
Solubilidade por radicais

Nesta seção veremos como será possível usar a teoria de Galois pra estudar a existência de “fórmulas” para raízes de polinômios. Iniciaremos nosso estudo com as raízes da unidade. Seja ζ uma raiz n -ésima da unidade em $\mathbb{C}$, ou seja, ζ é raiz de $x^n - 1 = 0$. Tomando $\zeta = \exp(2\pi i/n)$, então todas as raízes dessa equação são $\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$. Essas raízes se distribuem no círculo unitário $S^1 \subset \mathbb{C}$ formando os vértices de um polígono regular de n lados. Em grego ciclotomia significa divisão do círculo, daí o nome da classe de corpos que veremos à seguir.

Definição 1. Seja K um corpo. O corpo de decomposição S do polinômio de $f(x) = x^n - 1 \in K[x]$ é dito **extensão ciclotômica de ordem n sobre K** .

Isto significa que para estudarmos extensões ciclotômicas de um corpo precisamos estudar raízes da unidade neste corpo. Para o caso em que $K = \mathbb{C}$ temos uma expressão analítica para todas as soluções de $x^n = 1$, a saber $e^{\frac{2\pi i k}{n}}$ com $0 \leq k \leq n-1$, escrevendo todas elas, vemos que $e^{\frac{2\pi i}{n}}$ é um gerador para este grupo, mas o que acontece quando $K \neq \mathbb{C}$?

A teoria que vamos desenvolver aqui nos permitirá estudar essa questão não apenas em corpos de característica zero, por isso alguns comentários sobre corpos de característica positiva se farão úteis nesse momento.

Seja F um corpo. Considere o homomorfismo $f: \mathbb{Z} \rightarrow F$ tal que $f(n) = n \cdot 1_F$. É claro que f é um homomorfismo e temos duas possibilidades:

Caso 1: f é injetivo Neste caso $\mathbb{Z}$ pode ser mergulhado em F , e $\mathbb{Q}$ também pode ser mergulhado em F . De tado, defina $g: \mathbb{Q} \rightarrow F$ tal que $g\left(\frac{a}{b}\right) = f(a)f(b)^{-1}$. É claro que g é injetivo, e portanto $\mathbb{Q}$ pode ser mergulhado em F . Veremos agora que $\text{Char}(F) = 0$. De fato, como $\mathbb{Q}$ é subcorpo de F segue que não existe inteiro tal que n tal que $n \cdot 1_F = 0$, e portanto $\text{Char}(F) = 0$.

Caso 2: f não é injetivo Neste caso, $\ker f$ é um ideal próprio de $\mathbb{Z}$ e como $\mathbb{Z}$ é domínio de ideais principais, segue que existe $n \in \mathbb{Z}$ tal que $\ker f = (n)$. Vamos ver que n é um número primo. De fato, suponha que

existam $a, b \in \mathbb{Z}$ tal que $n = ab$. Assim, $0 = f(n) = f(a)f(b)$ em F , logo $f(a) = 0$ ou $f(b) = 0$, sem perda de generalidade suponha $f(a) = 0$. Assim $a \in (n)$, logo n divide a logo $n \leq a$ e como $n = ab$ segue que $n \geq a$, então $a = n$, e $b = 1$, e portanto n é primo. Veremos agora que $\text{Char}(F) = n$. De fato, seja $\text{char}(F) = m \neq 0$. Por definição $m \cdot 1_F = 0$ e assim $m \in \ker f = (n)$ assim $n|m$, como $n \cdot 1_F = 0$, temos pela minimalidade de $\text{char}(F)$ que $n = m$.

Isto mostra em particular que a característica de um corpo ou é zero, ou é prima.

Assim temos o seguinte resultado.

Teorema 2. *Seja F um corpo. Então a característica de F é zero, e neste caso $\mathbb{Q} \subset F$, ou é um número primo p e neste caso $\mathbb{F}_p := \mathbb{Z}/(p) \subset F$. Em particular, se F é um corpo finito, então $\text{char}(F) = p$, para algum primo p .*

Voltando ao nosso problema de estudar n -ésimas raízes da unidade sobre o corpo K , a primeira observação é que assumiremos que $n \neq 0$ em K assim, ou a característica de K é zero, ou a característica de K é p tal que p não divide n . Como $x^n - 1$ é relativamente primo com sua derivada nx^{n-1} , temos que $x^n - 1$ é separável em K , isto é, possui n raízes distintas em seu corpo de decomposição. Denotaremos o conjunto das soluções de $x^n - 1$ em K por μ_n . É fácil provar o seguinte resultado.

Teorema 3. *Seja K um corpo, e $n \in \mathbb{Z}$, tal que n não divide $\text{char } K$, ou $\text{char } K = 0$. Então μ_n é um grupo cíclico. Ademais, μ_n é um subgrupo de K^* , o grupo multiplicativo dos elementos não nulos K ,*

Exemplo 1. Se $K = \mathbb{C}$, temos $\mu_1 = \{1\}$, $\mu_2 = \{-1, 1\}$ e $\mu_4 = \{-1, 1, i, -i\}$.

Chamaremos um gerador do grupo μ_n de **raíz primitiva da unidade**, e o denotaremos por ζ_n . Um elemento de μ_n será chamado de **raíz da unidade**. Por exemplo, $1 \in \mu_4$ é raíz da unidade mas não é raíz primitiva da unidade.

Dado $a \in \mathbb{Z}$, a ordem de ζ_n^a é $\frac{n}{\text{mdc}(a, n)}$, então ζ_n^a é uma raíz primitiva da unidade se, e somente se, $\text{mdc}(a, n) = 1$. E portanto o número de raízes primitivas da unidade em $(\mathbb{Z}/n\mathbb{Z})^*$ é a quantidade de números a , menores ou iguais à n , que são coprimos com a . Para cada n , denotaremos esse número

por $\varphi(n)$. Essa função é bem conhecida, e tem o nome de **função totiente de Euler**.

Como não há um gerador único para o μ_n , para $n \geq 2$, fixar ζ_n exige uma escolha. No entanto, em se tratando de extensões do tipo $K(\zeta_n)$, como duas raízes primitivas são potências umas das outras, temos que $K(\zeta_n)$ é independente da escolha de gerador.

Nosso próximo passo será estudar o grupo de Galois de extensões do tipo $K \subset K(\zeta_n)$.

Em geral, mesmo para extensões galoisianas, não há um método para computarmos explicitamente o grupo de Galois. Veremos a seguir, como computar o grupo de Galois de extensões clicotômicas.

Para isso precisaremos da seguinte noção. Para cada n inteiro positivo, podemos definir o grupo

$$(\mathbb{Z}/(n))^* := \{a + (n) \in \mathbb{Z}/(n); \text{ existe } b + (n) \in \mathbb{Z}/(n); a \cdot b + (n) = 1 + (n)\}.$$

É fácil ver que a ordem do grupo multiplicativo $(\mathbb{Z}/(n))^*$ é $\varphi(n)$.

