Álgebra Separável

Def. Seja A uma $\mathbb{F}$-álgebra de $\mathbb{F}$-dimensão finita. Dizemos que A é separável se para toda extensão de corpos $\mathbb{E}/\mathbb{F}$, a álgebra $A^{\mathbb{E}}$ é semissimples.

Obs.: (i) Se A é separável, então $A \cong A^{\mathbb{F}}$ é semissimples.

(ii) Escreva $A = A_1 \oplus A_2$. Então A é separável se e só se cada A_i é separável.

(iii) Sejam $\mathbb{E}_1/\mathbb{F}$ e $\mathbb{E}_2/\mathbb{F}$ extensões de corpos. Então, existe $\mathbb{E}/\mathbb{F}$ que é extensão de $\mathbb{E}_1$ e de $\mathbb{E}_2$. De fato, seja $A = \mathbb{E}_1 \otimes_{\mathbb{F}} \mathbb{E}_2$. Como A tem unidade, existe ideal maximal $I \subseteq A$. Daí A/I é corpo. Além disso, temos

$$\mathbb{E}_i \longrightarrow \mathbb{E}_1 \otimes_{\mathbb{F}} \mathbb{E}_2 \longrightarrow A/I.$$

Daí $\mathbb{E} := A/I$ é corpo que é extensão de $\mathbb{E}_1$ e de $\mathbb{E}_2$.

Teorema. Seja A uma $\mathbb{F}$-álgebra. Então A é separável se e só se existe $\mathbb{E}/\mathbb{F}$ tal que

$$A^{\mathbb{E}} \cong M_{n_1}(\mathbb{E}) \oplus \cdots \oplus M_{n_s}(\mathbb{E}).$$

Dem.: Assuma que A é separável e seja $\overline{\mathbb{F}}$ o fecho algébrico de $\mathbb{F}$. Então $A^{\overline{\mathbb{F}}}$ é semissimples, e portanto,

$$A^{\overline{\mathbb{F}}} \cong M_{n_1}(\overline{\mathbb{F}}) \oplus \cdots \oplus M_{n_s}(\overline{\mathbb{F}}).$$

Reciprocamente, assuma que $\mathbb{E}/\mathbb{F}$ é tal que

$$\mathcal{A}^{\mathbb{E}} \cong M_{n_1}(\mathbb{E}) \oplus \cdots \oplus M_{n_s}(\mathbb{E}).$$

Seja $\mathbb{L}/\mathbb{F}$ uma extensão de corpos. Seja $\mathbb{K}$ um corpo que é extensão de $\mathbb{L}$ e de $\mathbb{E}$. Então

$$\mathcal{A}^{\mathbb{K}} = (\mathcal{A}^{\mathbb{E}})^{\mathbb{K}} \cong M_{n_1}(\mathbb{K}) \oplus \cdots \oplus M_{n_s}(\mathbb{K})$$

$$\mathcal{A}^{\mathbb{K}} = (\mathcal{A}^{\mathbb{L}})^{\mathbb{K}}$$

Daí $J(\mathcal{A}^{\mathbb{L}})^{\mathbb{K}} \subseteq J(\mathcal{A}^{\mathbb{K}}) = 0$. Portanto, $J(\mathcal{A}^{\mathbb{L}}) = 0$.

Então $\mathcal{A}^{\mathbb{L}}$ é semissimples, e $\mathcal{A}$ é separável. $\square$

Seja $\mathcal{A}$ uma $\mathbb{F}$-álgebra de Frobenius, f uma forma bilinear associativa não-degenerada de $\mathcal{A}$, $\{a_i\}$ e $\{b_j\}$ bases duais de $\mathcal{A}$ com respeito a f. Cada $a \in \mathcal{A}$ define uma aplicação $\mathbb{F}$-linear $\mathcal{A} \to \mathcal{A}$ via multiplicação à esquerda. Daí

$$\sum_{i=1}^{n} b_i a a_i \in \mathrm{End}_{\mathcal{A}} \mathcal{A}.$$

Isso significa que $\sum b_i a a_i =: c(a) \in Z(\mathcal{A})$. Defina

$$\Gamma(\mathcal{A}) = \{c(a) \mid a \in \mathcal{A}\} = \{\sum_{i=1}^{n} b_i a a_i \mid a \in \mathcal{A}\}.$$

Temos que $\Gamma(\mathcal{A})$ é um ideal de $Z(\mathcal{A})$

Lema. $\Gamma(\mathcal{A})$ não depende da base dual escolhida.

