1}^{j_1} \ldots {T_n}^{j_n}$$

um polinômio em $D[Z_1, \ldots, Z_m, T_1, \ldots, T_n]$ *simétrico em* $T_1, \ldots, T_n$.

Então, $G(Z_1, \ldots, Z_m, x_1, \ldots, x_n) \in D[Z_1, \ldots, Z_m]$ *cujos coeficientes podem ser efetivamente expressados como funções polinomiais nos* $\beta_{i_1,\ldots,i_m,j_1,\ldots,j_n}$ *e* $\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}$ *sobre* $\mathbb{Z}$. *Em outras palavras, se* f *for mônico (caso que sempre poderá ser considerado se* D *for um corpo) os coeficientes de* $G(Z_1, \ldots, Z_m, x_1, \ldots, x_n)$ *podem ser expressos como funções polinomiais nos coeficientes de* G *e de* f *com coeficientes em* $\mathbb{Z}$.

Demonstração: Vamos considerar

$$G(Z_1, \ldots, Z_m, T_1, \ldots, T_n) = \sum \beta_{j_1,\ldots,j_n}(Z_1, \ldots, Z_m){T_1}^{j_1} \ldots {T_n}^{j_n}$$

como um polinômio de $D[Z_1, \ldots, Z_m][T_1, \ldots, T_n]$.

Pela parte I (Teorema (3.2.7)), podemos calcular efetivamente um polinômio

$$H(Z_1, \ldots, Z_m, S_1, \ldots, S_n) \in (D[Z_1, \ldots, Z_m])[S_1, \ldots, S_n]$$

cujos coeficientes são funções polinomiais nos coeficientes de G (pertencentes a $D[Z_1, \ldots, Z_n]$) e nos $S_1, \ldots, S_n$ sobre $\mathbb{Z}$ e é tal que

$$G(Z_1, \ldots, Z_m, T_1, \ldots, T_n) = H(Z_1, \ldots, Z_m, S_1, \ldots, S_n)$$

Assim, avaliando em $T_i = x_i, \forall i \in \{1, \ldots, n\}$ e fazendo uso das relações de Viete (3.2.6), temos que

$$G(Z_1, \ldots, Z_m, x_1, \ldots, x_n) = H(Z_1, \ldots, Z_m, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0})$$

cujos coeficientes podem ser efetivamente expressados como funções polinomiais nos coeficientes de G e nos $\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}$ sobre $\mathbb{Z}$. Além disso, note que

$$H(Z_1, \ldots, Z_m, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}) \in D[Z_1, \ldots, Z_m]$$

■

Definição 3.2.10. *Seja $L : K$ uma extensão de corpos. Definimos o grau de transcendência da extensão $L : K$ que será denotado por $trdeg_K L$ como a maior cardinalidade de um subconjunto S de L algebricamente independente sobre K.*

Teorema 3.2.11. *Sejam $M : L$ e $L : K$ duas extensões de corpos. Então,*

$$trdeg_K M = trdeg_L M + trdeg_K L$$

Demonstração: Suponhamos que $trdeg_L M = s$, sendo $Y_1, \ldots, Y_s \in M$ os elementos algebricamente independentes sobre L e que $trdeg_K L = n$, sendo $X_1, \ldots, X_n \in L$ os elementos algebricamente independentes sobre K. Primeiramente, vamos mostrar que o conjunto $\{Y_1, \ldots, Y_s, X_1, \ldots, X_n\} \subseteq M$ é algebricamente independente sobre K.

Se não fosse, teríamos uma relação algébrica não nula destes elementos sobre K, logo sobre L, dos elementos de M que são algebricamente independentes sobre L, o que não ocorre, então todos os coeficientes dos termos que envolvem os elementos de L são nulos. Ou seja, denotando por $f_i(Y_1, \ldots, Y_s)$ os distintos monômios nos Y_i nesta relação algébrica, temos

$$0 = \sum \underbrace{f_i(Y_1, \ldots, Y_s)}_{\in K[Y_1,\ldots,Y_s]} \underbrace{g_i(X_1, \ldots, X_n)}_{\in K[X_1,\ldots,X_n] \subseteq L}$$

o que implica que $g_i(X_1, \ldots, X_n) = 0$ para todo i. Assim, encontramos uma relação algébrica sobre K dos elementos $X_1, \ldots, X_n$ que foram supostos algebricamente independentes sobre K, logo todos os coeficientes dso g_i devem ser nulos, o que nos mostra que o conjunto $\{Y_1, \ldots, Y_s, X_1, \ldots, X_n\} \in M$ é algebricamente independente sobre K.

Temos que mostrar agora que M é algébrico sobre $K(X_1, ..., X_n, Y_1, ..., Y_s)$. Temos, por hipótese, que L é algébrica sobre $K(X_1, ..., X_n)$ e que M é algébrica sobre $L(Y_1, ..., Y_s)$. Então

$$M \overset{\text{alg}}{\supseteq} L(Y_1, ..., Y_s) \overset{\text{alg}}{\supseteq} K(X_1, ..., X_n)(Y_1, ..., Y_s) = K(X_1, ..., X_n, Y_1, ..., Y_s)$$

Logo, M é algébrico sobre $K(X_1, ..., X_n, Y_1, ..., Y_s)$ e o teorema segue. ■

Corolário 3.2.12. *Sejam $T_1, \ldots, T_n$ elementos algebricamente independentes sobre K e $x_1, \ldots, x_n$ algébricos sobre K. Então $T_1, \ldots, T_n$ são ainda algebricamente independente sobre $K(x_1, \ldots, x_n)$.*

Demonstração: Para isso, basta mostrarmos que

$$trdeg_{K(x_1,\ldots,x_n)}K(x_1, \ldots, x_n)(T_1, \ldots, T_n) = n$$

Por hipótese temos que $trdeg_K K(x_1, \ldots, x_n) = 0$ e que $trdeg_K K(T_1, \ldots, T_n) = n$.

Pelo teorema anterior, considerando os corpos

$$K \subseteq K(x_1, \ldots, x_n) \subseteq K(x_1, \ldots, x_n, T_1, \ldots, T_n)$$

temos

$$trdeg_K K(x_1, \ldots, x_n, T_1, \ldots, T_n) = trdeg_{K(x_1,\ldots,x_n)}K(x_1, \ldots, x_n, T_1, \ldots, T_n)$$

Por outro lado, considerando os corpos

$$K \subseteq K(T_1, \ldots, T_n) \subseteq K(x_1, \ldots, x_n, T_1, \ldots, T_n)$$

temos

$$trdeg_K K(x_1, \ldots, x_n, T_1, \ldots, T_n) =$$

$$trdeg_{K(T_1,\ldots,T_n)}K(x_1, \ldots, x_n, T_1, \ldots, T_n) + trdeg_K K(T_1, \ldots, T_n) = n$$

pois $trdeg_{K(T_1,\ldots,T_n)}K(x_1, \ldots, x_n, T_1, \ldots, T_n) = 0$.

Assim, $trdeg_{K(x_1,\ldots,x_n)}K(x_1, \ldots, x_n)(T_1, \ldots, T_n) = n$. ■

Vejamos agora o que os resultados até aqui mencionados nos ajudam no cálculo do grupo de Galois da extensão $\Sigma_f(K) : K$ sob determinadas condições. Lembremos

que o objetivo dessa seção é mostrar que dado $f(X) \in \mathbb{Q}[X]$ podemos encontrar o grupo de Galois de f sobre $\mathbb{Q}$, o que será uma consequência imediata do seguinte teorema:

Teorema 3.2.13. *Seja K um corpo e seja $f(X) \in K[X]$ um polinômio separável sobre K. Seja S_n o grupo das permutações do conjunto das raízes $\{x_1, \ldots, x_n\}$ de $f(X)$ (raízes que não são conhecidas em geral e que podem ter multiplicidade maior do que um, em geral). Sejam $T_1, \ldots, T_n$ indeterminadas sobre K e seja*

$$t = T_1x_1 + \ldots + T_nx_n$$

Então

(i) $Gal(\Sigma_f(K) : K) = \{\sigma \in S_n; T_1\sigma(x_1) + \ldots + T_n\sigma(x_n)$ é um conjugado de t sobre $K(T_1, \ldots, T_n)\}$;

(ii) Se a fatoração em $K[X]$ é efetiva então para todo $\sigma \in S_n$ é possível reconhecer se $T_1\sigma(x_1) + \ldots + T_n\sigma(x_n)$ é um conjugado de t sobre $K(T_1, \ldots, T_n)$, ou não (isto é, é possível reconhecer se $\sigma \in Gal(\Sigma_f(K) : K)$ ou não).

Redução:

Antes de demonstrarmos esse teorema, observamos que podemos supor, sem perda de generalidade, que as raízes de $f(x)$ são todas distintas. De fato, se a fatoração em $K[X]$ é efetiva, podemos efetivamente calcular

$$f(X) = f_1(X)^{e_1} \ldots f_r(X)^{e_r}$$

onde $f_1(X), \ldots, f_r(X)$ são polinômios irredutíveis distintos. Se tomarmos

$$\overline{f}(X) = f_1(X) \ldots f_r(X)$$

temos que $f(X)$ e $\overline{f}(X)$ possuem as mesmas raízes, de tal forma que $\Sigma_f(K) = \Sigma_{\overline{f}}(K)$ e, portanto, $Gal(\Sigma_f(K) : K) = Gal(\Sigma_{\overline{f}}(K) : K)$.

Como $f(X)$ é separável sobre K, por hipótese, temos que todas as raízes de $\overline{f}(X)$ tem multiplicidade igual a um. Portanto, podemos trabalhar com $\overline{f}(X)$, ou seja, podemos supor que todas as raízes de f são distintas.

Note que, como consequência desse teorema, teremos que para qualquer polinômio $f(X) \in \mathbb{Q}[X]$ sempre poderemos encontrar $Gal(\Sigma_f(K) : K)$, uma vez que em $\mathbb{Q}[X]$ a fatoração é efetiva e todo polinômio $f(X) \in \mathbb{Q}[X]$ é separável sobre Q.

Agora, veremos alguns lemas que serão úteis para provar o teorema acima.

Notação 3.2.14. *No que segue, dado $f(X) \in K[X]$ separável sobre K e sendo $x_1, \ldots, x_n$ todas as suas raízes, vamos denotar por S_n o conjunto das permutações de $x_1, \ldots, x_n$. Assim, cada $\sigma \in S_n$ induz naturalmente um K-automorfismo de $Gal(\Sigma_f(K) : K)$, uma vez que $\Sigma_f(K) = K(x_1, \ldots, x_n)$.*

Continuaremos a denotar por σ o automorfismo induzido por $\sigma \in S_n$:

$$\sigma\left(\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}\right) = \frac{f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{g(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}$$

Fixadas n indeterminadas $T_1, \ldots, T_n$ algebricamente independentes sobre K (e portanto sobre $K(x_1, \ldots, x_n)$, pelo corolário (3.2.12)) cada K-automorfismo σ de $\Sigma_f(K) = K(x_1, \ldots, x_n)$ induz de maneira natural um $K(T_1, \ldots, T_n)$-automorfismo de $K(x_1, \ldots, x_n, T_1, \ldots, T_n)$ que passamos a denotar por $\overline{\sigma}$ e que é tal que

$$\overline{\sigma}(T_i) = T_i \text{ e } \overline{\sigma}|_{K(x_1,\ldots,x_n)} = \sigma$$

Lema 3.2.15. *Sejam K um corpo, $f(X) \in K[X]$ separável sobre K e $\{x_1, \ldots, x_n\}$ suas raízes que vamos supor todas distintas. Sejam $T_1, \ldots, T_n$ indeterminadas algebricamente independentes sobre K. Então, com a notação (3.2.14) e considerando f também como um polinômio de $K(x_1, \ldots, x_n, T_1, \ldots, T_n)[X]$, temos*
(i) $\sigma \in Gal(\Sigma_f(K) : K) \iff \overline{\sigma} \in Gal(\Sigma_f(K(T_1, \ldots, T_n)) : K(T_1, \ldots, T_n))$. Em outras palavras, podemos continuar denotando $\overline{\sigma}$ por σ;

Ainda, definindo

$$t = T_1x_1 + \ldots T_nx_n$$

temos

(ii) t é algébrico sobre $K(T_1, \ldots, T_n)$ e t é um elemento primitivo da extensão $K(x_1, \ldots, x_n, T_1, \ldots, T_n) : K(T_1, \ldots, T_n)$;

(iii) $\sigma \in Gal(\Sigma_f(K(T_1, \ldots, T_n)) : K(T_1, \ldots, T_n)) \iff \sigma(t)$ é um conjugado de t sobre $K(T_1, \ldots, T_n)$.

Demonstração: (i) É claro, devido à definição de $\overline{\sigma}$ apresentada na notação (3.2.14).

(ii) De fato, como a extensão $K(x_1, \ldots, x_n, T_1, \ldots, T_n) : K(T_1, \ldots, T_n)$ é algébrica, já que $x_1, \ldots, x_n$ são algébricos sobre K, e $t \in K(x_1, \ldots, x_n, T_1, \ldots, T_n)$ temos que t é algébrico sobre $K(T_1, \ldots, T_n)$.

Além disso, temos que t é um elemento primitivo da extensão $K(x_1, \ldots, x_n, T_1, \ldots, T_n) : K(T_1, \ldots, T_n)$.

Como $x_1, \ldots, x_n$ são raízes de $f(X)$ que é um polinõmio separável em $K[X] \subseteq K(T_1, \ldots)[X]$, temos que $P_{x_i|K(T_1,\ldots,T_n)}$ são separáveis sobre $K(T_1, \ldots, T_n)[X]$.