Lema 4. *Seja K um corpo, e $n \in \mathbb{Z}$, tal que $\text{char } K$ não divide n , ou $\text{char } K = 0$. Então para cada $\sigma \in \text{Gal}(K(\zeta_n)/K)$, existe $a \in \mathbb{Z}$ tal que $\sigma(\zeta) = \zeta^a$ para todo $\zeta \in \mu_n$. Ademais, este a é bem definido módulo n .*

Demonstração. Seja ζ_n um gerador para μ_n . Então $\zeta_n^n = 1$ e $\zeta_n^j \neq 1$ para $1 \leq j \leq n-1$, isto significa que $\sigma(\zeta_n) = \zeta_n^a$ para algum a tal que $\text{m.d.c.}(a, n) = 1$. Agora, para todo $a \in \mu_n$, temos:

$$\sigma(\zeta) = \sigma(\zeta_n^k) = \sigma(\zeta_n)^k = (\zeta_n^a)^k = (\zeta_n^k)^a = \zeta^a$$

como queríamos. Para ver que a é bem definido módulo n , note que $\zeta_n^a = \zeta_n^b$ se, e somente se $a \equiv b \pmod{n}$ □

Com isso podemos provar o nosso primeiro resultato.

Teorema 5. *Seja K um corpo, e $n \in \mathbb{Z}$, tal que n não divide $\text{char } K$, ou $\text{char } K = 0$. Então existe um monomorfismo de grupos*

$$\Psi : \text{Gal}(K(\zeta_n)/K) \rightarrow (\mathbb{Z}/(n))^*$$

Demonstração. Pelo lema anterior, para cada $\sigma \in \text{Gal}(K(\zeta_n)/K)$, existe único $a \in \mathbb{Z}/(n)$, com $\text{mdc}(a, n) = 1$ tal que $\sigma(\zeta) = \zeta^a$, logo podemos definir $\Psi(\sigma) = a$. Como σ é unicamente determinado pelo seu valor em ζ_n temos que Ψ é injetor. $\square$

A primeira conclusão que tiramos deste teorema é que o grupo de Galois de uma extensão ciclotômica é sempre abeliano.

Definição 6. Seja $K \subset L$ uma extensão de corpos. Diremos que esta extensão é **cíclica** se $\text{Gal}(L/K)$ é cíclica, e que a extensão é **abeliana** se $\text{Gal}(L/K)$ é abeliano.

É um problema não trivial decidir se dado uma extensão de corpos $K \subset L$ ela é cíclica ou abeliana, mas as extensões ciclotômicas nos fornecem exemplos.

Exemplo 2. Pelo Teorema 5, toda extensão ciclotômica de corpos é abeliana, uma vez que o grupo de Galois pode ser mergulhado em um grupo abeliano. E se p é um número primo, então ζ_p uma raiz primita da unidade então $K \subset K(\zeta_p)$ é uma extensão cíclica, uma vez que $\text{Gal}(K(\zeta_p)/K)$ é isomorfo a um subgrupo do grupo cíclico $\mathbb{Z}/(p)$

Existem exemplos de corpos K tal que o homorfismo dado pelo Teorema 5 não é sobrejetivo. De fato, se $K = \mathbb{R}$, e $n = 5$ então $R(\zeta_5) = R(i) = \mathbb{C}$, e como $|\text{Gal}(\mathbb{C}/\mathbb{R})| = 2$, temos que $\Psi : \text{Gal}(\mathbb{C}/\mathbb{R}) \rightarrow \mathbb{Z}/(5)$ não pode ser sobrejetivo. Deste modo, para explorarmos exemplos onde Ψ é sobrejetiva, precisamos estudar condições especiais do corpo K .

Um caso de especial interesse é quando $K = \mathbb{Q}$, uma vez que estaremos interessados em estudar quando um polômio $f \in \mathbb{Q}[x]$ poderá ser resolvido por meio de radicais, uma vez que esses foram os problemas que motivaram a teoria de Galois.

Relembraremos o Lema de Gauss e um de seus corolários para conveniência do leitor.

Lema 7 (Lema de Gauss). *Sejam $f(x), g(x) \in \mathbb{Z}[x]$ tais que os coeficientes de $f(x)$ são coprimos entre si, e o mesmo acontece para g . Então os coeficientes de $f.g(x)$ também são coprimos entre si.*

Lema 8. *Seja $f \in \mathbb{Z}[x]$ um polinômio mônico de grau positivo n , e seja p um primo. Seja f_p o polinômio mônico cujas raízes são as potências p -ésimas das raízes de f , então:*

- a) $f_p \in \mathbb{Z}[x]$;
- b) $f(x) \equiv f_p(x) \pmod{p}$

Teorema 9. *Seja n um inteiro positivo, e ζ_n uma raiz primitiva da unidade. Então existe um isomorfismo entre $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $(\mathbb{Z}/(n))^*$.*

Demonstração. Considere o mapa $\Psi : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \rightarrow (\mathbb{Z}/(n))^*$ dado pelo Teorema 5, Temos que $\Psi(\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})) \subseteq (\mathbb{Z}/(n))^*$. Vamos provar que $|\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |(\mathbb{Z}/(n))^*| = \varphi(n)$.

Seja $f \in \mathbb{Q}[x]$ o polinômio mínimo de ζ_n sobre $\mathbb{Q}$. Nosso objetivo será provar que para todo $a \in \mathbb{Z}$ tal que a não divide n , então ζ_n^a também é raiz de f . O primeiro passo será mostrar que se $p \in \mathbb{Z}$ primo tal que p não divide n , ζ_n^p também é raiz de f . Como f divide $x^n - 1$, temos que existe $g \in \mathbb{Q}[x]$ tal que $x^n - 1 = f(x)g(x)$. Como o coeficiente líder de $x^n - 1$ e f é 1, segue que o coeficiente líder de g também é 1, e Pelo Lema de Gauss segue que $f, g \in \mathbb{Z}[x]$. Assuma que ζ_n^p não é raiz de f . Então ζ_n^p é raiz de g . Seja $\tilde{g}$ o polinômio tal que $\tilde{g}(x) = g(x^p)$. Temos que $\tilde{g} \in \mathbb{Z}[x]$ e que ζ_n é raiz de $\tilde{g}$, logo existe $h \in \mathbb{Q}[x]$ tal que $\tilde{g} = f.h$, (pela minimalidade de f) o que implica que $h \in \mathbb{Z}[x]$. Pelo Lema 8 temos que $g(x) \equiv \tilde{g}(x) \pmod{p}$ Assim $g(x) \equiv \tilde{g}(x)$ em $\mathbb{F}_p$ e então $x^n - 1 = f(x)\tilde{g}(x)$ em $\mathbb{F}_p$.

