Revisão: Teoria de Corpos

Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos (ie, $\mathbb{F} \subseteq \mathbb{E}$). Um elemento $\alpha \in \mathbb{E}$ é dito ser algébrico sobre $\mathbb{F}$ se existe $0 \neq f \in \mathbb{F}[X]$ tal que $f(\alpha) = 0$.

O conjunto

$$\{ g \in \mathbb{F}[X] \mid g(\alpha) = 0 \}$$

é um ideal de $\mathbb{F}[X]$. Como $\mathbb{F}[X]$ é DIP, existe um único polinômio mônico que gera o ideal. Tal polinômio é denominado o polinômio minimal de α sobre $\mathbb{F}$, e é denotado por $\mathrm{Irr}(\alpha, \mathbb{F})$.

Def. Uma extensão $\mathbb{E}/\mathbb{F}$ é dita ser algébrica se todo $\alpha \in \mathbb{E}$ é alg. sobre $\mathbb{F}$.

Def. Seja $\mathbb{E}/\mathbb{F}$ algébrica. Dizemos que:

(i) $\mathbb{E}/\mathbb{F}$ é normal se $\mathbb{E}$ contém todas as raízes de $\mathrm{Irr}(\alpha, \mathbb{F})$, $\forall \alpha \in \mathbb{E}$,

(ii) $\mathbb{E}/\mathbb{F}$ é separável se todas as raízes de $\mathrm{Irr}(\alpha, \mathbb{F})$ são simples, $\forall \alpha \in \mathbb{E}$,

(iii) $\mathbb{E}/\mathbb{F}$ é galoisiana se é normal e separável,

(iv) $\mathbb{E}/\mathbb{F}$ é finita se $[\mathbb{E}:\mathbb{F}] := \dim_{\mathbb{F}} \mathbb{E} < \infty$.

Teorema. Se $\mathrm{char}\, F = 0$ então toda ext. alg. é separável.

Exemplo. Seja $F_p = \mathbb{Z}/p\mathbb{Z}$. Seja $F_p(X)$ o corpo de frações de $F_p[X]$. Então $F_p(X)/F_p(X^p)$ não é separável.

Notação. Denota-se

$$\mathrm{Aut}(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma(a) = a, \forall a \in F\},$$

$$\left(= \mathrm{Gal}(E/F) = G(E/F)\right)$$

Teorema. Se E/F é galoisiana e finita então

$$E^{\mathrm{Aut}(E/F)} := \{x \in E \mid \sigma x = x, \forall \sigma \in \mathrm{Aut}(E/F)\} = F.$$

Teorema. Seja E/F ext. alg. Então existe um menor corpo $L \supseteq E$ tal que L/F é normal. Denota-se $L = N(E/F)$. Se $[E:F] < \infty$, então $[L:F] < \infty$.

Corolário. Se $E/\mathbb{Q}$ é finita, então existe $L \supseteq E$, com $L/\mathbb{Q}$ galoisiana e finita.

Teorema (elem. prim.). Se E/F é separável e finita, então existe $\theta \in E$ tal que $E = F(\theta)$. Ainda

$$[E:F] = \mathrm{gr}(\mathrm{Irr}(\theta, F)).$$

Inteiros Algébricos

Def. Seja $\alpha \in \mathbb{C}$. Dizemos que α é um inteiro algébrico se $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]$.

Teorema. α é um inteiro algébrico $\iff$ α é raiz de um polinômio mônico $0 \neq f \in \mathbb{Z}[X]$.

Dem.: ($\Rightarrow$) ok.

($\Leftarrow$) Seja $f \in \mathbb{Z}[X]$ mônico tal que $f(\alpha) = 0$. Seja $g = \mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Q}[X]$, então existe $h \in \mathbb{Q}[X]$ tal que

$$f = gh.$$

Sejam $m, n \in \mathbb{Z}_{>0}$ tais que $mg, nh \in \mathbb{Z}[X]$ sejam primitivos, ou seja, o mdc dos seus coef. é 1.