Sejam $\sigma_1, \ldots, \sigma_n$ todos os possíveis K-automorfismos diferentes de $K(x_1, \ldots, x_n)$. Como já foi falado, podemos estender esses automorfismos até automorfismos de $K(x_1, \ldots, x_n, T_1, \ldots, T_n)$ tomando $\sigma_i(T_j) = T_j$. Tais extensões são elementos do conjunto $Aut(K(T_1, \ldots, T_n)(x_1, \ldots, x_n) : K(T_1, \ldots, T_n))$.

Então $\sigma_1, \ldots, \sigma_n$ são também todos os possíveis $K(T_1, \ldots, T_n)$-automorfismos diferentes de $K(T_1, \ldots, T_n, x_1, \ldots, x_n)$. De fato, se existisse σ_{n+1} distintos dos demais, como $\sigma_{n+1}(T_j) = T_j = \sigma_i(T_j)$, $\forall i \in \{1, \ldots, n\}$, então teríamos encontrado mais um K-automorfismo de $K(x_1, \ldots, x_n)$ distinto dos demais, o que não ocorre.

Consideremos o polinômio

$$p(t_1, \ldots, t_n) = \prod_{i \neq j} (t_1\sigma_i(x_1) + \ldots + t_n\sigma_i(x_n) - t_1\sigma_j(x_1) - \ldots - t_n\sigma_j(x_n))$$

pertencente a $K(x_1, \ldots, x_n)[t_1, \ldots, t_n] \subseteq K(T_1, \ldots, T_n)(x_1, \ldots, x_n)[t_1, \ldots, t_n]$.

Como $i \neq j$, temos que cada fator de $p(t_1, \ldots, t_n)$ é diferente de zero, logo, $p(t_1, \ldots, t_n) \neq 0$. Então, existe $(c_1, \ldots, c_n) \in K(T_1, \ldots, T_n)(x_1, \ldots, x_n)[t_1, \ldots, t_n]$ tal que $p(c_1, \ldots, c_n) \neq 0$. Mas note que $p(T_1, \ldots, T_n) \neq 0$, pois $T_1, \ldots, T_n$ são algebricamente independentes sobre $K(x_1, \ldots, x_n)$. Logo,

$$o \neq p(T_1, \ldots, T_n) = \prod_{i \neq j} (\sigma_i(T_1x_1 + \ldots + T_nx_n) - \sigma_j(T_1x_1 + \ldots + T_nx_n))$$

Então, $\sigma_1(T_1x_1 + \ldots + T_nx_n), \ldots, \sigma_n(T_1x_1 + \ldots + T_nx_n)$ são todos distintos.

Afirmação:$[K(T_1, \ldots, T_n)(T_1x_1 + \ldots + T_nx_n) : K(T_1, \ldots, T_n)] \geq n$

De fato, como qualquer $K(T_1, \ldots, T_n)$-automorfismo de $K(T_1, \ldots, T_n)(T_1x_1 + \ldots + T_nx_n)$ associa $T_1x_1 + \ldots + T_nx_n$ a alguma raiz do seu polinômio minimal e $\sigma_1(T_1x_1 + \ldots + T_nx_n), \ldots, \sigma_n(T_1x_1 + \ldots + T_nx_n)$ são todos distintos temos que o polinômio minimal de t sobre $K(T_1x_1, \ldots, T_nx_n)$ tem pelo menos n raízes, ou seja, tem pelos menos grau n.

Além disso, temos que $[K(T_1, \ldots, T_n)(x_1, \ldots, x_n) : K(T_1, \ldots, T_n)] = n$, uma vez que como $K(T_1, \ldots, T_n)(x_1, \ldots, x_n) : K(T_1, \ldots, T_n)$ é uma extensão finita, normal e separável, temos

$$[K(T_1, \ldots, T_n)(x_1, \ldots, x_n) : K(T_1, \ldots, T_n)] =$$

$$|Gal(K(T_1, \ldots, T_n)(x_1, \ldots, x_n) : K(T_1, \ldots, T_n))| = n$$

Portanto,

$$n \leq [K(T_1, \ldots, T_n)(T_1x_1 + \ldots + T_nx_n) : K(T_1, \ldots, T_n)]$$

$$\leq [K(T_1, \ldots, T_n)(x_1, \ldots, x_n) : K(T_1, \ldots, T_n)] = n$$

Logo, $K(T_1, \ldots, T_n)(x_1, \ldots, x_n) = K(T_1, \ldots, T_n)(t)$

(iii) $(\Longrightarrow)$ Como $P_{t|K(T_1,\ldots,T_n)}(X) \in K(T_1, \ldots, T_n)[X]$ temos que

$$P_{t|K(T_1,\ldots,T_n)}(X) = \sum \frac{f_i(T_1, \ldots, T_n)}{g_i(T_1, \ldots, T_n)} X^i$$

Logo,

$$0 = \sigma(0) = \sigma(P_{t|K(T_1,\ldots,T_n)}(t)) = \sigma\left(\sum \frac{f_i(T_1, \ldots, T_n)}{g_i(T_1, \ldots, T_n)} t^i\right)$$

Como $\sigma \in Gal(\Sigma_f(K(T_1, \ldots, T_n)) : K(T_1, \ldots, T_n))$, temos que

$$\sigma\left(\sum \frac{f_i(T_1, \ldots, T_n)}{g_i(T_1, \ldots, T_n)} t^i\right) = \left(\sum \frac{f_i(T_1, \ldots, T_n)}{g_i(T_1, \ldots, T_n)} \sigma(t)^i\right) = P_{t|K(T_1,\ldots,T_n)}(\sigma(t))$$

Logo, $\sigma(t)$ é um conjugado de t sobre $K(T_1, \ldots, T_n)$.

$(\Longleftarrow)$ Sendo $x_1, \ldots, x_n$ todos distintos e $t = T_1x_1 + \ldots T_nx_n$, afirmamos que, para todo $\tau \in S_n$, $\tau(t)$ são todos distintos. De fato, se existissem em S_n $\tau_1 \neq \tau_2$ tais que $\tau_1(t) = \tau_2(t)$, então o polinômio

$$p(X_1, \ldots, X_n) = X_1(\tau_1(x_1) - \tau_2(x_1)) + \ldots + X_n(\tau_1(x_n) - \tau_2(x_n))$$

seria não nulo em $K(x_1, \ldots, x_n)[X_1, \ldots, X_n]$ e anularia $T_1, \ldots, T_n$ o que contraria o fato de $T_1, \ldots, T_n$ serem algebricamente independentes sobre $K(x_1, \ldots, x_n)$.

Seja $\sigma \in S_n$. Se $\sigma(t)$ é um conjugado de t sobre $K(T_1, \ldots, T_n)$ então

$$P_{t|K(T_1,\ldots,T_n)} = P_{\sigma(t)|K(T_1,\ldots,T_n)}$$

ou seja, t e $\sigma(t)$ são raízes do $P_{t|K(T_1,\ldots,T_n)}$.

Além disso, no item (ii), mostramos que t é um elemento primitivo da extensão $K(x_1, \ldots, x_n, T_1, \ldots, T_n) : K(T_1, \ldots, T_n)$.

Dizer que $\tau \in Gal(K(T_1,\ldots,T_n)(t) : K(T_1,\ldots,T_n))$ significa que τ permuta as raízes de $P_{t|K(T_1,\ldots,T_n)}$. Como $\sigma(t)$ é uma raiz de $P_{t|K(T_1,\ldots,T_n)}$, temos que existe $\tau \in Gal(K(T_1,\ldots,T_n)(t) : K(T_1,\ldots,T_n))$ tal que $\tau(t) = \sigma(t)$. Mas

$$Gal(K(T_1,\ldots,T_n)(t) : K(T_1,\ldots,T_n)) = Gal(\Sigma_f(K(T_1,\ldots,T_n)) : K(T_1,\ldots,T_n))$$

Logo, existe $\tau \in Gal(\Sigma_f(K(T_1,\ldots,T_n)) : K(T_1,\ldots,T_n))$ tal que $\tau(t) = \sigma(t)$.

Como $\tau(t)$ são todos diferentes para toda permutação em S_n, temos que $\tau = \sigma$ e, assim, $\sigma \in Gal(\Sigma_f(K(T_1,\ldots,T_n)) : K(T_1,\ldots,T_n))$. ■

Introduzimos agora um outro automorfismo de $K(x_1,\ldots,x_n,T_1,\ldots,T_n)$. Denotaremos por σ_T a permutação do conjunto $\{T_1,\ldots,T_n\}$ dada por $\sigma_T(T_i) = T_{\sigma(i)}$. Como provamos em (3.2.12), $T_1,\ldots,T_n$ são algebricamente independentes sobre $K(x_1,\ldots,x_n)$, assim podemos estender naturalmente a permutação σ_T até um $K(x_1,\ldots,x_n)$-automorfismo de $K(x_1,\ldots,x_n,T_1,\ldots,T_n)$. Assim,

$$\sigma_T(T_i) = T_{\sigma(i)} \text{ e } \sigma_T(x_i) = x_i, \forall i, \text{ ou seja, } \sigma_T|_{K(x_1,\ldots,x_n)} = id_{K(x_1,\ldots,x_n)}$$

Notação 3.2.16. *Para os próximos resultados denotaremos por*

$$H(X) \in K(T_1,\ldots,T_n)[X]$$

o polinômio minimal de t sobre $K(T_1,\ldots,T_n)$*. Note que, afinal,*

$$H(X) = H(T_1,\ldots,T_n,X) \in K[T_1,\ldots,T_n,X]$$

Lema 3.2.17. *Nas mesmas condições do lema anterior, temos*
(i) $\sigma(t) = T_1x_{\sigma(1)} + \ldots + T_nx_{\sigma(n)}$ *é um conjugado de t sobre* $K(T_1,\ldots,T_n) \iff$ $\sigma_T(t) = T_{\sigma(1)}x_1 + \ldots + T_{\sigma(n)}x_n$ *é um conjugado de t sobre* $K(T_1,\ldots,T_n)$*;*
(ii) $\sigma_T(t)$ *é um conjugado de t sobre* $K(T_1,\ldots,T_n) \iff \sigma_T(H(T_1,\ldots,T_n,X)) =$ $H(T_1,\ldots,T_n,X)$*;*

Demonstração: (i) Como $Gal(\Sigma_f(K(T_1,\ldots,T_n)) : K(T_1,\ldots,T_n))$ é um grupo, pelo lema (3.2.15), temos que,

$$\sigma(t) \text{ é um conjugado de } t \text{ sobre } K(T_1,\ldots,T_n) \Longleftrightarrow$$
$$\sigma \in Gal(\Sigma_f(K(T_1,\ldots,T_n)) : K(T_1,\ldots,T_n)) \Longleftrightarrow$$
$$\sigma^{-1} \in Gal(\Sigma_f(K(T_1,\ldots,T_n)) : K(T_1,\ldots,T_n)) \Longleftrightarrow$$
$$\sigma^{-1}(t) \text{ é um conjugado de } t \text{ sobre } K(T_1,\ldots,T_n)$$

Por outro lado, temos que

$$\sigma^{-1}(t) = T_1\sigma^{-1}(x_1) + \ldots + T_n\sigma^{-1}(x_n) = T_1x_{\sigma^{-1}(1)} + \ldots + T_nx_{\sigma^{-1}(n)}$$
$$= T_{\sigma(\sigma^{-1}(1))}x_{\sigma^{-1}(1)} + \ldots + T_{\sigma(\sigma^{-1}(n))}x_{\sigma^{-1}(n)} =$$
$$\sigma_T(T_{\sigma^{-1}(1)}x_{\sigma^{-1}(1)} + \ldots + T_{\sigma^{-1}(n)}x_{\sigma^{-1}(n)}) = \sigma_T(t)$$

Portanto, $\sigma(t)$ é um conjugado de t sobre $K(T_1,\ldots,T_n) \Longleftrightarrow \sigma_T(t)$ é um conjugado de t sobre $K(T_1,\ldots,T_n)$.

(ii) Temos que $H(T_1,\ldots,T_n,X) = (X-t)H_1(T_1,\ldots,T_n,X)$, onde

$$(X-t), H_1(T_1,\ldots,T_n,X) \in K(T_1,\ldots,T_n,x_1,\ldots,x_n)[X]$$

Como σ_T é um $K(x_1,\ldots,x_n)$-automorfismo de $K(x_1,\ldots,x_n,T_1,\ldots,T_n)$, temos que

$$\sigma_T(H(T_1,\ldots,T_n,X)) = (X-\sigma_T(t))\sigma_T(H_1(T_1,\ldots,T_n,X))$$

$(\Longleftarrow)$ Se $H(T_1,\ldots,T_n,X) = \sigma_T(H(T_1,\ldots,T_n,X))$ então $\sigma_T(t)$ é também uma raiz de
$H(T_1,\ldots,T_n,X)$, ou seja, $\sigma_T(t)$ é um conjugado de t sobre $K(T_1,\ldots,T_n)$.

$(\Longrightarrow)$ Se $\sigma_T(t)$ é um conjugado de t sobre $K(T_1,\ldots,T_n)$ então $\sigma_T(t)$ é também uma raiz de $H(T_1,\ldots,T_n,X)$. Se $\sigma_T = id$ então é claro que $\sigma_T(H) = H$. Se $\sigma_T \neq id$ então podemos escrever

$$H(T_1,\ldots,T_n,X) = (X-t)(X-\sigma_T(t))H_2(T_1,\ldots,T_n,X)$$
$$\Longrightarrow \sigma_T(H(T_1,\ldots,T_n,X)) = (X-\sigma_T(t))(X-\sigma_T(\sigma_T(t)))\sigma_T(H_2(T_1,\ldots,T_n,X))$$

ou seja, os polinômios $\sigma_T(H(T_1,\ldots,T_n,X))$ e $H(T_1,\ldots,T_n,X)$ têm $\sigma_T(t)$ como raiz comum.