Como ζ_n é raiz de f e de $\tilde{g}$, temos que ζ_n é uma raiz múltipla de $x^n - 1$. Como p não divide n temos que $x^n - 1$ e sua derivada nx^{n-1} são coprimos e portanto $x^n - 1$ não admite raiz múltipla em $\mathbb{F}_p$, o que é uma contradição.

Assim ζ_n^p também é raiz de f . Como p é arbitrário, temos que para todo p que não divide n , ζ_n^p é raiz do polinômio minimal de ζ_n .

Agora, se p_1 e p_2 são primos que não dividem n , temos que $\zeta_n^{p_1}$ é raiz de f , e pelo que acabamos de provar, temos que $(\zeta_n^{p_1})^{p_2} = \zeta_n^{p_1 p_2}$ também é raiz de f . Logo se a é um inteiro menor que n que é coprimo com n , a admite uma decomposição $a = p_1 p_2 \cdots p_s$, com p_i 's primos, possivelmente repetidos, tais que ζ^a também é raiz de f . Pelo Teorema 3, temos que μ_n é cíclico, e portanto todas as raízes de f serão da forma ζ^a para algum a coprimo com n , deste modo, temos que o grau de f é $\varphi(n)$ e assim $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, e portanto $|\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n)$. Logo $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/(n))^*$. $\square$

Corolário 10. *Seja p um número primo. Então $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ é um grupo cíclico, e portanto $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ é uma extensão cíclica.*

A demonstração do Teorema 9, motiva a seguinte definição.

Definição 11. Seja K um corpo, e n um número inteiro positivo. O polinômio

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ raiz } n\text{-ésima} \\ \text{primitiva da unidade}}} (x - \zeta) = \prod_{p; p \text{ é coprimo com } n} (x - \zeta_n^p)$$

é dito **n -ésimo polinômio ciclotômico**.

A demonstração anterior mostra que Φ_n é o polinômio minimal irreduzível de uma raiz n primitiva da unidade e que Φ_n é separável sobre $\mathbb{F}_p$ para todo p que não divide n . Não existe uma fórmula fechada para uma expressão de Φ_n . Por exemplo $\Phi_2(x) = x + 1$, $\Phi_3(x) = 1 + x + x^2$, mas $\Phi_8(x) = x^4 + 1$. Mas ele pode ser calculado de maneira indutiva, usando-se o seguinte resultado.

Lema 12. *Seja n um inteiro positivo. Então*

$$x^n - 1 = \prod_{d; d|n} \Phi_d(x).$$

Também é importante notar que outros inteiros diferentes de -1 e 1 podem aparecer como coeficientes de Φ_n . Por exemplo, -2 é o coeficiente de x^{41} em Φ_{105} .

Podemos provar o seguinte Teorema

Teorema 13. *Seja K um corpo que contém uma raiz n -ésima primitiva da unidade, e $f(x) = x^n - c \in K[x]$. Se L é um corpo de raízes para $f(x)$ então existe um monomorfismo de grupos*

$$\Psi : \text{Gal}(L/K) \rightarrow \mathbb{Z}/(n)$$

Mais ainda, Ψ é isomorfismo, se, e somente se, f é irredutível.

Demonstração. Seja $\alpha \in L$ uma raiz de f , e ζ_n uma raiz primitiva da unidade. todas as raízes de f são $\alpha, \alpha\zeta_n, \dots, \alpha\zeta_n^{n-1}$. Logo $L = K(\alpha)$.

Cada $\sigma \in \text{Gal}(L/K)$, é dado por $\sigma(\alpha) = \alpha\zeta_n^i$, pois os automorfismos de L que fixam K levam raiz de f em raiz de f . Deste modo, definimos $\Psi : \text{Gal}(L/K) \rightarrow \mathbb{Z}/(n)$, tal que $\Psi(\sigma) = [i]$

Assim, pelo Lema 4, para cada $\sigma \in \text{Gal}(L/K)$, existe único $i \in \mathbb{Z}/(n)$ tal que $\sigma(\alpha) = \alpha\zeta_n^i$ temos que Ψ está bem definida módulo n , e é óbvio que é um homomorfismo. Como σ é unicamente determinado pelo seu valor em α temos que Ψ é injetor.

Se f é irredutível, com o f é mônico, segue que é o polinômio minimal de α , assim $[L : K] = n = |\text{Gal}(L/K)| = |\mathbb{Z}/(n)|$, e portanto Ψ é sobrejetivo.

Se Ψ é sobrejetivo, segue que $n = |\text{Gal}(L/K)| = |\mathbb{Z}/(n)| = [L : K]$ e como f é raiz de α de grau n segue que ele é o polinômio mínimo de α e portanto é irredutível. $\square$

Corolário 14. *Seja p um primo, e K um corpo contendo uma raiz primitiva p -ésima da unidade, e seja $f(x) = x^p - c \in K[x]$, com corpo de decomposição L . Então ou f possui fatores lineares, e neste caso $|\text{Gal}(L/K)| = 1$ ou f é irredutível e $|\text{Gal}(L/K)| = p$, e portanto $K \subset L$ é uma extensão cíclica.*

Solubilidade por meio de radicais

À seguir veremos como a teoria de Galois nos auxilia a determinar critérios para que as raízes de um polinômio sejam expressas por meio de radicais.

Para isto vamos começar relembrando alguns conceitos de teoria de grupos que se farão necessários.

Definição 15. Um grupo G é dito **solúvel** se existe um cadeia de subgrupos

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G,$$

tal que para todo $i = 0, 1, \dots, n$ tem-se:

1. G_i é normal em G_{i-1} ;
2. G_{i-1}/G_i é abeliano.

Exemplo 3. Todo grupo abeliano é solúvel.

Definição 16. Uma extensão $K \subset F$ é chamada **extensão radical** se existem $\alpha_1, \dots, \alpha_r \in F$ e inteiros positivos $n_1, \dots, n_r$ tais que

1. $F = K(\alpha_1, \dots, \alpha_r)$;
2. $\alpha_1^{n_1} \in K, \alpha_j^{n_j} \in K(\alpha_1, \dots, \alpha_{j-1})$ para $1 < j \leq r$.

Exemplo 4. Suponhamos que uma raiz α de um polinômio $f(x) \in \mathbb{Q}[x]$ seja expressa por meio dos seguintes radicais:

$$\alpha = \frac{\sqrt[5]{2 - \sqrt[3]{2}} + \sqrt{3}}{\sqrt[7]{1 - \sqrt[4]{5}}}.$$

Se denotarmos $a_1 = \sqrt[4]{5}, a_2 = \sqrt[7]{1 - a_1}, a_3 = \sqrt[3]{2}, a_4 = \sqrt[5]{2 - a_3}$ e $a_5 = \sqrt{3}$, teremos:

$$\mathbb{Q} \subset \mathbb{Q}(a_1, a_2, a_3, a_4, a_5)$$

uma extensão radical

Definição 17. Seja K um corpo. Um elemento $z \in \overline{K}$ é **exprimível por radicais** sobre K se existir uma extensão radical $K \subset F$ tal que $z \in F$

Exemplo 5. As raízes da unidade são expremíveis por radicais.