Dem.: Seja $\{a_i'\}$ e $\{b_j'\}$ outra base dual com respeito a f.

Escreva $a_i' = \sum_{l=1}^{n} \alpha_{il} a_l$, $b_j' = \sum_{m=1}^{n} \beta_{jm} b_m$. Então

$$\delta_{ij} = f(a_i', b_j') = f\left(\sum_l \alpha_{il} a_l, \sum_m \beta_{jm} b_m\right) =$$

$$= \sum_{l,m} \alpha_{il} \beta_{jm} f(a_l, b_m) = \sum_{l=1}^{n} \alpha_{il} \beta_{jl}.$$

Seja $a \in A$. Então

$$\sum_{h=1}^{n} b_h' a a_h' = \sum_h \sum_{l,m} \beta_{hm} \alpha_{hl} b_m a a_l =$$

$$= \sum_{l,m} \underbrace{\left(\sum_{h=1}^{n} \beta_{hm} \alpha_{hl}\right)}_{\delta_{ml}} b_m a a_l = \sum_{l=1} b_l a a_l = c(a).$$

$\square$

Lema. $\Gamma(A)$ independe da escolha da forma f.

Dem.: Seja f' uma outra forma bilinear associativa não-degenerada de A. Então temos isomorfismo de A-módulos

$$\theta : A \to A^* \quad \text{e} \quad \theta' : A \to A^*,$$

dados por

$a, b \in A$, $\langle a, \theta(b) \rangle = f(a,b)$, $\langle a, \theta'(b) \rangle = f'(a,b)$.

Então $\psi = \theta^{-1} \circ \theta' \in \mathrm{Aut}_A A$. Seja $r = \psi(1)$. Então

$$\psi(a) = \psi(a \cdot 1) = a\psi(1) = ar.$$

Assim, $\psi = R_a$. Além disso, r é invertível, pois ψ é auto.

Seja $\{a_i\}$ e $\{b_j\}$ uma base dual com respeito a f. Então, $\{b_j r^{-1}\}$ é $\mathbb{F}$-base de A. Além disso,

$$\delta_{ij} = f(a_i, b_j) = f(a_i, b_j r^{-1} r) = f(a_i, \psi(b_j r^{-1})) =$$

$$= f(a_i, \theta^{-1} \circ \theta'(b_j r^{-1})) = \langle a_i, \theta'(b_j r^{-1}) \rangle = f'(a_i, b_j r^{-1}).$$

Portanto, $\{a_i\}$ e $\{b_j r^{-1}\}$ é base dual com respeito a f'.

Além disso, se $a \in A$,

$$\ell(a) = \sum_{i=1}^{n} b_i a a_i = \sum_{i=1}^{n} (b_i r^{-1}) r a\, a_i$$

$\square$

Exemplos.

(1) Seja $A = M_n(\mathbb{F})$ uma $\mathbb{F}$-álgebra central e simples. Defina $f: A \times A \to \mathbb{F}$ via $f(a,b) = tr(ab)$. Uma base dual com respeito a f é $\{e_{ij}\}$ e $\{e_{ij}^{\tau}\}$, em que $\tau(e_{ij}) = e_{ji}$ é a transposta. Daí

$$\Gamma(A) \ni \sum_{i,j} e_{ij}^{\tau} \cdot e_{11} \cdot e_{ij} = \sum_{i,j} e_{ji} e_{11} e_{ij} =$$

$$= \sum_{j} e_{j1} e_{11} e_{1j} = \sum_{j} e_{jj} = Id_{n \times n}.$$

Daí $\Gamma(A) \cong \mathbb{F} \cong Z(A)$.

(2) Seja A uma $\mathbb{F}$-álgebra de Frobenius, e assuma que $A = A_1 \oplus A_2$. Seja f a forma bil. não-deg. associativa de A.