Sendo σ_T um automorfismo de $K(x_1,\ldots,x_n,T_1,\ldots,T_n) : K(x_1,\ldots,x_n)$, temos que $\sigma_T|_{K(T_1,\ldots,T_n)}$ continua sendo um K-automorfismo.

Assim, como $H(T_1,\ldots,T_n,X)$ é mônico e irredutível em $K(T_1,\ldots,T_n)[X]$ temos que $\sigma_T(H(T_1,\ldots,T_n,X))$ também é mônico e irredutível.

Portanto, ambos são polinômios minimais de $\sigma_T(t)$ em $K(T_1,\ldots,T_n)[X]$. Então, $H(T_1,\ldots,T_n,X) = \sigma_T(H(T_1,\ldots,T_n,X))$. ■

Agora, temos todos os requisitos para provarmos o teorema (3.2.13), mediante a redução que f tem todas as raízes distintas.

Demonstração: (i) Pelo lema (3.2.15), temos que $Gal(\Sigma_f(K) : K) = \{\sigma \in S_n; \sigma(t)$ é um conjugado de t sobre $K(T_1,\ldots,T_n)\}$, onde $t = T_1x_1 + \ldots + T_nx_n$.

Portanto, $Gal(\Sigma_f(K) : K) = \{\sigma \in S_n; T_1\sigma(x_1) + \ldots + T_n\sigma(x_n)$ é um conjugado de t sobre $K(T_1,\ldots,T_n)\}$.

(ii) Defina

$$G(T_1,\ldots,T_n,X,x_1,\ldots,x_n) := \prod_{\tau\in S_n}(X-\tau_T(t)) \tag{3.12}$$

pertencente a $K[T_1,\ldots,T_n,X][x_1,\ldots,x_n]$.

Logo, $H(T_1,\ldots,T_n,X)$ é um fator de $G(T_1,\ldots,T_n,X,x_1,\ldots,x_n)$.

Notemos que $G(T_1,\ldots,T_n,X,x_1,\ldots,x_n)$ é simétrico nos x_i. De fato, seja $\tau \in S_n$, então

$$\tau(G) = \prod_{\sigma\in S_n}(X-\tau(\sigma_T(t))) = \prod_{\varsigma\in S_n}(X-\varsigma_T(t)) = G$$

Logo, por (3.2.9), temos que $G(T_1, \ldots, T_n, X, x_1, \ldots, x_n)$ pode ser efetivamente calculado e $G(T_1, \ldots, T_n, X, x_1, \ldots, x_n) \in K[T_1, \ldots, T_n, X]$.

Como a fatoração em $K[X]$ é efetiva, por (3.1.9), a fatoração em $K[T_1, \ldots, T_n, X]$ é também efetiva.

Logo, $G(T_1, \ldots, T_n, X, x_1, \ldots, x_n)$ se fatora em irredutíveis de forma efetiva em $K[T_1, \ldots, T_n, X]$, digamos

$$G = G(T_1, \ldots, T_n, X, x_1, \ldots, x_n) = G_1 \ldots G_r$$

com $G_1, \ldots, G_r \in K[T_1, \ldots, T_n, X]$. Em particular, $H(T_1, \ldots, T_n, X)$ é então um destes fatores.

Afirmação: As permutações σ_T que deixam qualquer dos fatores, digamos G_1, invariante, formam um grupo com a composição e que denotaremos por $\mathcal{G}$.

De fato, se $\sigma_T \in \mathcal{G}$, temos que

$$G_1 = {\sigma_T}^{-1}\sigma_T(G_1) = {\sigma_T}^{-1}(G_1)$$

o que implica que ${\sigma_T}^{-1} \in \mathcal{G}$.

Além disso, pelos lemas (3.2.15) e (3.2.17), temos

$$\begin{aligned} Gal(\Sigma_f(K) : K) &\overset{(3.2.15)}{=} Gal(\Sigma_f(K(T_1, \ldots, T_n)) : K(T_1, \ldots, T_n)) \\ &\overset{(3.2.15)}{=} \{\sigma \in S_n | \sigma(t) \text{ é um conjugado de } t \text{ sobre} K(T_1, \ldots, T_n)\} \\ &\overset{(3.2.17)}{=} \{\sigma \in S_n | \sigma_T(t) \text{ é um conjugado de } t \text{ sobre} K(T_1, \ldots, T_n)\} \\ &\overset{(3.2.17)}{=} \{\sigma \in S_n | \sigma_T(H(T_1, \ldots, T_n, X)) = H(T_1, \ldots, T_n, X)\} \end{aligned}$$

Logo, para cada G_i, $i = 1, \ldots, r$, consideremos σ_T tais que $\sigma_T(G_i) = G_i$. E como $H(T_1, \ldots, T_n, X)$ é um dos fatores irredutíveis G_i de G, temos que $Gal(\Sigma_f(K) : K)$ é um dos conjuntos formado pelos σ_T que deixam algum fator irredutível de G fixo, mas aplicadas aos x_i ao invés dos T_i.

Pela forma que definimos G, temos que cada G_i é o polinômio minimal de algum $\sigma_T(t) = T_{\sigma(1)}x_1 + \ldots + T_{\sigma(n)}x_n$ sobre $K(T_1, \ldots, T_n)$. Seja G_j, para algum $j = 1, \ldots, r$, tal que G_j é o polinômio minimal de $\bar{t} = \sigma_T(t)$, para algum σ_T. Então se considerarmos $\bar{t}$ nos lemas (3.2.15) e (3.2.17), teremos que para todo σ_T tal que $\sigma_T(G_j) = G_j$, então $\sigma \in Gal(\Sigma_f(K) : K)$.

Agora, suponhamos que G_1 é o polinômio minimal de t sobre $K(T_1, \ldots, T_n)$. Logo, pelos lemas (3.2.15) e (3.2.17), temos que $\sigma_T(G_1) = G_1$.

Por outro lado, se existir algum $\tau \in S_n$ tal que $\tau_T(G_1) = G_1$, novamente pelos lemas (3.2.15) e (3.2.17), temos que $\tau \in Gal(\Sigma_f(K) : K)$. E assim, considerando $\bar{t}$ nos lemas (3.2.15) e (3.2.17), teremos que $\tau_T(G_j) = G_j$.

Portanto,

$$Gal(\Sigma_f(K) : K) = \{\sigma \in S_n | \sigma_T(H(T_1, \ldots, T_n, X)) = H(T_1, \ldots, T_n, X)\}$$

$$= \{\sigma \in S_n; \sigma_T(G_i) = G_i, \forall i = 1, \ldots, r\}$$

e note que com esta última caracterização, elimanou-se o desconhecido $H(T_1, \ldots, T_n, X)$.

Com isso, é possível reconhecer se $T_1\sigma(x_1) + \ldots + T_n\sigma(x_n)$ é ou não um conjugado de t sobre $K(T_1, \ldots, T_n)$, já que por (3.2.17)

$$\sigma_T(H(T_1, \ldots, T_n, X)) = H(T_1, \ldots, T_n, X)$$

se, e somente se, $\sigma(t)$ é um conjugado de t sobre $K(T_1, \ldots, T_n)$. ■

Então, no nosso "algoritmo", não precisamos falar de $H(T_1, \ldots, T_n, X)$.

Resumindo: Seja K um corpo tal que em $K[X]$ a fatoração é efetiva (por exemplo, $K = \mathbb{Q}$) e seja $f(X) \in K[X]$ separável sobre K e com todas as raízes distintas. Para determinar $Gal(\Sigma_f(K) : K)$ fazemos:

1º passo: Denotando por $x_1, \ldots, x_n$ todas as raízes de $f(X)$ (desconhecidas, em

geral) e $T_1, \ldots, T_n$ indeterminadas, definimos

$$t = T_1x_1 + \ldots + T_nx_n$$

e

$$G(T_1, \ldots, T_n, X, x_1, \ldots, x_n) := \prod_{\tau \in S_n} (X - \tau_T(t))$$

que pertence a $K[T_1, \ldots, T_n, X][x_1, \ldots, x_n]$ e que é simétrico nos x_i.

2º passo: Pelo Teorema (3.2.9), temos que $G(T_1, \ldots, T_n, X, Y_1, \ldots, Y_n)$ pode ser efetivamente calculado e quando avaliamos $Y_i = x_i, i \in \{1, \ldots, n\}$ torna-se um elemento de $K[T_1, \ldots, T_n, X]$ (expressões nos x_i sendo substituidos pelos coeficientes de $f(X)$, que são elementos de K).

3º passo: Fatoramos completamente $G(T_1, \ldots, T_n, X, x_1, \ldots, x_n)$ em $K[T_1, \ldots, T_n, X]$ (o que pode ser feito pois a fatoração em $K[T_1, \ldots, T_n, X]$ é efetiva), digamos

$$G = G(T_1, \ldots, T_n, X, x_1, \ldots, x_n) = G_1 \ldots G_r$$

4º passo: Determinamos todos os $\sigma \in S_n$ que satisfazem $\sigma_T(G_i) = G_i$, $\forall i \in \{1, \ldots, r\}$, isto é, $G_i(T_{\sigma(1)}, \ldots, T_{\sigma(n)}, X, x_1, \ldots, x_n) = G_i(T_1, \ldots, T_n, X, x_1, \ldots, x_n)$.

5º passo: $Gal(\Sigma_f(K) : K) = \{\sigma \in S_n; \sigma(G_i) = G_i, \forall i = 1, \ldots, r\}$

Este método não é tanto de interesse prático, como bem afirmou Van Der Waerden em ([9]). De fato, se consideremos, por exemplo, o polinômio $f(X) = X^2 - 1 \in \mathbb{Q}[X]$ cujas raízes vamos denotar por x_1, x_2[‡], indeterminadas T_1, T_2 algebricamente

[‡]Obviamente para este polinômio não só conhecemos suas raízes como sabemos determinar com outros métodos $Gal(\Sigma_f(\mathbb{Q}) : \mathbb{Q})$. O que queremos aqui é ilustrar a não praticidade deste método, mesmo neste caso simples. Sobre $f(X)$ vamos utilizar somente o fato de suas raízes serem diferentes, o que pode ser detectado pela condição $mdc(f, f') = 1$ sendo f' a derivada formal de f.

independentes sobre $\mathbb{Q}$ e definamos

$$t = T_1x_1 + T_2x_2$$

Sejam Y_1, Y_2 indeterminadas algebricamente independentes sobre $\mathbb{Q}$ e defina

$$G = G(T_1, T_2, X, Y_1, Y_2) =$$

$$X^2 - XT_1Y_1 - XT_1Y_2 - XT_2Y_1 - XT_2Y_2 + {T_1}^2Y_1Y_2 + T_1T_2{Y_1}^2 + T_1T_2{Y_2}^2 + {T_2}^2Y_1Y_2$$

que pertence a $\mathbb{Q}[T_1, T_2, X][Y_1, Y_2]$ e é simétrico nos Y_i. Fazendo uso do método explicitado no Teorema (3.2.7), devemos agora expressar G em função dos polinômios simétricos elementares de Y_1, Y_2.

Escrevendo G como um polinômio em Y_2, temos

$$G = T_1T_2{Y_2}^2 + ({T_1}^2Y_1 - XT_1 - XT_2 + {T_2}^2Y_1)Y_2 + \underbrace{(X^2 - XT_1Y_1 - XT_2Y_1 + T_1T_2{Y_1}^2)}_{\phi(Y_1)=\phi(S_1)}$$

sendo S_1 o polinômio simétrico elementar de Y_1, isto é, $S_1 = Y_1$. Agora, considerando S_1 como o polinômio simétrico em Y_1 e Y_2, temos que $G - \phi(S_1)$ é divisível por $S_2 = Y_1Y_2$. De fato,

$$G - \phi(S_1) = G - X^2 + XT_1Y_1 + XT_1Y_2 + XT_2Y_1 + XT_2Y_2 - T_1T_2{Y_1}^2 - T_1T_2{Y_2}^2 - 2T_1T_2Y_1Y_2$$

$$G - \phi(S_1) = {T_1}^2Y_1Y_2 - 2T_1T_2Y_1Y_2 + {T_2}^2Y_1Y_2 =$$

$$Y_1Y_2(T_1 - T_2)^2 = S_2(T_1 - T_2)^2$$

de modo que,

$$G = X^2 - XT_1S_1 - XT_2S_1 + T_1T_2{S_1}^2 + S_2(T_1 - T_2)^2$$

Agora, pelo algoritmo do Teorema (3.2.9), temos que avaliando $Y_1 = x_1$ e $Y_2 = x_2$ e fazendo uso das relações de Viète, vistas no lema (3.2.6), temos que $S_1 = 0$ e $S_2 = -1$

$$G(T_1, T_2, X, x_1, x_2) = X^2 - (T_1 - T_2)^2 \in \mathbb{Q}[T_1, T_2, X] \tag{3.13}$$

O objetivo, agora, é encontrar a fatoração em fatores irredutíveis de $G(T_1, T_2, X, x_1, x_2)$ em $\mathbb{Q}[T_1, T_2, X]$(onde a fatoração é efetiva).