Note que se K é um corpo, e existe a em alguma extensão de K tal que $a^n \in K$, então $K \subset K(a)$ é radical, suponha que $n = pq$, com p, q números primos. Então se fizermos $b = a^p$, temos uma extensão radical $K \subset K(a) \subset K(a, b)$, com $a^p = b$, e $b^q = a^{pq} = a^n \in K$. **Assim, podemos supor que os números n_j aparecendo em uma extensão radical são sempre primos.**

Dado um polinômio irredutível $f(x) \in K[x]$, se uma das raízes é esprimível por radicais, o teorema a seguir garante que as demais raízes também.

Teorema 18. *Seja $f(x) \in K[x]$ um polinômio irredutível. Se uma das raízes de f é esprimível por radicais, então todas as demais raízes também serão esprimíveis por radicais.*

Demonstração. Sejam $\alpha \in L$ uma raiz de $f \in K[x]$ esprimível por radicais, $K \subset L$ uma extensão radical e β outra raiz de f . Seja F o corpo de decomposição de f sobre $K(\alpha)$ e F' o corpo de decomposição de f sobre $K(\beta)$. Considere o homomorfismo de corpos $\tau : K(\alpha) \rightarrow K(\beta)$ que fixa os elementos de K e $\tau(\alpha) = \beta$, e considere $\sigma : F \rightarrow F'$ seu levantamento. Como $K \subset L$ é extensão radical, existem $\alpha_1, \dots, \alpha_r \in \overline{K}$ e também $n_1, \dots, n_r \in \mathbb{Z}$ tais que $K_0 = K \subset K_1 = K(\alpha_1) \subset \dots \subset K(\alpha_1, \dots, \alpha_r) = L$, tal que $\alpha_j^{n_j} \in K_{j-1}$ para todo j . Assim $K_j \subset L$ para todo j . Afirmamos que $K = K_0 \subset \sigma(K_1) \subset \dots \subset \sigma(L)$ é um extensão radical com $\beta \in \sigma(L)$. De fato, como $\sigma(K_j) = K(\sigma(\alpha_1), \dots, \sigma(\alpha_j))$, vale que $\sigma(\alpha_j)^{n_j} = \sigma(\alpha_j^{n_j}) \in \sigma(K_{j-1})$ pois $\alpha_j^{n_j} \in K_{j-1}$. Assim $K = K_0 \subset \sigma(K_1) \subset \dots \subset \sigma(L)$ é uma extensão radical com $\beta = \sigma(\alpha) \in \sigma(L)$. $\square$

Os seguintes Lemas serão importantes.

Lema 19. *Seja $K \subset F$ uma extensão radical de grau n onde K e F possuem característica zero, existe uma torre radical $K \subset F \subset L$ com a extensão $K \subset L$ galoisiana.*

Demonstração. Provaremos este Lema em passos

Passo 1: Existe L' corpo de decomposição de algum polinômio $f \in K[x]$, tal que $F \subset L'$.

De fato, como $K \subset F$ é finita de grau n , existem $\alpha_1, \dots, \alpha_m$ algébricos sobre K tal que $F = K[\alpha_1, \dots, \alpha_m]$. Seja p_i o polinômio minimal irredutível de α_i sobre K . Seja $f = \prod_{i=1}^m p_i$. Como característica de K é zero segue que cada raiz de p_i é simples e portanto podemos tomar L' como sendo o corpo de decomposição de f .

Passo 2: Existe um corpo de decomposição L tal que $K \subset L$ é radical.

Como L' é corpo de decomposição de um polinômio $f \in K[x]$, a extensão $K \subset L'$ é finita, considere $\{\sigma_1, \dots, \sigma_r\}$ os geradores de $\text{Gal}(L'/K)$.

Como $K \subset F$ é extensão radical, existem $\alpha_1, \dots, \alpha_s \in \overline{K}$ elementos tal que $K_0 = K \subset K_1 = K(\alpha_1) \subset \dots \subset K(\alpha_1, \dots, \alpha_s) = F$, tal que $\alpha_j^{n_j} \in K_{j-1}$ para todo j . Como $F \subset L'$, temos que $\sigma_i(\alpha_j)$ está definida para todo i, j . Assim, considere $L = K(\sigma_1(\alpha_1), \dots, \sigma_1(\alpha_s), \dots, \sigma_r(\alpha_1), \dots, \sigma_r(\alpha_s))$. Fixado um i , para todo $j > 1$ vale que

$$\sigma_i(\alpha_j)^{n_j} \in K(\sigma_1(\alpha_1), \dots, \sigma_1(\alpha_s), \dots, \sigma_i(\alpha_1), \dots, \sigma_i(\alpha_{j-1}))$$

e $\sigma_i(\alpha_1) \in K$ para todo i , temos que $K \subset L$ é radical e normal e como K possui característica zero e portanto $K \subset L$ é separável, temos que $K \subset L$ é radical e galoisiana, como queríamos. $\square$

O lemma anterior nos diz que sempre que tivermos uma extensão radical $K \subset L$, com K um corpo de característica zero, então podemos considerar que $K \subset L$ é uma extensão galoisiana. Nosso objetivo será utilizar estudar quando as raízes de um polinômio podem ser exprimíveis por radicais. Deste modo, considere a seguinte definição.

Definição 20. Seja K um corpo e $f \in K[x]$. Dizemos que $f(x)$ é **solúvel por radicais** se existe uma extensão radical $K \subset L$ tal que L contém o corpo de raízes de f .

Exemplo 6. $f(x) = x^n - 1$ é solúvel por radicais em $\mathbb{Q}$.

O seguinte resultado será útil.

Lema 21. Se $K = K_0 \subset K_1 = K(\alpha_1) \subset \dots \subset K_r = K(\alpha_1, \dots, \alpha_r) = L$ é uma extensão radical, satisfazendo:

-
- i) L é o corpo de decomposição de um polinômio em $K[x]$;
 - ii) Para $\alpha_i \in K(\alpha_1, \dots, \alpha_i)$ existe um primo p_i tal que $\alpha_i^{p_i} \in K(\alpha_1, \dots, \alpha_{i-1})$;
 - iii) K contém todas as raízes p_i -ésimas da unidade, para todo i .

Então $\text{Gal}(L/K)$ é solúvel.

