Revisão: extensão de corpos

Def. Uma extensão de corpos $\mathbb{E} \supseteq \mathbb{F}$ é dito ser separável se, $\forall a \in \mathbb{E}$, o polinômio minimal $Irr(a, \mathbb{F})$ é separável (isto é, todas as suas raízes são simples).

Def. Um corpo $\mathbb{F}$ é perfeito se $char\,\mathbb{F} = 0$ ou $char\,\mathbb{F} = p > 0$ e $\mathbb{F}^p = \mathbb{F}$.

Teorema. Um corpo $\mathbb{F}$ é perfeito se, e somente se, toda extensão algébrica $\mathbb{E}/\mathbb{F}$ (ie, $\mathbb{F} \leq \mathbb{E}$) é separável.

Exemplo. Todo corpo finito é separável.

Lema. Seja $f \in \mathbb{F}[X]$ irredutível e não separável. Então $char\,\mathbb{F} = p > 0$, e existe $g \in \mathbb{F}[X]$ tal que $f(X) = g(X^p)$.

Teorema. Sejam $\mathbb{L} \supseteq \mathbb{E} \supseteq \mathbb{F}$ corpos. Então $\mathbb{L}/\mathbb{F}$ é separável $\Leftrightarrow$ $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são separáveis.

Def. Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita de corpos. Cada $\alpha \in \mathbb{E}$ define um mapa $\mathbb{F}$-linear $R_\alpha : \mathbb{E} \to \mathbb{E}$ via multiplicação por α (em que $\mathbb{E}$ é um $\mathbb{F}$-espaço vetorial). Define-se

$$tr_{\mathbb{E}/\mathbb{F}}(\alpha) = tr(R_\alpha).$$

Teorema. Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita. Então $\mathbb{E}/\mathbb{F}$ é separável se e somente se $z \in \mathbb{E}$ tal que $tr_{\mathbb{E}/\mathbb{F}}(z) \neq 0$.

Extensão separável do corpo base

Exemplos.

(i) Seja $\mathbb{F} = \mathbb{F}_p(t)$, em que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, e t é transcendente sobre $\mathbb{F}_p(t)$. Seja $\mathbb{E} = \mathbb{F}(t^{1/p}) = \mathbb{F}[X]/(X^p - t)$.

Então $A = \mathbb{E}$ é uma $\mathbb{F}$-álgebra simples. Entretanto,

$$0 \neq t^{1/p} \otimes 1 - 1 \otimes t^{1/p} \in A^{\mathbb{E}} = \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}$$

Além disso,

$$\left(t^{1/p} \otimes 1 - 1 \otimes t^{1/p}\right)^p = \left(t^{1/p} \otimes 1\right)^p - \left(1 \otimes t^{1/p}\right)^p = t \otimes 1 - 1 \otimes t = 0.$$

Portanto, $t^{1/p} \otimes 1 - 1 \otimes t^{1/p} \in J(A^{\mathbb{E}})$. Portanto, $A^{\mathbb{E}}$ não é uma $\mathbb{E}$-álgebra semissimples.

(ii) Seja $\mathbb{E} \supseteq \mathbb{F}$ uma extensão não separável. Então, existe $\alpha \in \mathbb{E}$ tal que $f = Irr(\alpha, \mathbb{F})$ é não separável.

Daí, existe $g(X) = a_m X^m + \cdots + a_1 X + a_0 \in \mathbb{F}[X]$ tal que $f(X) = g(X^p)$. Então $a_m \alpha^{pm} + \cdots + a_1 \alpha^p + a_0 = 0$.

Seja $\mathbb{L} = \mathbb{F}(a_m^{1/p}, \ldots, a_1^{1/p}, a_0^{1/p})$.

Temos que $A = \mathbb{E}$ é uma $\mathbb{F}$-álgebra simples. Mas,

$$u = \alpha^m \otimes a_m^{1/p} + \cdots + \alpha \otimes a_1^{1/p} + 1 \otimes a_0^{1/p} \in A \otimes_{\mathbb{F}} \mathbb{L},$$

é tal que

$$u^p = \alpha^{pm} \otimes a_m + \cdots + \alpha^p \otimes a_1 + 1 \otimes a_0 = (\alpha^{pm} a_m + \cdots + a_0) \otimes 1 = 0.$$

Portanto, $0 \neq u \in J(A^{\mathbb{L}})$. Daí $A^{\mathbb{L}}$ não é semissimples.