Seja $e_i \in \mathcal{A}_i$ a unidade. Dado $0 \neq a \in \mathcal{A}_1$, existe $b \in \mathcal{A}$ tal que

$$0 \neq f(a,b) = f(a \cdot e_1, b) = f(a, \underbrace{e_1 b}_{\in \mathcal{A}_1}).$$

Portanto, podemos assumir que $b \in \mathcal{A}_1$. Segue que $f|_{\mathcal{A}_i}$ é não-degenerada. Daí uma base dual de $\mathcal{A}$ com respeito a f pode ser tomada como união de bases duais de $\mathcal{A}_i$ com respeito a $f|_{\mathcal{A}_i}$. Assim,

$$\Gamma(\mathcal{A}) = \Gamma(\mathcal{A}_1) \oplus \Gamma(\mathcal{A}_2).$$

(3) Sejam $\mathcal{A}$ uma $\mathbb{F}$-álgebra de Frobenius, $\mathbb{E}/\mathbb{F}$ ext., e $f: \mathcal{A} \times \mathcal{A} \to \mathbb{F}$. Daí $f^{\mathbb{E}}: \mathcal{A}^{\mathbb{E}} \times \mathcal{A}^{\mathbb{E}} \to \mathbb{E}$ é bilinear, ass. e não-deg. Então, se $\{a_i\}$ e $\{b_j\}$ é par de bases duais de $\mathcal{A}$ com respeito a f, então vão ser par de bases duais de $\mathcal{A}^{\mathbb{E}}$ com respeito a $f^{\mathbb{E}}$. Daí

$$\Gamma(\mathcal{A}^{\mathbb{E}}) = \Gamma(\mathcal{A})^{\mathbb{E}}.$$

Lema. Seja $\mathcal{A} = M_n(D)$ uma $\mathbb{F}$-álgebra separável. Então

$$\Gamma(\mathcal{A}) = Z(D).$$

Dem.: Já vimos que

$$\mathcal{A} \text{ separável} \Rightarrow \mathcal{A} \text{ semissimples} \Rightarrow \mathcal{A} \text{ é Frobenius.}$$

Como $Z(D)$ é corpo, basta mostrar que $\Gamma(\mathcal{A}) \neq 0$.

Sendo $\mathcal{A}$ separável, existe $\mathbb{E}/\mathbb{F}$ tal que
$$\mathcal{A}^{\mathbb{E}} \cong M_{n_1}(\mathbb{E}) \oplus \cdots \oplus M_{n_s}(\mathbb{E}).$$
Daí, dos exemplos,
$$\Gamma(\mathcal{A})^{\mathbb{E}} = \Gamma(\mathcal{A}^{\mathbb{E}}) = \Gamma\big(M_{n_1}(\mathbb{E})\big) \oplus \cdots \oplus \Gamma\big(M_{n_s}(\mathbb{E})\big) \cong \mathbb{E} \oplus \cdots \oplus \mathbb{E}.$$
Portanto, $\Gamma(\mathcal{A}) \neq 0$. $\square$

Teorema. Seja $\mathcal{A}$ uma $\mathbb{F}$-álgebra de dimensão finita. As seguintes afirmações são equivalentes:

(i) $\mathcal{A}$ é separável,

(ii) $\mathcal{A}$ é uma álgebra de Frobenius tal que $\Gamma(\mathcal{A}) = Z(\mathcal{A})$,

(iii) Existe uma $\mathbb{F}$-base de $\mathcal{A}$, $\{a_1, \dots, a_n\}$ satisfazendo o seguinte: existe $\{a_1', \dots, a_n'\}$ tal que
$$\sum_{i=1}^{n} a_i' a_i = 1,$$
$$\forall a \in \mathcal{A}, \quad a_i a = \sum_{j=1}^{n} \lambda_{ij}(a) a_j \quad (\lambda_{ij}(a) \in \mathbb{F}),$$
$$\Rightarrow \quad a a_j' = \sum_{i=1}^{n} \lambda_{ij}(a) a_i'.$$

Dem.: (i) $\Rightarrow$ (ii). Temos que $\mathcal{A}$ é semissimples (e, portanto, uma álgebra de Frobenius), e $\mathcal{A} = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s)$, em que cada $M_{n_i}(D_i)$ é $\mathbb{F}$-álgebra separável. Assim, dos exemplos,
$$\Gamma(\mathcal{A}) \cong \Gamma(M_{n_1}(D_1)) \oplus \cdots \oplus \Gamma(M_{n_s}(D_s)) = Z(D_1) \oplus \cdots \oplus Z(D_s) = Z(\mathcal{A}).$$

(ii) $\Rightarrow$ (iii). Seja $\{a_i\}$ e $\{b_i\}$ um par dual de bases. Como $\Gamma(A) = Z(A)$, existe $a \in A$ tal que

$$1 = \sum_{i=1}^{n} b_i a a_i.$$

Então, basta definir $a_i' = b_i a$. Da propriedade da base dual, segue que $\{a_1', \ldots, a_n'\}$ satisfaz a condição (iii), com respeito a base $\{a_1, \ldots, a_n\}$.