Demonstração. Seja $K \subset L$ uma extensão radical satisfazendo os 3 itens do lemma. Defina $G_i = \text{Gal}(K(\alpha_1, \dots, \alpha_r)/K(\alpha_1, \dots, \alpha_i))$. Por hipótese, K contém todas as raízes p_i -ésimas da unidade, então cada $K(\alpha_1, \dots, \alpha_i)$ é o corpo de decomposição de algum polinômio sobre $K(\alpha_1, \dots, \alpha_{i-1})$ (Você sabe qual polinômio?). Assim $K(\alpha_1, \dots, \alpha_{i-1}) \subset K(\alpha_1, \dots, \alpha_i)$ é de Galois e em particular normal. Pela Proposição 22 das notas de aula da semana anterior, temos que $G_{i-1}/G_i \simeq \text{Gal}(K(\alpha_1, \dots, \alpha_i)/K(\alpha_1, \dots, \alpha_{i-1}))$, e pelo Corolário 14, segue que $|\text{Gal}(K(\alpha_1, \dots, \alpha_i)/K(\alpha_1, \dots, \alpha_{i-1}))| = p_i$ e portanto é cíclico, logo abeliano. Assim, temos que $\text{Gal}(L/K) = G_0 \supset G_1 \supset \dots \supset G_r = \{1_L\}$ é uma cadeia de grupos, com G_i normal em G_{i-1} , e G_{i-1}/G_i abeliano. Assim $\text{Gal}(L/K)$ é solúvel. $\square$

Agora veremos como usar este lema para determinar um critério para quando um corpo de raízes de um polinômio não admite extensões radicais.

Teorema 22. *Sejam K um corpo de característica 0 e $f \in K[x]$ um polinômio irredutível, e L seu corpo de decomposição. Se f é esprimível por radicais, então $\text{Gal}(L/K)$ é um grupo solúvel.*

Demonstração. Como K tem característica 0 e f é irredutível, segue do Lema 19 que podemos supor $K \subset L'$ galoisiana, com $L \subset L'$ assim $K \subset L'$ satisfaz i) do Lema 21, para algum polinômio $h(x) \in K[x]$ e sempre podemos supor que uma extensão radical satisfaz ii) do Lema 21.

Deste modo, considere a extensão radical

$$K_0 = K \subset K(\alpha_1) \subset \dots \subset K(\alpha_1, \dots, \alpha_r) = L' \quad (1)$$

com $[K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})] = p_i$ satisfazendo i e ii) do Lemma 21. Vamos construir uma extensão satisfazendo iii). Seja m o mínimo múltiplo comum de todos p_i , e ζ_m uma raiz primitiva m -ésima da unidade.

A torre de extensões (1)

$$K_0 = K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \dots, \alpha_r) = L' \subset L'(\zeta_m)$$

podemos aplicar novamente o mesmo argumento anterior para obter uma extensão

$$K_0 = K \subset K'_1 = K(\alpha'_1) \subset \cdots \subset K'_r = K(\alpha'_1, \dots, \alpha'_r) = L' \subset L'(\zeta_m)$$

com $[K(\alpha'_1, \dots, \alpha'_i) : K(\alpha'_1, \dots, \alpha'_{i-1})] = p'_i$. Observe que L' é o corpo de decomposição de $g(x) = (x^n - 1)h(x)$. Podemos construir uma nova extensão adjuntando ζ_m primeiro

$$K_0 = K \subset K(\zeta_m) \subset K'_1 = K(\zeta_m, \alpha'_1) \subset \cdots \subset K'_r = K(\zeta_m, \alpha'_1, \dots, \alpha'_r) = L'(\zeta_m)$$

note que ainda temos que a torre é radical, e que o corpo de decomposição de f satisfaz $L \subset L' \subset L'(\zeta_m)$.

Agora como $K \subset K(\zeta_m)$, e $K(\zeta_m)$ é o corpo de decomposição de $x^n - 1 \in K[x]$, temos que $K \subset K(\zeta_m)$ é normal, e como temos a torre $K \subset K(\zeta_m) \subset K'_r$ com $K(\zeta_m) \subset K'_r$ normal, temos pela Proposição 22 das notas da semana passada que

$$\text{Gal}(K'_r/K)/\text{Gal}(K'_r/K(\zeta_m)) \simeq \text{Gal}(K(\zeta_m)/K)$$

Agora $\text{Gal}(K(\zeta_m)/K)$ é abeliano pelo Teorema 5, e portanto solúvel.

A torre

$$K(\zeta_m) \subset K'_1 = K(\zeta_m, \alpha'_1) \subset \cdots \subset K'_r = K(\zeta_m, \alpha'_1, \dots, \alpha'_r) = L'(\zeta_m)$$

satisfaz todas as condições do Lema 21, e assim $\text{Gal}(K'_r/K(\zeta_m))$ é solúvel, isso implica que $\text{Gal}(K'_r/K)$ é solúvel (Sejam G grupo e H subgrupo normal

G é solúvel se e só se H e G/H são solúveis).

Por fim, considere a torre de extensões $K \subset L \subset K'_r$. Como L e K'_r são corpos de decomposição de polinômios em $K[x]$, temos novamente da Proposição 22 das notas da semana passada que $\text{Gal}(L/K) \simeq \text{Gal}(K'_r/K)/\text{Gal}(K'_r/L)$, e como $\text{Gal}(K'_r/K)$ é solúvel temos que $\text{Gal}(L/K)$ é solúvel como queríamos. $\square$

É deste resultado que vem a etimologia de grupo solúvel na teoria de grupos. Além disso, é central para a prova da existência de polinômios que não são esprimíveis por radicais. Relembremos o seguinte resultado da teoria de Galois.

Proposição 23. *Seja K um corpo, e G um subgrupo finito do grupo de automorfismos de K . Então existe um corpo $L := \{x \in \overline{K}; \sigma(k) = k \ \forall \ \sigma \in G\}$ tal que $\text{Gal}(L/K) \simeq G$. Dizemos que L é o corpo fixo de K por G .*

Além disso, relembremos alguns conceitos de polinômios simétricos.

Seja K um corpo e $\{x_1, \dots, x_n\}$ variáveis sobre K . Considere o corpo de adjunção $K(x_1, \dots, x_n)$, e $f(y) = \prod (y - x_i) \in K(x_1, \dots, x_n)[y]$. Desenvolvendo f temos $f(y) = y^n - \omega_1 y^{n-1} + \dots + (-1)^n \omega_n$, onde os ω_i são os polinômios simétricos elementares dados pelas expressões

$$\begin{aligned}\omega_1 &= (x_1 + x_2 + \dots + x_n) \\ \omega_2 &= \sum_{1 \leq i < j \leq n} x_i x_j \\ \omega_r &= \sum_{1 \leq i_1 < i_2 < \dots < i_r \leq n} x_{i_1} \dots x_{i_r} \\ \omega_n &= (x_1 x_2 \dots x_n)\end{aligned}$$

O polinômio f é chamado **polinômio universal de grau n** . Nosso objetivo será provar que o Grupo de Galois do corpo de decomposição do polinômio universal é isomorfo a S_n .