Então, pelo algoritmo do Teorema (3.1.9), tomando $m = 3$ o valor mais econômico satisfazendo $m > \partial G(T_1, T_2, X, x_1, x_2)$ e substituindo

$$X \longmapsto Z$$

$$T_1 \longmapsto Z^3$$

$$T_2 \longmapsto Z^9$$

escrevemos $G(T_1, T_2, X, x_1, x_2)$ como um polinômio em $\mathbb{Q}[Z]$:

$$G(T_1, T_2, X, x_1, x_2) = G(Z) = Z^2 - (Z^3 - Z^9)^2$$

$$= Z^2 - [Z^3(1 - Z^6)]^2 = Z^2 - Z^6(1 - Z^6)^2$$

$$= Z^2[1 - Z^4(1 - Z^6)^2] = Z^2[1 - Z^2(1 - Z^6)][1 + Z^2(1 - Z^6)]$$

Agora, devemos aplicar o algoritmo obtido pelo Teorema (3.1.6) para podermos fatorar $G(Z)$.

Seja $g(Z) = 1 - Z^2 + Z^8$; considerando 8 inteiros distintos, digamos

$$a_1 = -4$$

$$a_2 = -3$$

$$a_3 = -1$$

$$a_4 = 0$$

$$a_5 = 1$$

$$a_6 = 2$$

$$a_7 = 3$$

$$a_8 = 4$$

e definimos os seguintes conjuntos

$$D_1 = \{a \in \mathbb{Z}; a \text{ é um divisor de } g(a_1)\} = \{\pm 1, \pm 65521\}$$
$$D_2 = \{a \in \mathbb{Z}; a \text{ é um divisor de } g(a_2)\} = \{\pm 1, \pm 6553\}$$
$$D_3 = \{a \in \mathbb{Z}; a \text{ é um divisor de } g(a_3)\} = \{\pm 1\}$$
$$D_4 = \{a \in \mathbb{Z}; a \text{ é um divisor de } g(a_4)\} = \{\pm 1\}$$
$$D_5 = \{a \in \mathbb{Z}; a \text{ é um divisor de } g(a_5)\} = \{\pm 1\}$$
$$D_6 = \{a \in \mathbb{Z}; a \text{ é um divisor de } g(a_6)\} = \{\pm 1, \pm 11, \pm 23, \pm 253\}$$
$$D_7 = \{a \in \mathbb{Z}; a \text{ é um divisor de } g(a_7)\} = \{\pm 1, \pm 6553\}$$
$$D_8 = \{a \in \mathbb{Z}; a \text{ é um divisor de } g(a_8)\} = \{\pm 1, \pm 65521\}$$

E com isso, a fórmula geral para o polinômio interpolador de Lagrange $M_{\alpha_1,\ldots,\alpha_8}(Z)$ com $M_{\alpha_1,\ldots,\alpha_8}(a_i) = \alpha_i$ para $i \in \{1, \ldots, 8\}$ e $(\alpha_1, \ldots, \alpha_8) \in D_1 \times \ldots \times D_8$ é a seguinte:

$$\begin{aligned}
M_{\alpha_1,\ldots,\alpha_8}(Z) = {} & \frac{-\alpha_1}{20160} Z(Z+3)(Z+1)(Z-1)(Z-2)(Z-3)(Z-4) \\
& + \frac{\alpha_2}{5040} Z(Z+4)(Z+1)(Z-1)(Z-2)(Z-3)(Z-4) \\
& + \frac{-\alpha_3}{720} Z(Z+4)(Z+3)(Z-1)(Z-2)(Z-3)(Z-4) \\
& + \frac{\alpha_4}{288} (Z+4)(Z+3)(Z+1)(Z-1)(Z-2)(Z-3)(Z-4) \\
& + \frac{-\alpha_5}{240} Z(Z+4)(Z+3)(Z+1)(Z-2)(Z-3)(Z-4) \\
& + \frac{\alpha_6}{360} Z(Z+4)(Z+3)(Z+1)(Z-1)(Z-3)(Z-4) \\
& + \frac{-\alpha_7}{1008} Z(Z+4)(Z+3)(Z+1)(Z-1)(Z-2)(Z-4) \\
& + \frac{\alpha_8}{6720} Z(Z+4)(Z+3)(Z+1)(Z-1)(Z-2)(Z-3)
\end{aligned}$$

Salientamos que, então, um polinômio de grau apenas igual a dois nos faz agora trabalhar em um polinômio de grau 8: a partir daqui, para cada $(\alpha_1, \ldots, \alpha_8)$ escolhido em $D_1 \times \ldots \times D_8$ teríamos que testar se $M_{\alpha_1,\ldots,\alpha_8}(Z)$ é ou não um divisor de $g(Z) = 1 - Z^2 + Z^8$ e repetir todo o processo acima para o polinômio $h(Z) = 1 + Z^2 - Z^8$ para só então olharmos às três indeterminadas e ainda testar se alguma das fatorações encontradas de $g(Z)$ e de $h(Z)$ servem para a fatoração

de $G(T_1, T_2, X, x_1, x_2)$ dado em (3.13). Esperamos com isto, ter convencido o leitor sobre o não interesse prático deste método.

Capítulo 4

Apêndices

.1 Apêndice A: Sobre as Raízes da Unidade em K

Começamos com algumas definições e notações. Considere K um corpo e $K^* = K \setminus \{0\}$ o seu grupo multiplicativo. Denote por $\mathcal{R}_n$ o conjunto de todas as raízes do polinômio $X^n - 1$. Para cada $n \geq 1$ denotaremos por

$$W_n(K) = \{a \in K^*; a^n = 1\} = \{a \in K^*; o(a)|n\} \subseteq K^*$$

que será chamado o grupo das raízes n-ésimas da unidade em K. Portanto, temos que

$$W_n(K) = \mathcal{R}_n \cap K$$

Em particular,

$$|W_n(K)| \leq n. \tag{1}$$

Teorema .1.1. *Seja V um subgrupo de K^* tal que $exp(V) = m < \infty$. Então $V = W_m(K)$ e V é cíclico de ordem m.*

Demonstração: Para todo $v \in V$, $o(v)$ divide $exp(V) = m$, logo $v^m = 1$, ou seja, $v \in W_m(K)$.

Assim, $V \subseteq W_m(K)$ e, portanto,

$$|V| \leq |W_m(K)| \leq m \tag{2}$$

Por outro lado, $m = exp(V)$ divide $|V|$. Consequentemente, $|V| = m$ e, então, por (2) concluímos que $|W_m(K)| = m$. Como $V \subseteq W_m(K)$, concluímos:

$$V = W_m(K)$$

Então, como $exp(V) = m = |V|$, pelo lema (1.1.10) item (ii), V é cíclico. ■

Corolário .1.2. *Seja V um subgrupo finito de K^*, digamos $|V| = m$. Então, $V = W_m(K)$ e V é cíclico.*

Demonstração: Do fato que $|V| = m < \infty$ resulta que $exp(V) = l < \infty$ e, assim, $exp(V)$ divide m.

Do teorema (.1.1), temos que $V = W_l(K)$ e V é cíclico de ordem l.

Por hipótese, $|V| = m$. Logo, $m = l$.

Assim, $V = W_m(K)$ e V é cíclico. ■

Corolário .1.3. *Para todo $n \geq 1$, $exp(W_n(K)) = |W_n(K)|$ divide n.*

Demonstração: Já sabemos por (1) que $|W_n(K)| \leq n$; em particular $W_n(K)$ é finito, logo temos também $exp(W_n(K))$ finito, digamos $exp(W_n(K)) = l$. Então, pelo lema (1.1.10) item (i), existe $y \in W_n(K)$ tal que $exp(W_n(K)) = o(y)$.

Como $y \in W_n(K)$, $y^n = 1$, ou seja, $exp(W_n(K)) = o(y)$ divide n.

Mostremos agora que $exp(W_n(K)) = |W_n(K)|$.

Como $exp(W_n(K)) = l < \infty$ e y é tal que $o(y) = l$, podemos aplicar o teorema

(.1.1) e concluir que $W_l(K) = W_n(K)$. Ainda, $W_n(K)$ é cíclico de ordem l. Então, $exp(W_n(K)) = l = |W_n(K)|$. ■

Ao considerarmos o grupo $W_n(K)$, é natural pensarmos no subconjunto de todas as raízes n-ésimas primitivas da unidade pertencentes a K, o qual será denotado por $\mathcal{P}_n(K)$. Assim,

$$\mathcal{P}_n(K) = \{ \text{ raízes } n\text{-ésimas primitivas da unidade em } K\} = \{a \in K^*; o(a) = n\}$$

enquanto

$$\mathcal{R}_n = \{ \text{ raízes } n\text{-ésimas da unidade}\}$$
$$W_n(K) = \{ \text{ raízes } n\text{-ésimas da unidade em } K\}$$

Proposição .1.4. *Para todo $n \geq 1$, as seguintes condições são equivalentes:*
(i) $|W_n(K)| = n$;
(ii) $\mathcal{P}_n(K)$ é não-vazio;
(iii) $car(K)$ não divide n e $X^n - 1$ fatora-se em $K[X]$ em polinômios lineares.
No caso em que elas se verificam, temos que $W_n(K) = \langle z \rangle$ se, e somente se, $z \in \mathcal{P}_n(K)$ e $\mathcal{P}_d(K)$ é não vazio para todo divisor d de n. Além disso,

$$W_n(K) = \bigcup_{d|n} \mathcal{P}_d(K)$$

Demonstração: Vamos denotar $car(K) = p$, sendo p igual a zero ou a um número primo.

$(i) \Rightarrow (ii)$
Do corolário (.1.2), temos que $W_n(K)$ é cíclico. Assim,

$$W_n(K) = \langle z \rangle \Leftrightarrow o(z) = n$$

E isso nos mostra que $z \in \mathcal{P}_n(K)$. Portanto, $\mathcal{P}_n(K)$ é não-vazio.

$(ii) \Rightarrow (iii)$ Seja $z \in \mathcal{P}_n(K)$.

Se p fosse um divisor de n, então teríamos que $p \neq 0$ e

$$(z^{\frac{n}{p}})^p = z^n = 1$$

Afirmação: Nestas condições, devemos ter $z^{\frac{n}{p}} = 1$.

De fato, como em $\mathbb{Z}_p$ todos os elementos são raízes p-ésimas da unidade e a quantidade de elementos em $\mathbb{Z}_p$ é a mesma quantidade de raízes do polinômio $X^p - 1$, quando pensamos na extensão $K : \mathbb{Z}_p$ não estamos acrescentando mais nenhuma raiz p-ésima da unidade. Assim, $z^{\frac{n}{p}} \in \mathbb{Z}_p$, pois é uma raiz p-ésima da unidade. Ainda, pode-se aplicar o teorema de Fermat para $z^{\frac{n}{p}}$ o qual garante que

$$(z^{\frac{n}{p}})^p \equiv z^{\frac{n}{p}} \pmod{p}$$

Mas como $(z^{\frac{n}{p}})^p = 1$, temos que $z^{\frac{n}{p}} \equiv 1 \pmod{p}$. Ou seja, $z^{\frac{n}{p}} = 1$.

Porém, isso é um absurdo, pois $o(z) = n$ e $\frac{n}{p} < n$. Portanto, p não divide n. Falta mostrar que $X^n - 1$ fatora-se em $K[X]$ em polinômios lineares.

Os elementos $1, z, z^2, \ldots, z^{n-1} \in K$ são distintos dois a dois, uma vez que $z \neq 1 (o(z) = n)$, e são raízes do polinômio $X^n - 1$, portanto

$$X^n - 1 = \prod_{j=0}^{n-1} (X - z^j)$$

o que nos mostra que o polinômio em questão se fatora em polinômios lineares em $K[X]$.

$(iii) \Rightarrow (i)$ Note que o polinômio $X^n - 1$ é separável, pois $X^n - 1$ e sua derivada nX^{n-1} ($\neq 0$, pois p não divide n) são primos entre si.

Por hipótese, $X^n - 1$ fatora-se em $K[X]$ em fatores lineares, digamos que

$$X^n - 1 = (X - y_1) \ldots (X - y_n)$$

Por separabilidade, os elementos $y_1, \ldots, y_n$ são distintos dois a dois. Logo, $W_n(K) = \{y_1, \ldots, y_n\}$, ou seja, consiste de exatamente n elementos.

Para provar as observações finais, vamos supor que tais condições equivalentes se verificam. Neste caso,

- $W_n(K) = \langle z \rangle$ se, e somente se, $z \in \mathcal{P}_n(K)$

De fato, se $z \in \mathcal{P}_n(K)$ então $o(z) = n$. Então $W_n(K)$, que tem n elementos, é gerado por z. Reciprocamente, se $W_n(K) = \langle z \rangle$ pela demonstração do item $(i) \Rightarrow (ii)$ temos que $o(z) = n$, logo $z \in \mathcal{P}_n(K)$.

Vamos mostrar, agora, que $\mathcal{P}_d(K)$ é não vazio para todo divisor d de n.

Segue da teoria de grupos que se $o(z) = n$ e $d|n$, então $o(z^{\frac{n}{d}}) = d$ e, consequentemente, $z^{\frac{n}{d}}$ é uma raiz d-ésima primitiva da unidade. Logo, $z \in \mathcal{P}_n(K)$ implica $z^{\frac{n}{d}} \in \mathcal{P}_d(K)$

Por fim, vamos verificar que

$$W_n(K) = \bigcup_{d|n} \mathcal{P}_d(K)$$

Seja $a \in W_n(K)$. Então, $a^n = 1$, o que implica que $o(a) = d$ divide n. Portanto, $a \in \mathcal{P}_d(K)$ com $d|n$. Por outro lado, seja $a \in \bigcup_{d|n} \mathcal{P}_d(K)$, então existe um d' divisor de n tal que $a \in P_{d'}(K)$. Assim, $o(a) = d'$ a qual divide n, ou seja, $a \in W_n(K)$. ■

Note que qualquer corpo algebricamente fechado tal que sua característica não divida n satisfaz as condições equivalentes de (.1.4), em particular o corpo $\mathbb{C}$ satisfaz as condições equivalentes de (.1.4).