Daí, obtemos que

$$mnf = (mg)(nh)$$

Afirm. O produto de dois pol. primitivos é primitivo.

De fato, assuma que não. Então existe $p \in \mathbb{N}$ primo que divide os coef. de $(mg)(nh)$. Portanto,

$$(mg)(nh) = 0 \in (\mathbb{Z}/p\mathbb{Z})[X]$$

Como $(\mathbb{Z}/p\mathbb{Z})[X]$ é domínio, segue que ou $mg=0$, ou $nh=0$. Isso contradiz o fato de mg e nh serem primitivos. Isso prova a afirmação.

Daí mnf é primitivo. Assim, $1=mn$. Daí $m=1$.

Portanto, $\mathrm{Irr}(\alpha,\mathbb{Q})=g=m\cdot g\in\mathbb{Z}[X]$. □

Teorema. α é inteiro algébrico $\Leftrightarrow \mathbb{Z}[\alpha]$ é um $\mathbb{Z}$-módulo finitamente gerado.

Dem.: ($\Rightarrow$) Seja $n=\mathrm{gr}(\mathrm{Irr}(\alpha,\mathbb{Q}))$. Então

$$\mathbb{Z}[\alpha]=\mathbb{Z}\cdot 1\oplus\mathbb{Z}\alpha\oplus\mathbb{Z}\alpha^2\oplus\cdots\oplus\mathbb{Z}\alpha^{n-1}.$$

($\Leftarrow$) Assuma que $\mathbb{Z}[\alpha]=\mathbb{Z}\beta_1\oplus\cdots\oplus\mathbb{Z}\beta_s$. Então, $\beta_i=f_i(\alpha)$, com $f_i\in\mathbb{Z}[X]$, p/ todo i. Seja $N\in\mathbb{N}$ tal que $N>\mathrm{gr}\, f_i$. Como $\alpha^N\in\mathbb{Z}[\alpha]$, vale que

$$\alpha^N=a_1\beta_1+\cdots+a_s\beta_s=a_1f_1(\alpha)+\cdots+a_sf_s(\alpha).$$

Daí α satisfaz

$$X^N-\sum_{i=1}^{s}a_if_i(X)\in\mathbb{Z}[X].$$ □

Corolário. Se α e β são inteiros algébricos, então $\alpha-\beta$ e $\alpha\beta$ são inteiros algébricos. □

Def. Um corpo de números algébricos é um corpo K que é uma extensão finita de $\mathbb{Q}$.

Seja $\mathbb{K}$ um corpo de números algébricos. Defina

$$\mathcal{R} = \text{alg. int.}(\mathbb{K}) := \{\alpha \in \mathbb{K} \mid \alpha \text{ é inteiro algébrico}\}.$$

Temos que $\mathcal{R}$ é um anel contendo $\mathbb{Z}$.

Proposição. $\text{Corpo fr.}\,\mathcal{R} = \mathbb{K}$. Ainda mais, dado $a \in \mathbb{K}$, existem $\alpha \in \mathcal{R}$ e $m \in \mathbb{Z}$ tais que $a = \frac{\alpha}{m}$.

Dem.: Sejam $a \in \mathbb{K}$ e $f = \text{Irr}(a, \mathbb{Q})$. Seja $c \in \mathbb{Z}$ tal que $cf \in \mathbb{Z}[X]$ é primitivo, e escreva

$$cf(X) = a_n X^n + \cdots + a_1 X + a_0.$$

Então

$$\begin{aligned} 0 &= a_n^n a^n + a_{n-1} a^{n-2} a_n^{n-1} + \cdots + a_1 a_n^{n-1} a + a_0 a_n^{n-1} \\ &= (a_n a)^n + a_{n-1} a_n (a_n a)^{n-1} + \cdots + a_1 a_n^{n-2} (a_n a) + a_0 a_n^{n-1}. \end{aligned}$$