Seja $G = S_n$ o grupo de permutações em n objetos. Como $K(x_1, \dots, x_n)$ é corpo de adjunção temos que S_n é um subgrupo do grupo de automorfismos

de $K(x_1, \dots, x_n)$, e portanto considere o corpo F , fixo de $K(x_1, \dots, x_n)$ por G . Temos pela Proposição 23 que $\text{Gal}(K(x_1, \dots, x_n)/F) \simeq G$. Precisaremos do seguinte teorema:

Teorema 24 (Teorema Fundamental dos Polinômios Simétricos). *Qualquer polinômio simétrico em $K[x_1, \dots, x_n]$, pode ser escrito como polinômio nas variáveis $\omega_1, \dots, \omega_n$ com coeficientes em K .*

Como $s_j \in F$, temos que $f(y) \in F[y]$, assim, $K(x_1, \dots, x_n)$ é o corpo de decomposição de f sobre o corpo $K(\omega_1, \dots, \omega_n)$, e assim

$$[K(x_1, \dots, x_n) : K(\omega_1, \dots, \omega_n)] \leq n!$$

Pelo Teorema anterior, temos que $K(\omega_1, \dots, \omega_n) \subset F$, e como $[K(x_1, \dots, x_n) : F] = n!$ assim $[K(\omega_1, \dots, \omega_n) : F] = 1$, e além disso

$$[K(x_1, \dots, x_n) : K(\omega_1, \dots, \omega_n)] = n!$$

Logo $K(\omega_1, \dots, \omega_n) \subset K(x_1, \dots, x_n)$ é uma extensão finita, cujo grupo de Galois é S_n , e $K(x_1, \dots, x_n)$ é o corpo de decomposição de $f(y) = y^n - \omega_1 y^{n-1} + \dots + (-1)^n \omega_n$.

Se supormos que K tem característica 0, pelo Teorema 22 e lembrando que S_n não é solúvel para $n \geq 5$ temos que f **NÃO** é esprimível por radicais. Assim provamos o

Teorema 25 (Abel-Rufini (1824)). *Seja K um corpo e $\{x_1, \dots, x_n\}$ variáveis algebricamente independentes sobre K , então nenhuma raiz do polinômio universal de grau n , para $n \geq 5$ não pode ser esprimível por radicais.*

O Teorema de Abel Rufini implica então que não existe uma fórmula geral que possa ser expressa por meio de radicais, para encontrar as raízes de um polinômio de grau maior ou igual a cinco. Mas é importante ressaltar que isto não significa que nenhum polinômio de grau maior ou igual a cinco pode ser solúvel por radicais. De fato, utilizando a correspondência de Galois, e os mesmos argumentos do Teorema 21 é possível demonstrar que

Teorema 26. *Sejam K um corpo de característica 0 e $f \in K[x]$ um polinômio irredutível, e L seu corpo de decomposição. Se $\text{Gal}(L/K)$ é um grupo solúvel então f é esprimível por radicais.*

Exemplo 7. Seja $f(x) = x^5 - 5x + 12 \in \mathbb{Q}[x]$. Seja L o corpo de decomposição de f sobre $\mathbb{Q}$. É possível mostrar que $\text{Gal}(L/\mathbb{Q}) \simeq D_5$ o grupo diedral de um polígono de cinco lados; Como D_5 é solúvel segue que as raízes de f são esprimíveis por radicais.

Exercícios

1. Calcule Φ_{105} .
2. Descreva todos os corpos intermediários da extensão $\mathbb{Q}(\zeta_7) : \mathbb{Q}$, onde ζ_7 é uma 7-ésima raiz primitiva da unidade.
3. Seja $f(x) = x^5 - 5x + 12 \in \mathbb{Q}[x]$. Prove que o grupo de Galois de f é isomorfo à D_5 .
4. (*) Seja p um número primo, e f um polinômio com coeficientes em $\mathbb{Q}$ tal que f é solúvel por radicais. Prove que f possui 1 ou p raízes reais.
5. (**) Prove que o grupo de Galois do polinômio $x^5 - 20x + 6$ é isomorfo a S_5 . Dica: Estude os sinais das derivadas de f para concluir (usando cálculo diferencial) que f possui exatamente 3 raízes reais, e depois use o fato que se p é primo e $G \leq S_p$ contém um p -ciclo e uma transposição, então $G = S_p$.
6. Você deverá entregar os exercícios 3 e 5.

1 Opcional: Polinômios Simétricos e Identidade de Newton

O estudo de polinômios simétricos está intimamente ligado ao estudo de raízes de equações polinomiais e é uma importante ferramenta para a Teoria

de Galois, e mais recentemente para teoria de representação de álgebras.

Estudaremos nessas notas como os polinômios simétricos apareceram no estudo de equações polinomiais, e apresentaremos alguns resultados interessantes, como a identidade de Newton. Cabe ressaltar, que apesar de terem ficado conhecidas como identidades de Newton, por terem aparecido no livro *Arithmetica Universalis* (1707), elas já foram estudadas por Girard em *Invention nouvelle en algebre* de 1629 e por isso também são conhecidas como relações de Girard.

Considerando um polinômio (mônico, pois sempre podemos dividir o seu coeficiente líder) $f(x) = x^n + \cdots + a_{n-1}x + a_n$, será possível relacionar suas raízes com os coeficientes?

Primeiramente vamos considere um polinômio mônico de grau 3, $f(x) = x^3 + a_1x^2 + a_2x + a_3$, suponha que $\alpha_1, \alpha_2, \alpha_3$ sejam suas raízes. Então $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - (\alpha_1\alpha_2\alpha_3)$. Logo temos

$$\begin{aligned} a_1 &= -(\alpha_1 + \alpha_2 + \alpha_3) \\ a_2 &= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\ a_3 &= -(\alpha_1\alpha_2\alpha_3) \end{aligned}$$

Não é difícil ver que se $f(x) = x^n + \cdots + a_{n-1}x + a_n$ é um polinômio e $\alpha_1, \alpha_2, \dots, \alpha_n$ são suas raízes então

$$a_r = (-1)^r \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq n} \alpha_{i_1} \cdots \alpha_{i_r}$$

E isto motiva a seguinte definição.

Definição 27. Sejam $x_1, \dots, x_n$ variáveis sobre um corpo K , definimos

$$\sigma_r = (-1)^r \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq n} x_{i_1} \cdots x_{i_r}$$

para $1 \leq r \leq n$, onde cada σ_i é dito **polinômio simétrico elementar**.

Observação 28. 1. É claro que $\omega_r \in K[x_1, \dots, x_n]$.

2. Seja $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$, Segue dos nossos comentários que $\sigma_r(\alpha_1, \cdots, \alpha_n) = a_r$.