Proposição. Seja $\mathbb{E}/\mathbb{F}$ uma extensão separável finita. Então o mapa

$$f: \mathbb{E}\times\mathbb{E} \to \mathbb{F}, \quad f(x,y) = tr_{\mathbb{E}/\mathbb{F}}(xy)$$

é bilinear, associativa e não-degenerada. Ainda, se $\{e_i\}$ e $\{e_j'\}$ é um par dual de bases com respeito a f, então

$$\sum_{i=1}^{n} e_i' \cdot e_i \neq 0.$$

Dem.: Claro que f é bilinear e associativa. Como $\mathbb{E}/\mathbb{F}$ é separável, existe $z \in \mathbb{E}$ tal que $tr_{\mathbb{E}/\mathbb{F}}(z) \neq 0$. Seja $0 \neq x \in \mathbb{E}$. Então $f(x, x^{-1}z) = tr_{\mathbb{E}/\mathbb{F}}(xx^{-1}z) \neq 0$. Da mesma forma, $f(x^{-1}z, x) = f(x, x^{-1}z) \neq 0$. Portanto, f é não-degenerada.

Seja $\{e_i\}$ e $\{e_j'\}$ um par dual de bases com respeito a f. Assuma que $\sum e_i' e_i = 0$. Assim, para cada e_ℓ, temos que

$$0 = e_\ell \sum_{i=1}^{n} e_i' e_i = \sum_{i=1}^{n} e_\ell e_i' e_i = \sum_{i=1}^{n}\sum_{j=1}^{n} \lambda_{ij}(e_\ell) e_j' e_i.$$

Tomando $tr_{\mathbb{E}/\mathbb{F}}$, temos que

$$0 = tr_{\mathbb{E}/\mathbb{F}}\left(\sum_{i,j} \lambda_{ij}(e_\ell) e_j' e_i\right) = \sum_{i,j} \lambda_{ij}(e_\ell)\, tr(e_j', e_i)$$

$$= \sum_{i,j} \lambda_{ij}(e_\ell) f(e_i, e_j') = \sum_{i=1}^{n} \lambda_{ii}(e_\ell) = tr_{\mathbb{E}/\mathbb{F}}(e_\ell).$$

Daí $tr_{\mathbb{E}/\mathbb{F}}(e_\ell) = 0$, $\forall e_\ell$. Isso implica que $tr_{\mathbb{E}/\mathbb{F}}(x) = 0$, $\forall x \in \mathbb{E}$. Isso contradiz o fato de $tr_{\mathbb{E}/\mathbb{F}}(z) \neq 0$. $\square$

Lema. Sejam $\mathcal{A}$ uma $\mathbb{F}$-álgebra semissimples e $\mathbb{E}/\mathbb{F}$ uma extensão separável e finita. Então $\mathcal{A}^{\mathbb{E}}$ é semissimples.

Dem.: Sejam M um $\mathcal{A}^{\mathbb{E}}$-módulo e $N \subseteq M$ um $\mathcal{A}^{\mathbb{E}}$-submódulo. Note que M e N são $\mathcal{A}$-módulos. Como $\mathcal{A}$ é semissimples, M é completamente redutível como $\mathcal{A}$-módulo. Portanto, existe um $\mathcal{A}$-módulo N_0 tal que $M = N \oplus N_0$. Equivalentemente, existe $\pi \in \mathrm{End}_{\mathcal{A}} M$ tal que $\pi(M) \subseteq N$ e $\pi|_N = id_N$.

Seja $\{e_i\}$ e $\{e_j'\}$ um par dual de $\mathbb{F}$-bases de $\mathbb{E}$ como na proposição anterior. Seja $x = \sum e_i' e_i \neq 0$. Defina

$$\pi_0 = \frac{1}{x} \sum_{i=1}^{n} e_i' \pi e_i \in \mathrm{End}_{\mathbb{E}} M.$$

