CAPITOLO 2

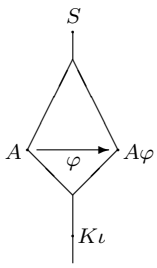
Automorfismi nella teoria delle algebre associative

Anche in questo capitolo sia K un campo. Per ogni algebra associativa unitaria B su K scriviamo $U(B)$ per il gruppo degli elementi invertibili di B. Per ogni $y \in U(B)$, la coniugazione mediante y [14] è un automorfismo non solo del gruppo $U(B)$ ma anche dell'algebra B, detto l'automorfismo interno tramite y. La seguente proposizione risulterà essere la spina dorsale della teoria.

2.1. Teorema (Skolem-Noether (1927)). *Sia S un'algebra associativa semplice su K, A una sottoalgebra semplice unitale di S. Se S o A è centrale, allora ogni monomorfismo unitale φ da A in S si estende ad un automorfismo interno di S, cioè, esiste un $y \in U(S)$ tale che $x\varphi = y^{-1}xy$ per ogni $x \in A$.*

Dimostrazione. Senza perdere di generalità assumiamo che $S = D^{n\times n}$ per un'algebra di divisione D su K e $n \in \mathbb{N}$. Il K-spazio D^n è un D^--modulo tramite moltiplicazione a sinistra, e per 1.4(1) vale

$$\mathrm{End}_{D^-} D^n \cong \big(\mathrm{End}(D,\lambda)\big)^{n\times n} \cong (D\rho)^{n\times n} \cong S.$$



Sia ψ un isomorfismo di K-algebre da $\mathrm{End}_{D^-} D^n$ su S. Allora D^n è un A-modulo rispetto a *due* D^--rappresentazioni unitali di A: ${\psi^{-1}}_{|A}$ e $\varphi\psi^{-1}$. Siano $\overline{{\psi^{-1}}_{|A}}$ e $\overline{\varphi\psi^{-1}}$ le rappresentazioni corrispondenti di $A \underset{K}{\otimes} D^-$ (v. 1.7.1). Per il caso speciale (2) dopo 1.10, $A \underset{K}{\otimes} D^-$ è semplice, allora il Corollario a p. 2 implica l'esistenza di un isomorfismo α dell'$A \underset{K}{\otimes} D^-$-modulo $(D^n, \overline{{\psi^{-1}}_{|A}})$ sullo $A \underset{K}{\otimes} D^-$-modulo $(D^n, \overline{\varphi\psi^{-1}})$. Per ogni $x \in A$ vale allora $(x\psi^{-1})\alpha = \alpha(x\varphi\psi^{-1})$ ossia $x(\alpha\psi) = (\alpha\psi)(x\varphi)$, applicando ψ. L'elemento $y := \alpha\psi$ è invertibile perché α è un automorfismo del K-spazio D^n, e vale $x\varphi = y^{-1}xy$ per ogni $x \in A$. □

Nel **caso speciale** $S = A$ si ottiene[15]: $\mathrm{Aut}_K A = \mathrm{Inn}_K A$ *per ogni algebra associativa centrale semplice A di dimensione finita* (dove il gruppo degli automorfismi interni di A è denotato con $\mathrm{Inn}_K A$)[16].

L'osservazione 1.4(1) permette la seguente semplice generalizzazione di cui avremo bisogno nel seguito:

[14] cioè, la applicazione da B in B che porta ogni $x \in B$ in $y^{-1}xy$.

[15] È questo il risultato di Skolem.

[16] Vale $\mathrm{Inn}_K A \cong U(A)/\dot{K}\iota$

2.1.1. *Sia A un'algebra associativa unitaria, B una sottoalgebra unitale di A. Allora $(A,+)$ è un $A^- \underset{K}{\otimes} A$-modulo*[17]*, a maggior ragione allora anche un $A^- \underset{K}{\otimes} B$-modulo, e vale*

$$C_A(B)\rho = \mathrm{End}_{A^- \underset{K}{\otimes} B}(A,+).$$

Dimostrazione. Per 1.4(1) vale $\mathrm{End}(A,\lambda) = A\rho$, allora

$$\mathrm{End}_{A^- \underset{K}{\otimes} B}(A,+) = \mathrm{End}(A,\lambda) \cap \mathrm{End}_{B\rho}(A,+) = C_{A\rho}(B\rho) = C_A(B)\rho.$$

□

2.2. Teorema. *Sia A un'algebra associativa centrale semplice di dimensione finita su K, B una sottoalgebra semplice unitale di A. Allora si ha*

(1) *$C_A(B)$ è semplice,*
(2) $\dim_K B \, \dim_K C_A(B) = \dim_K A$,
(3) $C_A(C_A(B)) = B$ [18]
(4) *Se B è centrale, allora $C_A(B)$ è centrale e $A = B \dot{\underset{K}{\otimes}} C_A(B)$.*

Dimostrazione. (1), (2) Sia $T := A^- \underset{K}{\otimes} B$. Per 2.1.1 si ha $C_A(B) \cong \mathrm{End}_T(A,+)$, poi T è semplice per il caso speciale (2) dopo 1.10. Sia R un ideale destro minimale di T. Allora esiste un $k \in \mathbb{N}$ tale che vale l'isomorfismo di T-moduli $A \underset{T}{\cong} \underbrace{R \oplus \cdots \oplus R}_{k}$. Ponendo $D := \mathrm{End}_T R$ otteniamo

$$C_A(B) \cong \mathrm{End}_T(A,+) \cong D^{k\times k},$$

quindi (1). Poi vale $T \cong (D^-)^{n\times n}$ per un $n \in \mathbb{N}$, quindi $R \underset{K}{\cong} D^n$, $T \underset{K}{\cong} R^n$, implicando

$$\dim_K B \, \dim_K C_A(B) = \frac{\dim_K T}{\dim_K A} \dim_K C_A(B) = \frac{n \dim_K R \, k^2 \dim_K D}{k \dim_K R}$$
$$= nk \dim_K D = \dim_K R^k = \dim_K A.$$

(3) Ovviamente vale $B \subseteq C_A(C_A(B))$, e (2) comporta

$$\dim_K B \, \dim_K C_A(B) = \dim_K A = \dim_K C_A(B) \, \dim_K C_A(C_A(B))$$

perché $C_A(B)$ è semplice per (1). Ne segue la tesi.

