Corpos Quadráticos e Aplicações

Linara Stéfani Facini & Antonio Aparecido de Andrade

Unesp - Ibilce - Departamento de Matemática

linarafacini@gmail.com

Resumo

Faremos uma breve abordagem sobre os corpos quadráticos. Veremos como são construídos através de teoremas e proposições importantes que direcionam toda a teoria conhecer o anel de inteiros, identificar o grupo de Galois e ver algumas aplicações como norma, traço e discriminante.

Introdução

O matemático francês Évariste Galois (1811-1832) foi o primeiro a unificar a teoria de corpos. A abordagem moderna da teoria de Galois foi desenvolvida por Richard Dedekind, Leopold Kronecker e Emil Artin entre outros, que envolve o estudo de automorfismos de extensões de corpos. Os corpos quadráticos fazem parte desses estudos, que nos proporciona conhecer a sua estrutura.

Objetivos

1. Definir um corpo quadrático e explicitar sua forma.
2. Encontrar o anel de inteiros dos corpos quadráticos.
3. Definir e encontrar o grupo de Galois dos corpos quadráticos.
4. Definir o discriminante o discriminante do anel de inteiros dos corpos quadráticos.

Resultados

Definição: Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos. Um elemento $\alpha \in \mathbb{K}$ é chamado de algébrico sobre $\mathbb{Q}$ se existe um polinômio $f(x) \in \mathbb{Q}[x]$ tal que $f(\alpha) = 0$.

Se $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{Q}$, sempre existe um polinômio $p(x) \in \mathbb{Q}[x]$ que seja mônico e de grau mínimo cujo α é raiz. Esse polinômio será irredutível e o minimal de α.

Definição: Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos e $\alpha \in \mathbb{K}$. Definimos:

1. $\mathbb{Q}(\alpha)$ será definido como o menor corpo que contém $\mathbb{Q}$ e α.
2. $\mathbb{Q}[\alpha]$ será definido como o menor anel que contém $\mathbb{Q}$ e α.

Proposição: Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos e $\alpha \in \mathbb{K}$, então:

1. $\mathbb{Q}(\alpha) = \left\{ \dfrac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in \mathbb{Q}[x] \; e \; g(\alpha) \neq 0 \right\}$.
2. $\mathbb{Q}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Q}[x]\}$.

De imediato temos que $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}(\alpha)$.

Teorema: Consideremos $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos e $\alpha \in \mathbb{K}$. Definimos $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$ por $\varphi(f(x)) = f(\alpha)$, então:

1. φ é um homomorfismo.
2. $\Im(\varphi) = \mathbb{Q}[\alpha]$.
3. $Ker(\varphi) = \{0\} \Leftrightarrow \alpha$ é transcendente.
4. $Ker(\varphi) \neq \{0\} \Leftrightarrow \alpha$ é algébrico.

Teorema: Nas condições do Teorema anterior, seja $Ker(\varphi) \neq \{0\}$, então:

1. $\dfrac{\mathbb{Q}[x]}{Ker(\varphi)} \cong \mathbb{Q}[\alpha]$.
2. $Ker(\varphi) = \langle p(x) \rangle$, sendo $p(x) \in \mathbb{Q}[x]$ o polinômio minimal de α.
3. $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

Proposição: Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos e $\alpha \in \mathbb{K}$ um elemento algébrico sobre $\mathbb{Q}$. O conjunto $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forma uma base para $\mathbb{K}$ sobre $\mathbb{Q}$ e $[\mathbb{K} : \mathbb{Q}] = n$, com $n \in \mathbb{N}$ o grau do polinômio minimal de α.

Definição: Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos, dizemos que $\mathbb{K}$ é um corpo quadrático se $[\mathbb{K} : \mathbb{Q}] = 2$.

Proposição: Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, escrito como $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$, onde d é um inteiro livre de quadrados.

Definição: Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos. O conjunto $\mathcal{O}_{\mathbb{K}}$ é formado por elementos de $\mathbb{K}$ que são algébricos sobre $\mathbb{Q}$. Esse conjunto é um anel e chamamos-o de anel de inteiros de $\mathbb{K}$.

Lema: Seja $\mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde d é um inteiro livre de quadrados. Se $\alpha = a + b\sqrt{d}$ é um inteiro algébrico, então $2a$ e $2b$ são números inteiros.

Teorema: Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados, então o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é dado por:

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z}[\sqrt{d}], \; se \; d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right], \; se \; d \equiv 1 \pmod 4 \end{cases}$$

Definição: Seja $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos. O grupo de Galois é o conjunto de $\mathbb{Q}$-automorfismos de $\mathbb{K}$ que fixam os elementos de $\mathbb{Q}$. Denotaremos por $Gal(\mathbb{K} : \mathbb{Q})$.

Exemplo: Considere $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados, temos que $Gal(\mathbb{K} : \mathbb{Q}) = \{\sigma_1, \sigma_2\}$, onde σ_1 e σ_2 são $\mathbb{Q}$-automorfismos definidos por $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$ e $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$, com $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.

Definição: A norma e o traço de um elemento $\alpha \in \mathbb{Q}(\sqrt{d})$, onde d é livre de quadrados, são definidos respectivamente como $N(\alpha) = \alpha\sigma_2(\alpha)$ e $Tr(\alpha) = \alpha + \sigma_2(\alpha)$.

Teorema: Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados e $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$. Assim:

1. Se $d \equiv 2, 3 \pmod 4$, então o discriminante de $\mathcal{O}_{\mathbb{K}}$ é dado por $4d$.
2. Se $d \equiv 1 \pmod 4$, então o discriminante de $\mathcal{O}_{\mathbb{K}}$ é dado por d.

Exemplo: Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, como $5 \equiv 1 \pmod 4$, temos:

$$D_{\mathbb{K}/\mathbb{Q}}\left(1, \frac{1+\sqrt{5}}{2}\right) = \begin{vmatrix} Tr(1) & Tr\left(\frac{1+\sqrt{5}}{2}\right) \\ Tr\left(\frac{1+\sqrt{5}}{2}\right) & Tr\left(\frac{1+\sqrt{5}}{2}\right)^2 \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \frac{1+5}{2} \end{vmatrix} = 5.$$

Conclusão

Os corpos quadráticos e seus automorfismos nos levam ao grupo de Galois. Assim, particularizando a teoria de reticulados para os corpos quadráticos, podemos intervir que na teoria da transmissão de dados, que nos permite minimizar as interferências no sinal e melhorará-lo.

Referências

[1] RIBENBOIN, P., *Classical Theory of Algebraic Numbers*, Springer Verlag, New York, 2001.

[2] SAMUEL, P., *Algebraic Theory of Numbers*, Hermann, Paris, 1982.

[3] WASHINGTON,L., *Introduction to Cyclotomic Fields*, Springer-Verlag, New-York, 1982.

Agradecimentos

PICME PROGRAMA DE INICIAÇÃO CIENTÍFICA E MESTRADO