(iii) $\Rightarrow$ (i). Seja $\mathbb{E}/\mathbb{F}$ ext. de corpos. Sejam M um $A^{\mathbb{E}}$-módulo, e $N \subseteq M$ um $A^{\mathbb{E}}$-submódulo. Daí, existe $\pi \in \operatorname{End}_{\mathbb{E}} M$ tal que $\pi(M) \subseteq N$ e $\pi|_N = id_N$.

Defina
$$\pi_0 = \sum_{i=1}^{n} a_i' \pi a_i.$$

Repetindo o argumento de um lema anterior, conclui-se que $\pi_0 \in \operatorname{End}_{A^{\mathbb{E}}} M$. Sendo N um $A^{\mathbb{E}}$-submódulo, obtemos que $\pi_0(M) \subseteq N$. Dado $u \in N$, temos que

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

Segue que $\pi_0|_N = id_N$. Então $M = N \oplus \operatorname{Ker} \pi_0$ como $A^{\mathbb{E}}$-módulos. Portanto M é complet. red. $\Rightarrow A^{\mathbb{E}}$ é semissimples. $\square$

Corolário. Seja $\mathbb{E}/\mathbb{F}$ finita. Então $\mathbb{E}/\mathbb{F}$ é separável se e só se $\mathbb{E}$ é uma $\mathbb{F}$-álgebra separável. $\square$

Teorema. Seja $\mathcal{A} = M_n(D)$ uma $\mathbb{F}$-álgebra de $\mathbb{F}$-dimensão finita. Assuma que $Z(D)/\mathbb{F}$ é separável. Então $\mathcal{A}$ é separável.

Dem.: Seja $\mathbb{E}/\mathbb{F}$ ext. de corpos. Então

$$\mathcal{A}^{\mathbb{E}} \cong M_n(D) \otimes_{\mathbb{F}} \mathbb{E} \cong \left(M_n(D) \otimes_{Z(D)} Z(D)\right) \otimes_{\mathbb{F}} \mathbb{E}$$
$$\cong M_n(D) \otimes_{Z(D)} \left(Z(D) \otimes_{\mathbb{F}} \mathbb{E}\right)$$

Temos que $Z(D)^{\mathbb{E}} = Z(D) \otimes_{\mathbb{F}} \mathbb{E} \cong \mathbb{E}^{Z(D)}$ é semissimples, pois $Z(D)/\mathbb{F}$ é separável. Portanto, $\mathbb{E}^{Z(D)} \cong \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_s$, com $\mathcal{A}_i$ simples. Como $M_n(D)$ é $Z(D)$-central simples, segue que $M_n(D) \otimes_{Z(D)} \mathcal{A}_i$ é simples. Portanto, $\mathcal{A}^{\mathbb{E}}$ é semissimples. $\square$

Def. Sejam $\mathbb{E}/\mathbb{F}$ e $\mathcal{A}$ uma $\mathbb{E}$-álgebra. Dizemos que $\mathcal{A}$ é *realizável* em $\mathbb{F}$ se existe uma $\mathbb{F}$-álgebra $\mathcal{A}_0$ tal que $\mathcal{A} \cong \mathcal{A}_0^{\mathbb{E}}$.

Corolário.

(i) Seja $\mathcal{A}$ uma $\mathbb{E}$-álgebra de $\mathbb{E}$-dimensão finita, e assuma que $\mathcal{A}$ é realizável em um corpo perfeito $\mathbb{F}$. Então $\mathcal{A}/J(\mathcal{A})$ é separável.

(ii) Seja G um grupo finito e $\mathbb{F}$ um corpo qualquer. Então $\mathbb{F}G/J(\mathbb{F}G)$ é separável. $\square$