Segue abaixo um caso particular dessa proposição para um corpo algebricamente fechado.

Corolário .1.5. *Seja Ω um corpo algebricamente fechado. Para todo $n \geq 1$ as seguintes condições são equivalentes:*

(i) $|W_n(\Omega)| = n$ *e é cíclico;*

(ii) $\mathcal{P}_n(\Omega)$ *é não-vazio;*

(iii) $X^n - 1$ *é separável e se fatora em fatores lineares em* $\Omega[X]$*;*

(iv) $car(\Omega)$ *não divide* n*.*

E $W_n(\Omega) = \bigcup_{d|n} \mathcal{P}_d(\Omega)$.

Da teoria de grupos sabemos que os geradores do grupo aditivo $\mathbb{Z}_n$ são exatamente os elementos do grupo multiplicativo $\mathcal{U}_{\mathbb{Z}_n}$ que consiste dos elementos invertíveis do anel $\mathbb{Z}_n$, ou seja, são as classes $\overline{l} = l + (n)$ tais que $l \in \mathbb{Z}$ e $mdc(l, n) = 1$. Além disso, temos que se $z \in \mathcal{P}_n(K)$ então

$$\mathcal{P}_n(K) = \{z^l; 1 \leq l \leq n; mdc(l, n) = 1\}$$

Isso decorre do fato de que se $|W_n(K)| = n$ então para qualquer $z \in \mathcal{P}_n(K)$ existe um isomorfismo do grupo $(\mathbb{Z}_n, +)$ sobre $(W_n(K), \bullet)$, dado por

$$\begin{aligned} \phi : (\mathbb{Z}_n, +) &\longrightarrow (W_n(K), \cdot) \\ \overline{j} &\longmapsto z^j \end{aligned}$$

Assim, temos que o isomorfismo ϕ induz uma aplicação bijetiva entre $\mathcal{U}_{\mathbb{Z}_n}$ e $\mathcal{P}_n(K)$. Então devido à essa bijeção, concluimos que, se $z \in \mathcal{P}_n(K)$ então

$$\mathcal{P}_n(K) = \{z^l; 1 \leq l \leq n; mdc(l, n) = 1\}$$

Em particular, a ordem de $\mathcal{P}_n(K)$ é dada por $\varphi(n)$ onde φ é a função de Euler, cujas propriedades passamos a registrar.

Proposição .1.6. (Propriedades da Função φ de Euler)

As seguintes afirmações são válidas:

(i) $\varphi(p^r) = p^{r-1}(p-1)$*, para todo primo* p *e todo* $r \geq 1$*;*

(ii) Para quaisquer $m, n \geq 1$, com $mdc(m,n) = 1$ temos $\varphi(mn) = \varphi(m)\varphi(n)$;

(iii) Para todo $n \geq 1$ temos que

$$\varphi(n) = n\prod_{p|n}(1 - \frac{1}{p})$$

Demonstração: Relembramos, aqui, apenas a prova de *(iii)*. As demais podem ser encontradas em [2].

(iii) Seja $n = {p_1}^{r_1} \dots {p_s}^{r_s}$ a fatoração de n. Generalizando o item anterior para os s números ${p_1}^{r_1} \dots {p_s}^{r_s}$ que são primos entre si, obtemos que

$$\begin{aligned}\varphi(n) = \varphi({p_1}^{r_1}) \dots \varphi({p_s}^{r_s}) &\overset{\text{(i)}}{=} \prod_{j=1}^{s} {p_j}^{r_j - 1}(p_j - 1) \\ &= \prod_{j=1}^{s} {p_j}^{r_j}(1 - \frac{1}{p_j}) = n\prod_{p|n}(1 - \frac{1}{p})\end{aligned}$$

■

Proposição .1.7. *Seja G um grupo cíclico de ordem $n < \infty$. Então:*

(i) Para todo $l \in \mathbb{Z}$ tal que $mdc(l,n) = 1$ a aplicação

$$\begin{aligned}\tilde{l} : G &\longrightarrow G \\ a &\longmapsto a^l\end{aligned}$$

é um automorfismo de G;

(ii) A aplicação que a cada $l \in \mathbb{Z}$ com $mdc(l,n) = 1$ associa $\tilde{l}$ induz um isomorfismo de $\mathcal{U}_{\mathbb{Z}_n}$ sobre $Aut(G)$:

$$\begin{aligned}\phi : \mathcal{U}_{\mathbb{Z}_n} &\longrightarrow Aut(G) \\ \bar{l} &\longmapsto \tilde{l}\end{aligned}$$

Demonstração: *(i)* Como $mdc(l,n) = 1$, existem $k, m \in \mathbb{Z}$ tais que $kl + mn = 1$. Logo, $mdc(k,n) = 1$ e para todo $a \in G$

$$(\tilde{k} \circ \tilde{l})(a) = \tilde{k}(a^l) = a^{lk} = a^{1-mn} = a\underbrace{(a^{mn})^{-1}}_{=1} = a$$

De modo análogo, $(\tilde{l} \circ \tilde{k})(a) = a$ Então, $\tilde{k} \circ \tilde{l} = \tilde{l} \circ \tilde{k} = id_G$, ou seja, $\tilde{l}$ é uma bijeção. Além disso, como todo grupo cíclico é abeliano,

$$\tilde{l}(ab) = (ab)^l = a^l b^l = \tilde{l}(a)\tilde{l}(b)$$

Portanto, $\tilde{l}$ é um automorfismo de G.

(ii) Temos que mostrar que ϕ é um isomorfismo.

- ϕ está bem definida e é injetora

  Para isso, vamos mostrar a seguinte equivalência: $\tilde{l} = \tilde{l'}$ se, e somente se, $l \equiv l' \pmod{n}$.

  Como G é cíclico, suponhamos que $G = \langle g \rangle$, para algum $g \in G$. Então

$$\tilde{l} = \tilde{l'} \iff \tilde{l}(g) = \tilde{l'}(g) \iff g^l = g^{l'}$$
$$\iff g^{l-l'} = 1 \iff o(g)|l - l' \iff n|l - l' \iff l \equiv l' \pmod{n}$$

- ϕ é um homomorfismo

  Como para cada $a \in G$, $\widetilde{xy}(a) = a^{xy} = a^{yx} = (a^y)^x = \tilde{x}(a^y) = \tilde{x}(\tilde{y}(a))$, concluímos

$$\phi(\overline{xy}) = \widetilde{xy} = \tilde{x}\tilde{y} = \phi(x)\phi(y)$$

- ϕ é sobrejetora

  Supondo que $G = \langle g \rangle$, temos para todo $w \in Aut(G)$,

$$w(g) = g^l, \text{ para algum } l \in \{1, \ldots, n-1\}$$

  e como w é um automorfismo $w(g^j) = g^{jl}$, para todo $j \in \{0, \ldots, n-1\}$. Logo, se mostrarmos que $mdc(l, n) = 1$ então teremos $w = \tilde{l}$. De fato, sendo w um

automorfismo de G, temos que $g^l = w(g)$ é também um gerador de G, de modo que $g^{lj} = (g^l)^j \neq 1$ enquanto $j \in \{1, \ldots, n-1\}$. Então, se $mdc(l,n) = c \neq 1$ segue que $c|l$ e $c|n$, ou seja, $l = cq$, para algum $q \in \mathbb{Z}$, e $n = ck$, para algum $k \in \{1, \ldots, n-1\}$.

Então, $g^{jl} = g^{jcq}$. Mas como $j, k \in \{1, \ldots, n-1\}$, quando j for igual a k teremos

$$g^{jl} = g^{jcq} = g^{kcq} = g^{nq} = 1$$

o que é um absurdo. Portanto, $mdc(l,n) = 1$, o que implica que $w = \tilde{l}$, ou seja, a aplicação ϕ é sobrejetora. ■

Agora, aplicando a proposição (.1.7) ao grupo $W_n(K)$ obtemos o seguinte resultado:

Corolário .1.8. *Seja K um corpo tal que $\mathcal{P}_n(K) \neq \emptyset$. Então, a aplicação definida por $\bar{l} \longmapsto \tilde{l}$ $(l \in \mathbb{Z}; mdc(l,n) = 1)$ induz um isomorfismo* de $\mathcal{U}_{\mathbb{Z}_n}$ sobre $Aut(W_n(K))$.*

.2 Apêndice B: Construções com Régua e Compasso

O objetivo desta seção é evidenciar as relações que ocorrem entre as construções geométricas e as extensões de corpos. Para tal, vamos efetuar tais construções no plano complexo $\mathbb{C}$, partindo de um conjunto $\mathcal{M} \subseteq \mathbb{C}$, chamado conjunto de pontos iniciais sempre supondo que $\{0,1\} \subseteq \mathcal{M}$[†].

*Induz vários, dependendo do gerador que escolhermos para $W_n(K)$ (ou G, em (.1.7)).

†Normalmente, o conjunto de pontos iniciais é tomado como sendo apenas o conjunto $\{0,1\}$ ou então um conjunto de três pontos como $\{0,1,z_0\} \subseteq \mathbb{C}$, mas no nosso estudo essas considerações não são muito relevantes por isso apenas suporemos que $\{0,1\} \subseteq \mathcal{M}$, ou seja, não faremos nenhuma restrição quanto à cardinalidade de $\mathcal{M}$.

A construção com régua e compasso é regida por duas "regras":

1) Pode-se traçar apenas uma reta que liga quaisquer dois pontos já construídos;

2) Pode-se traçar apenas um círculo de centro em um ponto já construído passando por outro ponto já construído.

Definição .2.1. *Denotaremos por* $\Gamma(\mathcal{M})$ *o conjunto das retas e dos círculos construídos a partir de pontos de* $\mathcal{M}$.

Definição .2.2. *O conjunto dos pontos simplesmente construtíveis a partir de* $\mathcal{M}$ *denotado por* $\mathcal{M}^{(1)}$ *é definido por*

$$\mathcal{M}^{(1)} = \{z \in \mathbb{C}; z \in \gamma_1 \cap \gamma_2; \gamma_1, \gamma_2 \in \Gamma(\mathcal{M}); \gamma_1 \neq \gamma_2\}$$

Indutivamente, definimos $\mathcal{M}^{(n+1)} = (\mathcal{M}^{(n)})^{(1)}, \forall n \in \mathbb{N}$, sendo que consideraremos que $\mathcal{M}^{(0)} = \mathcal{M}$. Assim,

$$\mathcal{M}^{(0)} \subseteq \mathcal{M}^{(1)} \subseteq \mathcal{M}^{(2)} \subseteq \ldots$$

Além disso, a união $\mathcal{M}^{(\infty)} = \cup_{n\in\mathbb{N}}\mathcal{M}^{(n)}$ é denominada o conjunto dos pontos construtíveis a partir de $\mathcal{M}^{(0)}$.

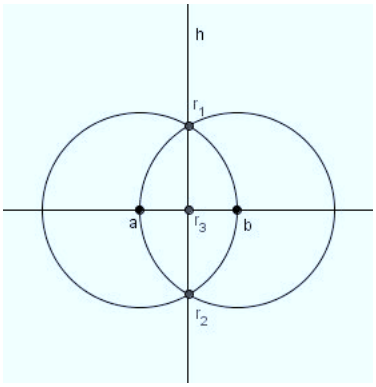
Definição .2.3. *Denotaremos por* $\Gamma(\mathcal{M}^{(i)})$ *o conjunto das retas e dos círculos construídos a partir de pontos de* $\mathcal{M}^{(i)}$.

Com excessão de alguns momentos, não vamos estar tão interessados no número n tal que os pontos construídos estejam em $\mathcal{M}^{(n)}$, assim, em vários momentos, iremos trabalhar com $\mathcal{M}^{(\infty)}$ no lugar de $\mathcal{M}$ e simplesmente vamos nos referir a eles como "pontos construtíveis" e aos elementos de $\Gamma(\mathcal{M}^{(i)})$ como "retas e\ou círculos construtíveis".

Nos resultados que seguem vamos indicar algumas construções sem provar todos os detalhes.

Lema .2.4. *Sejam $a, b \in \mathcal{M}$. Então, o ponto médio desses pontos é construtível a partir de $\mathcal{M}$. Mais precisamente, o ponto médio entre a e b pertence a $\mathcal{M}^{(2)}$.*

Demonstração: Seja t a reta que passa por a e b.



- Trace um círculo com centro em a e raio $|a - b|$;
- Trace um círculo com centro em b e raio $|a - b|$;

  Sejam r_1, r_2 pontos da interseção dos círculos, então $r_1, r_2 \in \mathcal{M}^{(1)}$.
- Trace a reta h que passa por r_1 e r_2;

  Note que $h \in \Gamma(\mathcal{M}^{(1)})$.
- O ponto da interseção da reta h com a reta t é o ponto médio de a e b, denotado por r_3 que pertence a $\mathcal{M}^{(2)}$. ■

Proposição .2.5. *Seja $z \in \mathcal{M}$ e $\rho \in \Gamma(\mathcal{M})$ uma reta. Então, a reta paralela a ρ passando por z e a reta perpendicular a ρ passando por z pertencem a $\Gamma(\mathcal{M}^{(3)})$.*

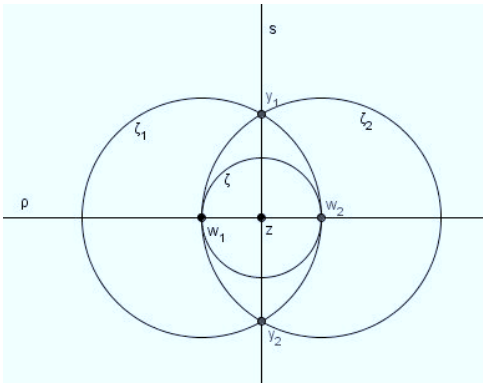
Demonstração: Vamos denotar por r a reta paralela a ρ passando por z e por s a reta perpendicular a ρ passando por z.