Como $\mathbb{E} \subseteq Z(\mathcal{A}^{\mathbb{E}})$, temos que π_0 é endomorfismo de $\mathcal{A}$-módulos. Portanto $\pi_0 \in \mathrm{End}_{\mathcal{A}^{\mathbb{E}}} M$. Além disso, como N é um $\mathbb{E}$-subespaço, temos que $\pi_0(M) \subseteq N$. Por fim, se $u \in N$, então $\pi(u) = u$. Daí

$$\pi_0(u) = \frac{1}{x} \sum_{i=1}^{n} e_i' \pi e_i(u) = \frac{1}{x} \sum_{i=1}^{n} e_i' e_i u = u.$$

Segue que $\pi_0|_N = id_N$. Conclui-se que $M = N \oplus \mathrm{Ker}\, \pi_0$ como $\mathcal{A}^{\mathbb{E}}$-módulos. Assim, M é $\mathcal{A}^{\mathbb{E}}$-módulo completamente redutível. Daí $\mathcal{A}^{\mathbb{E}}$ é semissimples. $\square$

Teorema. Sejam $\mathcal{A}$ uma $\mathbb{F}$-álgebra semissimples e $\mathbb{E} \supseteq \mathbb{F}$ uma extensão separável. Então $\mathcal{A}^{\mathbb{E}}$ é semissimples.

Dem.: Assuma que existe $0 \neq a \in J(\mathcal{A}^{\mathbb{E}})$. Então existe $m \in \mathbb{N}$ tal que $(\mathcal{A}^{\mathbb{E}} a \mathcal{A}^{\mathbb{E}})^m = 0$. Seja $\{a_1, \ldots, a_n\}$ uma $\mathbb{F}$-base de $\mathcal{A}$. Então,

$$a = \alpha_1 a_1 + \cdots + \alpha_n a_n, \quad \text{com } \alpha_1, \ldots, \alpha_n \in \mathbb{E}.$$

Seja $\mathbb{L} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. Então $\mathbb{L}/\mathbb{F}$ é uma extensão separável e finita. Do lema anterior, $J(\mathcal{A}^{\mathbb{L}}) = 0$. Entretanto, $a \in \mathcal{A}^{\mathbb{L}}$. Além disso,

$$(\mathcal{A}^{\mathbb{L}} a \mathcal{A}^{\mathbb{L}})^m \subseteq (\mathcal{A}^{\mathbb{E}} a \mathcal{A}^{\mathbb{E}})^m = 0.$$

Portanto, $0 \neq a \in J(\mathcal{A}^{\mathbb{L}})$, uma contradição. Portanto, $\mathcal{A}^{\mathbb{E}}$ é semissimples. $\square$

Corolário. Sejam $\mathcal{A}$ uma $\mathbb{F}$-álgebra com $\dim_{\mathbb{F}} \mathcal{A} < \infty$, e $\mathbb{E}/\mathbb{F}$ uma extensão separável de corpos. Então $J(\mathcal{A}^{\mathbb{E}}) = J(\mathcal{A})^{\mathbb{E}}$.

Dem.: Por um lado, sabe-se que $J(\mathcal{A})^{\mathbb{E}} \subseteq J(\mathcal{A}^{\mathbb{E}})$. Temos que $\mathcal{A}/J(\mathcal{A})$ é semissimples. Portanto, $(\mathcal{A}/J(\mathcal{A}))^{\mathbb{E}} = \mathcal{A}^{\mathbb{E}}/J(\mathcal{A})^{\mathbb{E}}$ é semissimples (pelo Teorema anterior). Portanto, $J(\mathcal{A}^{\mathbb{E}}) \subseteq J(\mathcal{A})^{\mathbb{E}}$. $\square$

Proposição. Sejam M um $\mathcal{A}$-módulo completamente redutível e $\mathbb{E} \supseteq \mathbb{F}$ separável. Então $M^{\mathbb{E}}$ é $\mathcal{A}^{\mathbb{E}}$-módulo completamente redutível.

Dem.: M é A-mód. comp. red. $\Rightarrow$ M é $A/J(A)$-mód. complet. red.

$\Rightarrow$ $M^{\mathbb{E}}$ é um $A^{\mathbb{E}}/J(A)^{\mathbb{E}}$-módulo e $A^{\mathbb{E}}/J(A)^{\mathbb{E}}$ é semissimples

$\Rightarrow$ $M^{\mathbb{E}}$ é $A^{\mathbb{E}}/J(A)^{\mathbb{E}}$-módulo completamente redutível

$\Rightarrow$ $M^{\mathbb{E}}$ é $A^{\mathbb{E}}$-módulo completamente redutível. $\square$