É importante observar que para estudarmos raízes de polinômios em uma variável, devido aos polinômios simétricos elementares nos deparamos com polinômios em n variáveis. E mais, quando escrevemos que $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ para estudar as raízes de um polinômio f , estamos implicitamente ordenando as raízes (escrevendo que a "primeira" é α_1 por exemplo. Mas é claro que poderíamos considerar qualquer ordenação das raízes. Por isso, estudaremos uma classe de polinômios que passaremos a definir.

Seja $\tau \in S_n$, uma permutação dos inteiros $\{1, \cdots, n\}$. Dado um polinômio $f(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$; Definimos τf como:

$$\tau f(x_1, \cdots, x_n) = f(x_{\tau(1)}, \cdots, x_{\tau(n)}).$$

Se $\tau_1, \tau_2 \in S_n$, então $(\tau_1\tau_2)f = \tau_1(\tau_2f)$. Deste modo podemos ver que S_n opera em $K[x_1, \cdots, x_n]$.

Definição 29. Diremos que $f(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ é **simétrico** se $\tau f = f$, para todo $\tau \in S_n$.

Exemplo 8. $x_1x_2x_3$ é simétrico, mas $x_1x_2^2x_3$ não é. (Agir com (12), (13), (23), (123) (132))

Exemplo 9. σ_i é simétrico para todo i . De fato, considere a identidade $(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n - \sigma_1x^{n-1} + \cdots + (-1)^n\sigma_n$, como o lado esquerdo da igualdade é simétrico, o lado direito também é, e portanto cada σ_i o é.

O primeiro resultado surpreendente que provaremos é que **qualquer** polinômio simétrico pode ser escrito como um polinômio nas variáveis σ'_i s. Este resultado é conhecido como Teorema Fundamental dos Polinômios Simétricos. Para que possamos demonstrá-lo, precisaremos introduzir uma ordem (total) no espaço de todos os polinômios.

Definição 30. Dados dois monômios m_1 e m_2 diremos que $m_1 \prec m_2$ se, e somente se, uma das seguintes condições são satisfeitas

- $\deg m_1 < \deg m_2$;
- $\deg m_1 = \deg m_2$, e existe $j \in \{1, \dots, n\}$ tal que $a_j < b_j$ e $a_i = b_i$ para todo $i < j$

Essa ordem é dita **ordem lexicográfica** nos monômios.

É claro que a ordem lexicográfica define uma ordem total no conjunto dos monômios em n variáveis.

É importante notar que fixado um monômio $x_1^{a_1} \cdots x_n^{a_n}$, existem **finitos** monômios $x_1^{b_1} \cdots x_n^{b_n}$ tal que $x_1^{b_1} \cdots x_n^{b_n} \prec x_1^{a_1} \cdots x_n^{a_n}$.

A partir da ordem lexicográfica nos monômios, podemos definir uma ordem no conjunto de todos os polinômios também. De fato, dado $f \in K[x_1, \dots, x_n]$, f pode ser escrito como soma de monômios, isto é, $f = m_1 + \cdots + m_s$, onde $m_i \in K[x_1, \dots, x_n]$, como a ordem lexicográfica é uma ordem total nos espaços dos monômios, existe um m_{i_0} tal que $m_t \prec m_{i_0}$ para todo $t \in \{1, \dots, s\}$. Diremos que m_{i_0} é o **termo líder** de f . Dados dois polinômios f e g diremos que $f \prec g$ se o termo líder de f é menor que o termo líder de g na ordem lexicográfica.

Exemplo 10. Seja $\omega_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$, o termo líder de ω_2 é x_1x_2 .

Teorema 31 (Teorema Fundamental dos Polinômios Simétricos). *Any symmetric polynomial in $K[x_1, \dots, x_n]$ can be written as a polynomial in $\sigma_1, \dots, \sigma_n$ with coefficients in K .*

Demonstração. Seja $f \in K[x_1, \dots, x_n]$ com coeficiente líder $cx_1^{a_1} \cdots x_n^{a_n}$.

Afirmção 1: $a_1 \geq a_2 \geq \cdots \geq a_n$ Suponha que $a_i < a_{i+1}$, para algum $1 \leq i \leq n-1$. Como f é simétrico, segue que $cx_1^{a_1} \cdots x_i^{a_{i+1}} x_{i+1}^{a_i} \cdots x_n^{a_n}$ também é um termo de f . E como temos que $cx_1^{a_1} \cdots x_i^{a_{i+1}} x_{i+1}^{a_i} \cdots x_n^{a_n}$ e $cx_1^{a_1} \cdots x_i^{a_i} x_{i+1}^{a_{i+1}} \cdots x_n^{a_n}$ possuem o mesmo grau, que os expoentes das variáveis x_1 até x_{i-1} coincidem e que assumimos que $a_i < a_{i+1}$, segue que $cx_1^{a_1} \cdots x_i^{a_i} x_{i+1}^{a_{i+1}} \cdots x_n^{a_n} \prec$

$cx_1^{a_1} \cdots x_i^{a_{i+1}} x_{i+1}^{a_i} \cdots x_n^{a_n}$ o que é uma contradição pois $cx_1^{a_1} \cdots x_i^{a_i} x_{i+1}^{a_{i+1}} \cdots x_n^{a_n}$ é termo líder de f . Logo segue nossa afirmação

Afirmação 2: $g = \sigma_1^{a_1-a_2} \sigma_2^{a_2-a_3} \cdots \sigma_n^{a_n}$ é um polinômio em $K[x_1, \dots, x_n]$ com termo líder $x_1^{a_1} \cdots x_i^{a_i} x_{i+1}^{a_{i+1}} x_n^{a_n}$

Pela afirmação 1) temos que g é polinômio, e como é fável ver que o termo líder de um produto é o produto dos termos líderes, temos a afirmação.

Assim, f e cg têm o mesmo coeficiente líder. E deste modo $f_1 = f - cg$ possui termo líder com coeficiente c_1 e expoentes **estritamente menores** que o expoente de f . Podemos aplicar o mesmo processo e obteremos um $f_2 = f_1 - c_1 g_1$. f_2 novamente possui expoentes extritamente menores que f_1 .

Afirmação 3: O processo descrito acima sempre para. Isto é, existe f_m tal que $f_m = 0$.

De fato, se $f_k \neq 0$ pra todo f_k teríamos uma sequência infinita de moômios com coeficientes estritamente decrescente, mas isso não pode ocorrer. Logo o processo para.

Assim, existem $g_1, \dots, g_m$ onde cada g_i é produto de polinômios simétricos elementares, tal que $f = cg + c_1 g_1 + \cdots c_m g_m$ o que conclui nossa demonstração. $\square$

Dado um polinômio $f \in K[x]$ de grau n seria interessante encontrar um critério para decidir se as raízes de f estão todas contidas em K . Neste sentido, o **discriminante** de f denotado por $\Delta(f)$, e definido como a seguir.