1º caso)$z \in \rho$

Neste caso, r coincide com ρ e $\rho \in \Gamma(\mathcal{M}) \subseteq \Gamma(\mathcal{M}^{(3)})$, já que $\mathcal{M} \subseteq \mathcal{M}^{(1)} \subseteq \mathcal{M}^{(2)} \subseteq \mathcal{M}^{(3)}$.

Por outro lado, s constrói-se da seguinte forma: inicialmente, observe que, como $\rho \in \Gamma(\mathcal{M})$ a reta ρ é determinada por z e w_1, para algum $w_1 \in \mathcal{M} \setminus \{z\}$. Seja ζ o círculo com centro em z e passando por w_1. Então, $\rho \cap \zeta = \{w_1, w_2\}$ para algum $w_2 \in \mathcal{M}^{(1)}$.

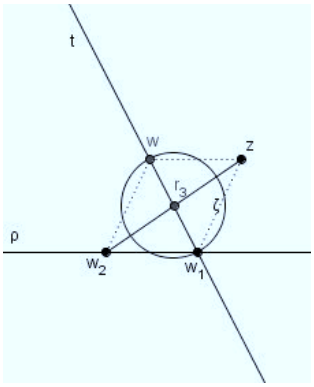
Seja ζ_j o círculo com centro em w_j e raio igual à distância entre w_1 e w_2 para $j = 1, 2$. Então, $\zeta_1 \cap \zeta_2$ consiste de dois pontos, digamos y_1 e y_2. Assim, $y_1, y_2 \in \mathcal{M}^{(2)}$ e estes determinam a reta $s \in \Gamma(\mathcal{M}^{(2)}) \subseteq \Gamma(\mathcal{M}^{(3)})$.



Deixamos para o leitor a tarefa de comprovar que s é de fato perpendicular a ρ.

2º caso)$z \notin \rho$

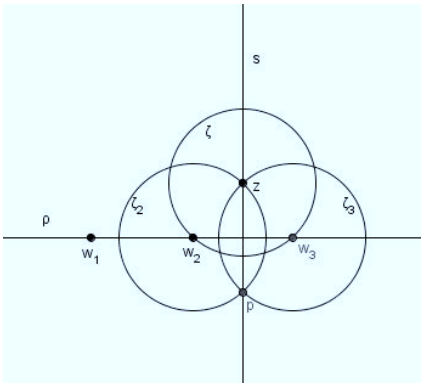
A reta ρ é determinada por dois pontos que vamos denotar por $w_1, w_2 \in \mathcal{M}$. Como $z \in \mathcal{M}$, pelo lema (.2.4), temos que o ponto médio de w_2 e z, denotado por r_3, é construtível (mais precisamente, pertence a $\mathcal{M}^{(2)}$).



Tracemos a reta t determinada por r_3 e w_1, bem como o círculo ζ com centro em r_3 passando por w_1, e seja $w \in \zeta \cap t$ tal que $w \neq w_1$. Então, $w \in \mathcal{M}^{(3)}$. Assim, o polígono $w_2 w_1 z w$ é um paralelogramo, pois suas diagonais encontram-se em seus pontos médios. Então, o segmento wz é paralelo ao segmento $w_2 w_1$. Logo, w, z determinam a reta $r \in \Gamma(\mathcal{M}^{(3)})$.

Para construir a reta s, podemos supor que z não pertence a reta perpendicular a ρ passando por w_2, pois caso contrário, nada há a fazer. Como $z \in \mathcal{M}$, por hipótese, podemos considerar o círculo ζ com centro em z e passando por w_2, então $\rho \cap \zeta = \{w_2, w_3\}$ para algum $w_3 \in \mathcal{M}^{(1)}$ (note que, como z não pertence à reta perpendicular a ρ passando por w_2 a existência deste segundo ponto w_3 está garantida).

Seja ζ_j ($j \in \{2, 3\}$) o círculo com centro em w_j e raio igual a $|z - w_2| = |z - w_3|$ então $\zeta_2 \cap \zeta_3 = \{z, p\}$, para algum $p \in \mathcal{M}^{(2)} \setminus \{z\}$. Afirmamos que p, z determinam a reta $s \in \Gamma(\mathcal{M}^{(2)}) \subseteq \Gamma(\mathcal{M}^{(3)})$, cuja prova deixamos ao leitor.



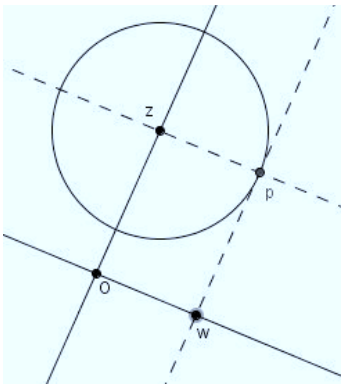
■

Nas próximas construções, iremos utilizar as seguintes notações:

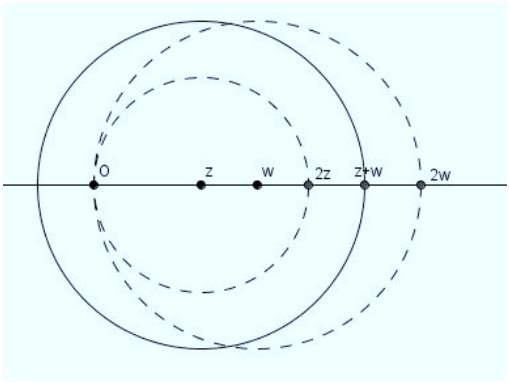
ζ_r: o círculo com centro em 0 e raio r
$r_{z,w}$: a reta determinada pelos pontos z, w
ε: a reta determinada pelos pontos 0,1
ε': a reta perpendicular a ε passando pelo 0

Corolário .2.6. *Dados $z, w \in \mathcal{M}$ não nulos e distintos é possível traçar o círculo de centro em z e raio igual a $|w|$.*

Demonstração: Suponhamos que $0, z, w$ não são colineares. Como $z, w \in \mathcal{M}$, é possível traçar por w a reta paralela a $r_{0,z}$ e por z a reta paralela a $r_{0,w}$. O ponto p da intersecção de tais retas é portanto construtível e, obviamente, o círculo de centro z e que passa por p tem raio $|w|$.



Suponha, agora, que $0, z, w$ são colineares. Tracemos por z o círculo de raio $|z|$, o que origina o ponto $2z$. Da mesma forma, tracemos por w o círculo de raio $|w|$, o que origina o ponto $2w$. E, assim, o ponto médio de $2z$ e $2w$ é $z + w$, logo podemos traçar o círculo de centro em z e raio $|w|$.



Proposição .2.7. *Considerando o plano complexo*[‡]*, temos:*

(i) $i \in \mathcal{M}^{(\infty)}$*, isto é, i é um ponto construtível;*

(ii) Quaisquer que sejam $r > 0$ *e* φ *tais que* $0 \leq \varphi < \pi$*, temos que* $r, e^{i\varphi} \in \mathcal{M}^{(\infty)}$ *se, e somente se,* $re^{i\varphi} \in \mathcal{M}^{(\infty)}$*;*

(iii) Se $z \in \mathcal{M}^{(\infty)}$ *então* $\overline{z} \in \mathcal{M}^{(\infty)}$*, bem como* $-z \in \mathcal{M}^{(\infty)}$*;*

(iv) Se $z, w \in \mathcal{M}^{(\infty)}$ *então* $z+w \in \mathcal{M}^{(\infty)}$*. Em particular, todos os naturais maiores do que 1 são construtíveis;*

(v) Se $z, w \in \mathcal{M}^{(\infty)}$*,* $w \neq 0$ *então* $zw^{-1} \in \mathcal{M}^{(\infty)}$*. Em particular, todos os racionais são construtíveis;*

(vi) Se $z \in \mathcal{M}^{(\infty)}$ *e* $y \in \mathbb{C}$ *tais que* $y^2 = z$ *então* $y \in \mathcal{M}^{(\infty)}$*.*

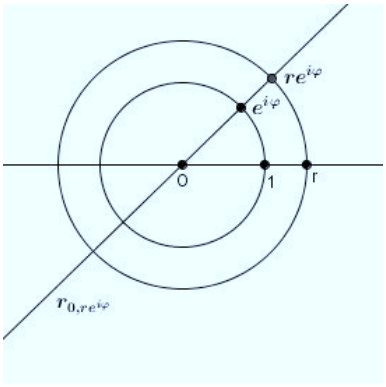
Demonstração: Vamos supor que $\mathcal{M} = \mathcal{M}^{(\infty)}$, o que não causa nenhuma confusão em nossas notações, conforme foi explicado anteriormente.

(i) Note que $i \in \zeta_1 \cap \varepsilon' \subseteq \mathcal{M}$.

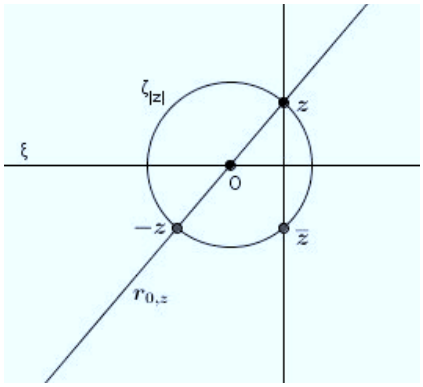
(ii) Suponhamos que $r, e^{i\varphi} \in \mathcal{M}$ então $re^{i\varphi} \in \zeta_r \cap r_{0,e^{i\varphi}} \subseteq \mathcal{M}$.

Reciprocamente, suponhamos que $re^{i\varphi} \in \mathcal{M}$. Como $r = |re^{i\varphi}|$, temos que $\zeta_r \in \Gamma(\mathcal{M})$. Logo, $r \in \varepsilon \cap \zeta_r \in \mathcal{M}$. Além disso, $e^{i\varphi} \in \zeta_1 \cap r_{0,re^{i\varphi}} \subseteq \mathcal{M}$.

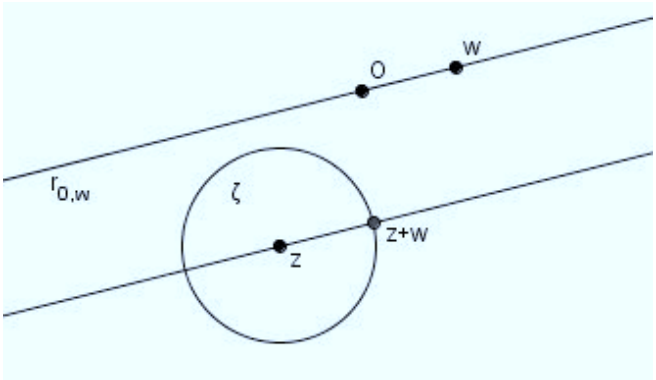
[‡]Estamos, aqui, nos permitindo falar ora em pontos, ora em números, usando livremente a correspondência $a + bi \leftrightarrow (a, b)$.



(iii) Temos que $\overline{z}$ pertence a intersecção de $\zeta_{|z|}$ e da reta perpendicular a ε passando por z, logo $\overline{z} \in \mathcal{M}$. E mais, $-z \in \zeta_{|z|} \cap r_{0,z} \subseteq \mathcal{M}$.



(iv) Se $0, z, w$ são colineares a demonstração é a mesma feita no corolário (.2.6). Se $0, z, w$ não são colineares, novamente, pelo corolário (.2.6), podemos tomar ζ o círculo com centro em z e raio igual a $|w|$, então $z + w$ pertence a intersecção de ζ com a reta paralela a $r_{0,w}$ passando por z, logo, $z + w \in \mathcal{M}$.



(v) Vamos considerar

$$z = re^{i\varphi}$$

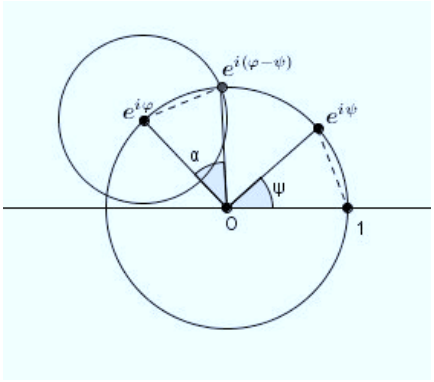
$$w = se^{i\psi}$$

Então, como $zw^{-1} = rs^{-1}e^{i(\varphi-\psi)}$, pelo item (ii) basta provarmos as seguintes implicações:

$$e^{i\varphi}, e^{i\psi} \in \mathcal{M} \Longrightarrow e^{i(\varphi-\psi)} \in \mathcal{M}$$

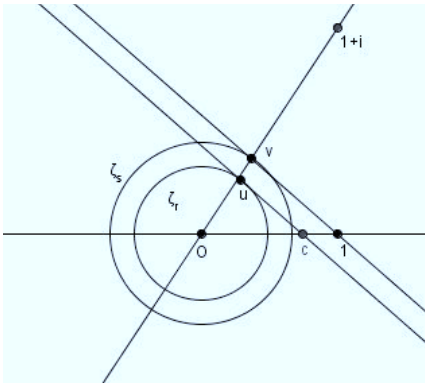
$$r, s \in \mathcal{M} \Longrightarrow rs^{-1} \in \mathcal{M}$$

Se $\psi = 0$ precisamos mostrar apenas a segunda implicação. Supondo $\psi \neq 0$, seja ζ o círculo com centro em $e^{i\varphi}$ e raio igual a $|1 - e^{i\psi}|$ (note que o ponto $1 - e^{i\psi}$ é construtível, por (iv)).