Portanto, $a_n a \in \mathcal{R}$, e $a_n \in \mathbb{Z}$. ∎

Obs. $\text{alg. int.}\,\mathbb{Q} = \mathbb{Z}$. Mais ainda,

$$\text{alg. int.}(\mathbb{K}) \cap \mathbb{Q} = \mathbb{Z}.$$

Teorema. Sejam $\mathbb{K}$ um corpo de números algébricos e $\mathcal{R} = \text{alg. int.}(\mathbb{K})$. Então $\mathcal{R}$ é um $\mathbb{Z}$-módulo fin. gerado, $[\mathcal{R} : \mathbb{Z}] = \operatorname{rank}_{\mathbb{Z}} \mathcal{R} = [\mathbb{K} : \mathbb{Q}]$.

Dem.: Temos que $\mathbb{K} = \mathbb{Q}(\gamma)$ (por Teorema do Elemento Primitivo). Então, existe $m \in \mathbb{Z}$ t.q. $\alpha = m\gamma \in \mathcal{R}$. Então $\mathbb{K} = \mathbb{Q}(\alpha)$. Sejam $n = [\mathbb{K} : \mathbb{Q}]$, $\mathbb{L} = N(\mathbb{K}/\mathbb{Q})$ e

$$\sigma_1, \dots, \sigma_n \in \operatorname{Aut}(\mathbb{L}/\mathbb{Q})$$

tais que $\{\sigma_1\alpha, \dots, \sigma_n\alpha\}$ são as raízes de $\operatorname{Irr}(\alpha, \mathbb{Q})$. Denote $\alpha_i := \sigma_i \alpha$. Temos que $\alpha_i \neq \alpha_j$ se $i \neq j$.

Defina $A = (\alpha_i^j)_{(i,j)}$. Então

$$0 \neq \det A = \prod_{i<j} (\alpha_i - \alpha_j)$$

é soma e diferença de produto dos α_i. Como cada α_i é int. alg. (pois é raiz de $\operatorname{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$), segue que $\det A$ é um int. alg. Tome

$$c = (\det A)^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Dado $\sigma \in Aut(L/\mathbb{Q})$, $\sigma(\det A)^2 = (\det A)^2$.
Portanto, $c = \det A^2 \in \mathbb{Q}$. Portanto, $c \in \mathbb{Z}$.

Seja $\beta \in R$. Então

$$\beta = \sum_{i=0}^{n-1} b_i \alpha^i, \quad b_0, \dots, b_{n-1} \in \mathbb{Q}.$$

Então,

$$\beta_j := \sigma_j \beta = \sum_{i=0}^{n-1} b_i \alpha_j^i.$$

Portanto, obtemos

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = A \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

Daí

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \frac{1}{\det A} \operatorname{ad} A \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

As entradas de $\operatorname{ad} A$ são inteiras alg. Ainda, como β é int. alg, segue que $\beta_1, \dots, \beta_n$ são int. alg. Portanto, cb_i é um inteiro alg. Além disso, $cb_i \in \mathbb{Q}$. Daí $cb_i \in \mathbb{Z}$.

Assim, $c\beta = \sum_{i=0}^{n-1} (cb_i)\alpha^i \in \mathbb{Z}[\alpha]$.

Daí, vale que $\mathcal{R} \subseteq c^{-1}\mathbb{Z}[\alpha]$. Portanto, como $c^{-1}\mathbb{Z}[\alpha]$ é $\mathbb{Z}$-fin. gerado, vale que $\mathcal{R}$ é $\mathbb{Z}$-fin. gerado.

Por fim, uma $\mathbb{Z}$-base de $\mathcal{R}$ é uma $\mathbb{Q}$-base de K (exercício). Portanto, $[\mathcal{R}:\mathbb{Z}] = [K:\mathbb{Q}]$. □