Definição 32. Sejam $r_1, \dots, r_n$ todas as raízes de f contidas em alguma extensão de K . Definimos como **discriminante** de f o número $\Delta(f) := \prod_{1 \leq i < j \leq n} (r_i - r_j)^2$.

É claro que $r_1, \dots, r_n$ estão em K se, e somente se, $\sqrt{\Delta(f)} \in K$, e mais ainda, como $\Delta(f)$ é um polinômio simétrico, temos pelo Teorema fundamental que ele pode ser escrito como combinação linear dos polinômios simétricos elementares, e deste modo, $\Delta(f)$ pode ser escrito em função dos coeficiente de f .

Exemplo 11. Seja $f(x) = ax^2 + bx + c$ com $a \neq 0$. Temos que $f(x) = x^2 + \frac{b}{a}x + \frac{c}{a}$. Assim, temos que $\sigma_1(r_1, r_2) = r_1 + r_2 = -\frac{b}{a}$ e $\sigma_2(r_1, r_2) = r_1 r_2 = \frac{c}{a}$.

Como $\Delta(f) = (r_1 - r_2)^2 = (r_1 + r_2)^2 - 4r_1r_2 = \sigma_1(r_1, r_2)^2 - 4\sigma_2(r_1, r_2) = \frac{b^2 - 4ac}{a^2}$ Temos que $\sqrt{\Delta(f)} \in K$ se, e somente se, $\sqrt{b^2 - 4ac} \in K$, como era esperado.

Muitas vezes ao trabalhar com polinômios não estamos interessado em contrar todas as suas raízes mas sim em encontrar alguma função das raízes como sua soma, ou soma de suas potências.

Para isso, sejam $f \in K[x]$ e $r_1, \dots, r_n$ suas raízes, e considere

$$P_k(r_1, \dots, r_n) = \sum_{i=1}^n r_i^k$$

para $k \in \mathbb{Z}$, positivo. É claro que cada um dos P_j é invariante por S_n , e logo é simétrico. Assim pelo Teorema fundamental, podemos escrever os P_j s como soma de polinômios elementares. As identidades de Newton nos darão esses coeficientes.

Teorema 33 (Identidade de Newton). *Sejam $f \in K[x]$, tal que $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + e$ e $r_1, \dots, r_n$ suas raízes, e considere P_i s como definido acima. Temos a identidade*

$$P_1(r_1, \dots, r_n) = \sigma_1(r_1, \dots, r_n)$$

$$P_k(r_1, \dots, r_n) = \sigma_1 P_{k-1} - \sigma_2 P_{k-2} + \dots + (-1)^{k-1} \sigma_{k-2} P_1 + (-1)^{k-1} k \sigma_k, \text{ se } 1 < k \leq n$$

$$P_k(r_1, \dots, r_n) = \sigma_1 P_{k-1} - \sigma_2 P_{k-2} + \dots + (-1)^{k-1} \sigma_{k-1} P_1 + (-1)^{k-1} \sigma_n P_{n-k}, \text{ se } k \geq n$$

Demonstração. Seja $f(x) = \sum_{i=1}^n (-1)^i \sigma_{n-i} x^i$, e Como cada r_i é raiz de f temos $f(x) = (x - r_1) \cdots (x - r_n)$, derivando formalmente com respeito a x temos que

$$f'(x) = \sum_{i=1}^n \frac{f(x)}{x - r_i}$$

Multiplicando ambos os lados por x^{k+1} temos:

$$x^{k+1} f'(x) = \sum_{i=1}^n \frac{x^{k+1} f(x)}{x - r_i} = \sum_{i=1}^n \frac{(x^{k+1} + \cancel{r_i^{k+1}} - \cancel{r_i^{k+1}}) f(x)}{x - r_i} = f(x) \underbrace{\sum_{i=1}^n \frac{x^{k+1} - r_i^{k+1}}{x - r_i}}_{q(x)} + \underbrace{\sum_{i=1}^n \frac{r_i^{k+1} f(x)}{x - r_i}}_{g(x)}$$

Então

$$x^{k+1}f'(x) = f(x)q(x) + g(x) \quad (2)$$

onde $g(x)$ é um polinômio de grau $n - 1$. Note também que

$$q(x) = \sum_{i=1}^n \frac{x^{k+1} - r_i^{k+1}}{x - r_i} = \sum_{i=1}^n \frac{(x - r_i)(x^k + x^{k-1}r_i + \cdots + xr_i^{k-1} + r_i^k)}{x - r_i} = \sum_{i=1}^n \frac{x^k + x^{k-1}r_i + \cdots + xr_i^{k-1} + r_i^k}{(3)}$$

agrupando as potências de x temos:

$$q(x) = nx^k + x^{k-1}P_1 + \cdots P_k \quad (4)$$

Assim, o coeficiente de x^n no polinômio $f(x)p(x)$ é dado por

$$P_k - \sigma_1 P_{k-1} + \sigma_2 P_{k-2} + \cdots + (-1)^{k-2} \sigma_{k-2} P_1 + (-1)^k n \sigma_k$$

Por outro lado, o coeficiente de x^n em $x^{k+1}f'(x)$ é $(-1)^k(n - k)\sigma_k$ se $1 \leq k \leq n$, e 0 se $k > n$, assim, pela equação (2) temos

$$P_k = \sigma_1 P_{k-1} - \sigma_2 P_{k-2} + \cdots + (-1)^{k-1} \sigma_{k-2} P_1 + (-1)^{k-1} k \sigma_k, \text{ se } 1 < k \leq n$$

$$P_k = \sigma_1 P_{k-1} - \sigma_2 P_{k-2} + \cdots + (-1)^{k-1} \sigma_{k-1} P_1 + (-1)^{k-1} \sigma_n P_{n-k}, \text{ se } k > n$$

O que conclui nossa demonstração. $\square$

Com o auxílio da identidade de Newton, podemos estudar a relação entre raízes de polinômios e seus coeficientes.

Exemplo 12. Seja $p(x) = x^3 + ax + b$, com $a, b \in \mathbb{R}$. Se todas as raízes de p são reais, vamos mostrar que $a \leq 0$. De fato, sejam r_1, r_2, r_3 raízes de p temos pela identidade de Newton que

$$P_2(r_1, r_2, r_3) = \sigma_1(r_1, r_2, r_3)P_1(r_1, r_2, r_3) - 2\sigma_2(r_1, r_2, r_3),$$

mas temos que $\sigma_1(r_1, r_2, r_3) = 0$ e $\sigma_2(r_1, r_2, r_3) = a$, assim temos

$$P_1(r_1, r_2, r_3) = 0$$

$$P_2(r_1, r_2, r_3) = -2a \implies a = -\frac{r_1^2 + r_2^2 + r_3^2}{2},$$

Como cada r_i é real, segue que $a \leq 0$