Os dois triângulos acima são congruentes pela congruência LLL, assim, $\psi = \alpha$. Então $e^{i(\varphi-\psi)} \in \zeta_1 \cap \zeta \subseteq \mathcal{M}$.

Sejam $u \in \zeta_r \cap r_{0,1+i}$, $v \in \zeta_s \cap r_{0,1+i}$ (lembre que $1, i$ são construtíveis e, portanto, por (iv), $1 + i$ é construtível) e c pertencente a intersecção de ε com a reta paralela a $r_{1,v}$ passando por u. Então, temos que $u, v, c \in \mathcal{M}$.



Assim, pelo Teorema de Tales, temos que

$$\frac{r}{s} = \frac{|u|}{|v|} = \frac{c}{1} = c \in \mathcal{M}$$

Logo, $rs^{-1} \in \mathcal{M}$.

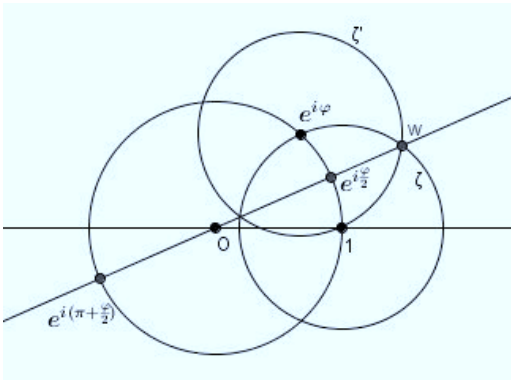
(vi) Se $y^2 = z = re^{i\varphi} \in \mathcal{M}$ então

$$y \in \{\sqrt{r}e^{i\frac{\varphi}{2}}, \sqrt{r}e^{i(\frac{\varphi}{2}+\pi)}\}$$

e pelo item (ii) basta provarmos que $\sqrt{r}, e^{i\frac{\varphi}{2}}, e^{i(\frac{\varphi}{2}+\pi)} \in \mathcal{M}$.

Se $\varphi = 0$, basta mostrarmos que $\sqrt{r} \in \mathcal{M}$. Supondo $\varphi \neq 0$ sejam ζ o círculo com centro em 1 e raio igual a $|e^{i\varphi} - 1|$ e ζ' o círculo com centro em $e^{i\varphi}$ com o mesmo raio do círculo ζ. Seja $w \in \zeta \cap \zeta'$, então

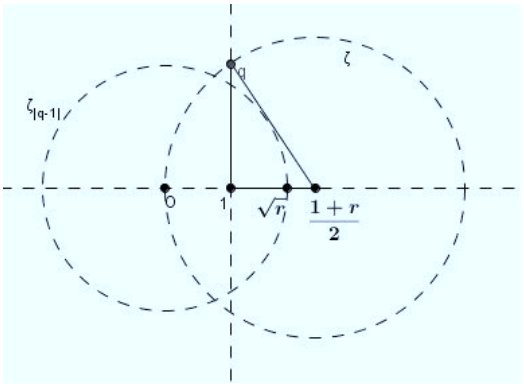
$$e^{i\frac{\varphi}{2}}, e^{i(\frac{\varphi}{2}+\pi)} \in \zeta_1 \cap r_{0,w} \subseteq \mathcal{M}$$



No caso em que $r > 1$, seja ζ o círculo com centro e raio iguais a $\frac{1+r}{2}$ (note que $1, r$ construtíveis implica que o ponto médio entre eles é construtível, pelo lema(.2.4)) e seja q pertencente a intersecção de ζ com a reta perpendicular a ε passando por 1. Então,

$$|q-1|^2 + \left(\frac{r-1}{2}\right)^2 = \left(\frac{r+1}{2}\right)^2$$

donde $|q-1|^2 = \frac{r^2+2r+1-r^2+2r-1}{4} = \frac{4r}{4} = r$ Assim, $\sqrt{r} = |q-1| \in \zeta_{|q-1|} \cap \varepsilon \subseteq \mathcal{M}$.



No caso em que $r \leq 1$, temos que $r^{-1} \geq 1$ então pelo o que fizemos acima $\sqrt{r^{-1}} \in \mathcal{M}$. Como $1, \sqrt{r^{-1}} \in \mathcal{M}$, pelo item (v), temos que $(\sqrt{r^{-1}})^{-1} \in \mathcal{M}$, isto é, $\sqrt{r} \in \mathcal{M}$. ■

Notação .2.8. *Denotaremos por $\mathcal{K}_{\mathcal{M}}$ o corpo $\mathbb{Q}(\mathcal{M} \cup \overline{\mathcal{M}})$ sendo que $\overline{\mathcal{M}} = \{\overline{z}; z \in \mathcal{M}\}$.*

Corolário .2.9. *$\mathcal{M}^{(\infty)}$ é um subcorpo de $\mathbb{C}$ que contém $\mathbb{Q}(i)$ e $\mathcal{K}_{\mathcal{M}}$.*

É importante notar que quando $\mathcal{M} = \{0, 1\}$ então $\mathcal{K}_{\mathcal{M}} = \mathbb{Q}$.

Queremos estudar com mais detalhes a extensão $\mathcal{M}^{(\infty)}|\mathcal{K}_{\mathcal{M}}$; para isso, vamos antes analisar melhor o corpo $\mathcal{K}_{\mathcal{M}}(z)$, onde $z \in \mathcal{M}^{(1)}$. Para tal, precisamos introduzir a equação complexa da reta e do círculo.

A reta $r_{u,v}$ é dada por

$$r_{u,v} = \{u + (v-u)t; t \in \mathbb{R}\} = \left\{y \in \mathbb{C}; \frac{y-u}{v-u} = \frac{\overline{y}-\overline{u}}{\overline{v}-\overline{u}}\right\}$$

ou seja, essa é uma outra maneira de dizer que $\frac{y-u}{v-u}$ é um número real.

Portanto, a equação da reta determinada por u e v é dada por

$$(Y-u)\frac{\overline{v}-\overline{u}}{v-u}-(\overline{Y}-\overline{u})=0$$

Da mesma forma, o círculo ζ com centro em w e raio r é dado por

$$\zeta=\{y\in\mathbb{C};|y-w|=r\}=\{y\in\mathbb{C};(y-w)(\overline{y}-\overline{w})=r^2\}$$

Portanto, a equação desse círculo é dado por

$$(Y-w)(\overline{Y}-\overline{w})-r^2=0$$

Proposição .2.10. *Para todo $z\in\mathcal{M}^{(1)}$, temos $[\mathcal{K}_{\mathcal{M}}(z):\mathcal{K}_{\mathcal{M}}]\leq 2$ e $[\mathcal{K}_{\mathcal{M}}(\overline{z}):\mathcal{K}_{\mathcal{M}}]\leq 2$.*

Demonstração: Como $z\in\mathcal{M}^{(1)}$ então existem $\gamma_1,\gamma_2\in\Gamma(\mathcal{M})$, $\gamma_1\neq\gamma_2$ tais que $z\in\gamma_1\cap\gamma_2$. Analisaremos os seguintes casos:

1) γ_1,γ_2 são retas não paralelas, digamos $\gamma_j=r_{u_j,v_j}$ com $u_j,v_j\in\mathcal{M}$ com $j=1,2$, então $v_2-u_2\neq t(v_1-u_1),\forall t\in\mathbb{R}$.

Seja $c_j=\frac{\overline{v_j}-\overline{u_j}}{v_j-u_j}$ então $c_1\neq c_2$, pois caso contrário

$$\frac{\overline{v_2}-\overline{u_2}}{\overline{v_1}-\overline{u_1}}=\frac{v_2-u_2}{v_1-u_1}$$

Portanto, $\frac{v_2-u_2}{v_1-u_1}\in\mathbb{R}$, o que é uma contradição com a desigualdade acima.

Consideremos as equações complexas das retas γ_1 e γ_2, respectivamente:

$$(Y-u_1)\frac{\overline{v_1}-\overline{u_1}}{v_1-u_1}-(\overline{Y}-\overline{u_1})=0$$

$$(Y-u_2)\frac{\overline{v_2}-\overline{u_2}}{v_2-u_2}-(\overline{Y}-\overline{u_2})=0$$

Então, como $z\in\gamma_1\cap\gamma_2$ ela satisfaz as duas equações acima e, portanto, após alguns cálculos, temos que z satisfaz uma equação do tipo

$$Y(c_1-c_2)-u_1c_1+u_2c_2+\overline{u_1}-\overline{u_2}=0$$

com $c_1, c_2 \in \mathbb{C}$, ou seja, satisfaz uma equação polinomial de grau um com coeficientes em $\mathcal{K}_{\mathcal{M}}$. E assim, $z \in \mathcal{K}_{\mathcal{M}}$.

Como z é um ponto construtível, pela demonstração da proposição (.2.7) item (iii), temos que $\overline{z} \in \mathcal{M}^{(1)}$, então da mesma forma feita acima, prova-se que $\overline{z} \in \mathcal{K}_{\mathcal{M}}$.

Então, $[\mathcal{K}_{\mathcal{M}}(z) : \mathcal{K}_{\mathcal{M}}] = 1 \leq 2$ e $[\mathcal{K}_{\mathcal{M}}(\overline{z}) : \mathcal{K}_{\mathcal{M}}] = 1 \leq 2$.

2) γ_1 é a reta $r_{u,v}$ e γ_2 é o círculo ζ com centro em w e raio igual a $|z - z'|$ onde $u, v, w, z, z' \in \mathcal{M}$.

Denotando $c = \frac{\overline{v}-\overline{u}}{v-u} \neq 0$, temos que as equações complexas da reta e do círculo, respectivamente, são:

$$(Y - u)c - (\overline{Y} - \overline{u}) = 0$$

$$(Y - w)(\overline{Y} - \overline{w}) - |z - z'|^2 = 0$$

Da primeira igualdade, temos que $\overline{Y} = (Y - u)c + \overline{u}$. Substituindo na segunda equação, obtemos:

$$(Y - w)((Y - u)c + \overline{u} - \overline{w}) - (z - z')(\overline{z} - \overline{z'}) = 0$$

Renomeando e arrumando a igualdade acima, recaimos em uma equação da seguinte forma:

$$cY^2 + dY + e = 0$$

onde $d, e \in \mathcal{K}_{\mathcal{M}}$. Como $z \in \gamma_1 \cap \gamma_2$, z satisfaz essa equação, logo $[\mathcal{K}_{\mathcal{M}}(z) : \mathcal{K}_{\mathcal{M}}] \leq 2$.

Analogamente, prova-se que $[\mathcal{K}_{\mathcal{M}}(\overline{z}) : \mathcal{K}_{\mathcal{M}}] \leq 2$.

3) γ_1, γ_2 são círculos ζ_1, ζ_2 com centros w_j distintos e com raios iguais a $|z_j - z'_j|$ onde $j = 1, 2$ e $w_1, w_2, z_1, z'_1, z_2, z'_2 \in \mathcal{M}$.

Consideremos as equações complexas dos círculos ζ_1, ζ_2, respectivamente:

$$(Y - w_1)(\overline{Y} - \overline{w_1}) - (z_1 - z'_1)(\overline{z_1} - \overline{z'_1}) = 0$$

$$(Y - w_2)(\overline{Y} - \overline{w_2}) - (z_2 - z_2')(\overline{z_2} - \overline{z_2'}) = 0$$

Subtraindo a segunda equação da primeira, temos

$$\overline{Y}(w_2 - w_1) + Y(\overline{w_2} - \overline{w_1}) + w_1\overline{w_1} - w_2\overline{w_2} - (z_1 - z_1')(\overline{z_1} - \overline{z_1'}) + (z_2 - z_2')(\overline{z_2} - \overline{z_2'}) = 0$$

Como $w_2 \neq w_1$, dividindo por $w_2 - w_1$ obtemos uma equação da forma

$$\overline{Y} - Yc + b = 0$$

para certos $b, c \in \mathcal{K}_{\mathcal{M}}$.

Substituindo $\overline{Y}$ por $Yc - b$ na equação complexa de ζ_2, recaímos em uma equação do tipo $cY^2 + dY + e = 0$ com $d, e \in \mathcal{K}_{\mathcal{M}}$.

Novamente, como $z \in \gamma_1 \cap \gamma_2$, z satisfaz essa equação, então $[\mathcal{K}_{\mathcal{M}}(z) : \mathcal{K}_{\mathcal{M}}] \leq 2$.

Analogamente, prova-se que $[\mathcal{K}_{\mathcal{M}}(\overline{z}) : \mathcal{K}_{\mathcal{M}}] \leq 2$. ■

Teorema .2.11. *Para todo $z \in \mathcal{M}^{(\infty)}$ existe uma cadeia finita*

$$\mathcal{K}_{\mathcal{M}} = \mathcal{L}_0 \subseteq \mathcal{L}_1 \subseteq \ldots \subseteq \mathcal{L}_r$$

de subcorpos de $\mathbb{C}$ tais que $z, \overline{z} \in \mathcal{L}_r$ e $[\mathcal{L}_j : \mathcal{L}_{j-1}] = 2$ para $j = 1, \ldots, r$.

Em particular, $[\mathcal{K}_{\mathcal{M}}(z) : \mathcal{K}_{\mathcal{M}}]$ e $[\mathcal{K}_{\mathcal{M}}(\overline{z}) : \mathcal{K}_{\mathcal{M}}]$ são potências de 2.

Demonstração: Como $z \in \mathcal{M}^{(\infty)}$, existe $k \in \mathbb{N}$ tal que $z \in \mathcal{M}^{(k)}$, então $z \in \gamma \cap \gamma'$ para certos $\gamma, \gamma' \in \Gamma(\mathcal{M}^{(k-1)})$, os quais são obtidos a partir de um número finito de elementos $z_1^{(k-1)}, \ldots, z_s^{(k-1)} \in \mathcal{M}^{(k-1)}$.

Da mesma forma, $z_j^{(k-1)} \in \gamma_j \cap \gamma_j'$ para certos $\gamma_j, \gamma_j' \in \Gamma(\mathcal{M}^{(k-2)})$ e $\gamma_1, \gamma_1', \ldots, \gamma_s, \gamma_s'$ são obtidos a partir de um número finito de elementos $z_1^{(k-2)}, \ldots, z_t^{(k-2)} \in \mathcal{M}^{(k-2)}$, assim sucessivamente.

Reunindo os elementos assim obtidos, temos

$$z; z_1^{(k-1)}, \ldots, z_s^{(k-1)}; z_1^{(k-2)}, \ldots, z_t^{(k-2)}; \ldots; z_1^{(0)}, \ldots, z_u^{(0)}$$

na ordem inversa, dessa maneira obtemos uma sequência finita $z_1, \ldots, z_g = z$.

Para todo $j \in \{0, \ldots, g\}$ sejam $\mathcal{M}_j = \mathcal{M} \cup \{z_1, \ldots, z_j\}$ e $\mathcal{L}_j = \mathcal{K}_{\mathcal{M}_j}$ então $\mathcal{L}_j = \mathcal{L}_{j-1}(z_j, \overline{z_j})$

Note que pela construção dos z_i, z_j foi construído a partir dos elementos do conjunto $\{z_1, \ldots, z_{j-1}\}$, logo

$$z_j \in (\mathcal{M}_{j-1})^{(1)}$$

Pela proposição (.2.10), temos que $[\mathcal{K}_{\mathcal{M}_{j-1}}(z_j) : \mathcal{K}_{\mathcal{M}_{j-1}}] \leq 2$ e $[\mathcal{K}_{\mathcal{M}_{j-1}}(\overline{z_j}) : \mathcal{K}_{\mathcal{M}_{j-1}}] \leq 2$.

Pela definição de $\mathcal{L}_{j-1}$, temos $[\mathcal{L}_{j-1}(z_j) : \mathcal{L}_{j-1}] \leq 2$ e $[\mathcal{L}_{j-1}(\overline{z_j}) : \mathcal{L}_{j-1}] \leq 2$.

Note que $[\mathcal{L}_{j-1}(z_j, \overline{z_j}) : \mathcal{L}_{j-1}(z_j)] \leq 2$, uma vez que como $[\mathcal{L}_{j-1}(\overline{z_j}) : \mathcal{L}_{j-1}] \leq 2$, $\overline{z_j}$ satisfaz um polinômio de grau no máximo 2 em $\mathcal{L}_{j-1}$, logo satisfaz um polinômio de grau no máximo 2 em $\mathcal{L}_{j-1}(z_j)$.

Portanto, considerando a cadeia

$$\mathcal{K}_{\mathcal{M}} = \mathcal{L}_0 \subseteq \mathcal{L}_0(z_1) \subseteq \mathcal{L}_0(z_1, \overline{z_1}) = \mathcal{L}_1 \subseteq$$

$$\subseteq \mathcal{L}_1(z_2) \subseteq \mathcal{L}_1(z_2, \overline{z_2}) = \mathcal{L}_2 \subseteq \ldots \subseteq \mathcal{L}_{g-1}(z_g, \overline{z_g}) = \mathcal{L}_g$$

após a eliminação de corpos repetidos, temos a propriedade desejada.

Por conseguinte, a última afirmação do teorema é decorrente do fato que os graus indicados dividem $[\mathcal{L}_g : \mathcal{K}_{\mathcal{M}}]$, que é uma potência de 2. ■

Os próximos resultados serão úteis para o nosso objetivo de construir uma raiz m-ésima primitiva da unidade, ζ_m, a partir de $\mathcal{M} = \{0, 1\}$.

Teorema .2.12. *Se $N|\mathcal{K}_{\mathcal{M}}$ for uma extensão normal com $[N : \mathcal{K}_{\mathcal{M}}] = 2^m$ para algum $m \in \mathbb{N}$ então $N \subseteq \mathcal{M}^{(\infty)}$.*

Demonstração: Se $m = 0$ então $[N : \mathcal{K}_{\mathcal{M}}] = 2^0 = 1$. Assim, $N = \mathcal{K}_{\mathcal{M}} \subseteq \mathcal{M}^{(\infty)}$, devido ao corolário (.2.9). Logo, para $m = 0$ o teorema é válido.

Por indução, suponhamos que o teorema seja válido para $m-1$ onde $m>1$. Seja $N|\mathcal{K}_{\mathcal{M}}$ uma extensão normal com $[N:\mathcal{K}_{\mathcal{M}}]=2^m$ e seja $G=Gal(N|\mathcal{K}_{\mathcal{M}})$.

Por hipótese, temos que $N|\mathcal{K}_{\mathcal{M}}$ é normal e $[N:\mathcal{K}_{\mathcal{M}}]=2^m$, logo $N|\mathcal{K}_{\mathcal{M}}$ é finita e como $\mathbb{Q}\subseteq\mathcal{K}_{\mathcal{M}}$ temos que $N|\mathcal{K}_{\mathcal{M}}$ é separável. Portanto, pelo teorema (1.2.18), temos que G tem ordem 2^m.

O centro de G

$$Z(G)=\{\rho\in G;\sigma\circ\rho=\rho\circ\sigma,\forall\sigma\in G\}$$

é um subgrupo não-trivial, pois G é um 2-grupo (veja lema (1.1.3)). Seja ρ um elemento do centro (que é também um 2-grupo), $\rho\neq id$ tal que $|\langle\rho\rangle|=2$ (existe devido ao teorema de Cauchy). Então, $\langle\rho\rangle$ é um subgrupo normal de G, logo, o corpo intermediário $L=Fix(\langle\rho\rangle)$ correspondente a $\langle\rho\rangle$ é uma extensão normal de $\mathcal{K}_{\mathcal{M}}$, devido ao teorema (1.2.18). Além disso,

$$[L:\mathcal{K}_{\mathcal{M}}]=\frac{|G|}{|L^*|}=\frac{|G|}{|(Fix(\langle\rho\rangle))^*|}=\frac{|G|}{|\langle\rho\rangle|}\overset{|\rho|=2}{=}2^{m-1}$$

Portanto, pela hipótese de indução, $L\subseteq\mathcal{M}^{(\infty)}$.

Como $2^m=[N:\mathcal{K}_{\mathcal{M}}]=[N:L][L:\mathcal{K}_{\mathcal{M}}]=[N:L].2^{m-1}$, temos $[N:L]=2$. Assim, por (1.2.5), $N=L(y)$ para algum $y\in\mathbb{C}$ tal que $y^2=z\in L\subseteq\mathcal{M}^{(\infty)}$. Pela proposição (.2.7)$(vi)$ resulta que $y\in\mathcal{M}^{(\infty)}$ e, portanto, $N=L(y)\subseteq\mathcal{M}^{(\infty)}$. ■

Corolário .2.13. (Gauss) *O m-polígono regular é construtível com régua e compasso*[§] *se, e somente se, $\varphi(m)$ for uma potência de 2.*

Demonstração: Pelo teorema (1.3.4), temos que $[\mathbb{Q}(\zeta_m):\mathbb{Q}]=\varphi(m)$ onde ζ_m é uma raiz m-ésima primitiva da unidade.

Suponhamos que $\varphi(m)$ é uma potência de 2, como $\mathbb{Q}(\zeta_m):\mathbb{Q}$ é uma extensão normal, já que $\mathbb{Q}(\zeta_m)$ é o corpo de raízes do polinômio X^m-1, pelo teorema

[§]O m-polígono regular é construtível com régua e compasso se, e somente se, for possível construir uma raiz m-ésima primitiva da unidade.

(.2.12) temos que $\zeta_m \in \mathbb{Q}(\zeta_m) \subseteq \mathcal{M}^{(\infty)}$. Então é possível construir uma raiz m-ésima primitiva da unidade, logo é possível construir todas as m-ésimas raízes da unidade, uma vez que produto de construtíveis é construtível e todas as demais raízes são potências de ζ_m. Logo, o m-ésimo polígono regular é construtível com régua e compasso.

Reciprocamente, suponhamos que o m-ésimo polígono regular pode ser construído com régua e compasso, isto é, $\zeta_m \in \mathcal{M}^{(\infty)}$. Partindo de $\mathcal{M} = \{0, 1\}$ temos que $\mathcal{K}_{\mathcal{M}} = \mathbb{Q}$ e, então, por (.2.11), $\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ é uma potência de 2. ■

Encerramos esta seção indicando quais são os números $m \geq 1$ tais que $\varphi(m)$ é uma potência de 2 e provando uma propriedade dos primos de Fermat.

Definição .2.14. *Um primo ímpar p é chamado primo de Fermat se $\varphi(p)$ for uma potência de 2 ou, equivalentemente (veja .1.6), quando $p = 2^r + 1$ para algum $r \geq 1$.*

Proposição .2.15. *Dado $m \in \mathbb{N}$, temos que $\varphi(m)$ será uma potência de 2 se, e somente se, $m = 2^s p_1 \dots p_k$ sendo $p_1, \dots, p_k$ primos de Fermat distintos e $s \in \mathbb{N}$.*

Demonstração: Suponhamos que $m = 2^s p_1 \dots p_k$ sendo $p_1, \dots, p_k$ primos de Fermat distintos e $s \in \mathbb{N}$. Então, pela proposição (.1.6), temos

$$\varphi(m) = \varphi(2^s p_1 \dots p_k) = \varphi(2^s)\varphi(p_1) \dots \varphi(p_k) = 2^{(s-1)}(p_1 - 1) \dots (p_k - 1)$$

que é potência de 2, pela definição de primos de Fermat.

Por outro lado, suponhamos que $\varphi(m)$ é uma potência de 2, digamos $\varphi(m) = 2^l$, com $l \in \mathbb{N}$. Seja $m = 2^s p_1^{s_1} \dots p_r^{s_r}$ fatoração de m com p_i primos ímpares e distintos. Então, novamente pela proposição (.1.6),

$$2^l = \varphi(m) = \varphi(2^s p_1^{s_1} \dots p_r^{s_r}) = \varphi(2^s)\varphi(p_1^{s_1}) \dots \varphi(p_r^{s_r}) =$$

$$2^{s-1} p_1^{s_1 - 1}(p_1 - 1) \dots p_r^{s_r - 1}(p_r - 1)$$

Como p_i são primos ímpares, obtemos que $s_i = 1$ para $i = 1, \ldots, r$. E, além disso, $p_i = 2^{k_i} + 1$. Assim, $m = 2^s p_1 \ldots p_k$ onde $p_i = 2^{k_i} + 1$. ■

Proposição .2.16. *Para todo p primo de Fermat existe um* $t \in \mathbb{N}$ *tal que* $p = 2^{2^t} + 1$.

Demonstração: Suponhamos $p = 2^u + 1$, para algum $u \geq 1$. Queremos mostrar que u não é divisível por nenhum número primo ímpar s, pois assim u será necessariamente uma potência de 2. Suponhamos então $u = rs$, com $r \geq 1$ e s um primo ímpar.

A ideia principal da demonstração é analisar a fatoração do polinômio $X^s + 1$ aplicado em 2^r o qual nos produz uma fatoração de $p = 2^u + 1$.

Como s é ímpar, -1 é raiz de $X^s + 1$, logo $X^s + 1 = (X + 1)F(X)$ para algum $F(X) \in \mathbb{Z}[X]$, devido ao lema (1.3.3). Portanto, substituindo $X = 2^r$, temos

$$p = 2^u + 1 = 2^{rs} + 1 = (2^r + 1)F(2^r),$$

Como $r \geq 1$ e s é primo, $2^{rs} + 1 \neq 2^r + 1 > 1$. Portanto, $2^{rs} + 1 = (2^r + 1)F(2^r)$ é uma fatoração não trivial para o primo p, o que gera um absurdo.

Resulta que se $2^u + 1$ for primo, então u não será divisível por nenhum número primo ímpar s, ou seja, u será uma potência de 2. ■

Essa propriedade dos primos de Fermat será útil na demonstração de algumas aplicações do teorema que será apresentado no capítulo 2 (veja corolário(2.2.5)).

Referências Bibliográficas

[1] Cox, D., *Galois Theory*, Wiley-Interscience, 2004.

[2] Endler, O., *Teoria dos Corpos*, Publicações Matemáticas, Rio de Janeiro, IMPA, 2010.

[3] Garcia, A.; Lequain, Y., *Elementos de Álgebra*, Projeto Euclides, 4.ed., Rio de Janeiro, IMPA, 2006.

[4] Lequain, Y., *Tópicos da teoria de Galois*, Atas da 8ª Escola de Álgebra, Rio de Janeiro, IMPA, 1985.

[5] Morandi, P., *Field and Galois Theory*, Graduate Texts in Mathematics 167, Springer, 1996.

[6] Moreira, C., *"Um Teorema sobre Solubilidade de Equações Polinomiais por Radicais Reais "*, Matemática universitária n.12, Rio de Janeiro, SBM, 1990.

[7] Ripoll, J.; Ripoll, C.; Silveira, F., *O Tormento de Cardano*, maio de 2012. Disponível em: ¡http:
klein.sbm.org.br¿. Acesso em: 22 jul. 2012.

[8] Stewart, I., *Galois Theory*, London Chapman and Hall, 1973.

[9] Van Der Waerden, B., *Álgebra*, Vol. 1, NY, Springer-Verlag, 2003.