(4) Per (1), $C_A(B)$ è semplice. Allora $B \underset{K}{\otimes} C_A(B)$ è semplice per il caso speciale (2) dopo 1.10. Allora l'epimorfismo $B \underset{K}{\otimes} C_A(B) \to BC_A(B)$ è un isomorfismo. Concludiamo per (2) che

$$\dim_K A = \dim_K B \, \dim_K C_A(B) = \dim_K(BC_A(B)),$$

quindi $A = BC_A(B)$ e $Z(C_A(B)) = Z(A) = K\iota$. □

Chiamando minimale un elemento E di $\mathcal{B}(K)$ se $E \neq K$ e $K\iota$ è l'unica sottoalgebra centrale semplice propria di E, otteniamo

2.3. Corollario. $\mathcal{B}(K) = \langle E | E \in \mathcal{B}(K) \text{ minimale} \rangle_{\odot}$.

[17] dove A^- agisce mediante λ, A mediante ρ

[18] =Teorema del *doppio centralizzante*

DIMOSTRAZIONE. Sia $\mathcal{P} := \{E | E \in \mathcal{B}(K) \text{ minimale}\}$. Se $D \in \mathcal{B}(K)$ è minimale o $D = K$, allora $D \in \langle \mathcal{P} \rangle_{\odot}$. Altrimenti esiste $E \in \mathcal{P}$ tale che E è isomorfa ad una sottoalgebra propria E' di D. Per 2.2(4), $C_D(E') \underset{K}{\otimes} E' \cong D$. Sia $D' \in \mathcal{B}(K)$ tale che $C_D(E') \cong D'^{m\times m}$ per un $m \in \mathbb{N}$. Allora $\dim_K D' < \dim_K D$ e $D' \odot E = D$. Induttivamente possiamo assumere che esistano $E_1, \ldots, E_k \in \mathcal{P}$ tali che $D' = E_1 \odot \cdots \odot E_k$. Ne segue che $D \in \langle \mathcal{P} \rangle_{\odot}$. □

2.4. TEOREMA. *Sia $D \in \mathcal{B}(K)$, L un sottocampo massimale di D, $n := \dim_K L$. Allora*

$$L = C_D(L), \quad \dim_K D = n^2, \quad D \underset{K}{\otimes} L \cong L^{n\times n} \text{ (isomorfismo di } L\text{-algebre)}$$

DIMOSTRAZIONE. Ovviamente vale $L \subseteq C_D(L)$. Se $y \in C_D(L)$, $L[y]$ è un campo, per 1.3(1). Ne segue $y \in L$ per la massimalità di L. Ora 2.2(2) implica che $\dim_K D = n^2$.

Resta da dimostrare l'ultima affermazione. Per il caso speciale (2) dopo 1.10, $D^- \underset{K}{\otimes} L$ è una K-algebra semplice e, per 1.8(1), centrale come L-algebra. A meno di isomorfismi, $(D, +)$ è il suo unico modulo irriducibile su L. Applicando successivamente la descrizione di $D^- \underset{K}{\otimes} L$ dalla teoria di base (v. p. 1), 2.1.1 e la prima parte di questo teorema otteniamo le seguente catena di isomorfismi come L-algebre:

$$D^- \underset{K}{\otimes} L \cong \left((\mathrm{End}_{D^- \underset{K}{\otimes} L}(D, +))^-\right)^{m\times m} \cong C_D(L)^{m\times m} = L^{m\times m}$$

per un $m \in \mathbb{N}$. Ne segue che $D \underset{K}{\otimes} L \cong (D^- \underset{K}{\otimes} L)^- \cong L^{m\times m}$. Per la seconda parte di questo teorema consegue $m = n$. □

Dalla seconda parte di 2.4 si ha

2.5. COROLLARIO. *Sia S un corpo di dimensione finita su $K := Z(S)$. Allora $\dim_K S$ è un quadrato perfetto.* □

2.6. DEFINIZIONE. *Sia $D \in \mathcal{B}(K)$. Per la seconda parte di* 2.4 *tutti i sottocampi massimali di D hanno la stessa dimensione su K. Tale dimensione viene detta* l'indice di Schur *di D e denotata con* $\mathrm{ind}\, D$.

2.6.1. *Sia $D \in \mathcal{B}(K)$, $m \in \mathbb{N}$, $A := D^{m\times m}$ e L un sottocampo di A tale che $L = C_A(L)$.*[19] *Sia R un ideale destro minimale di A. Allora vale* $\dim_L R = \mathrm{ind}\, D$.

DIMOSTRAZIONE. Vale $(m \,\mathrm{ind}\, D)^2 = \dim_K A = (\dim_K L)^2$ per 2.2(2), allora

$$\dim_K L \,\mathrm{ind}\, D = m \dim_K D = \dim_K R = \dim_K L \dim_L R,$$

quindi la tesi. □

2.7. TEOREMA (Wedderburn (1905)). *Ogni corpo finito è un campo.*

Dunque, per ogni campo finito K vale $\mathcal{B}(K) = \{K\}$.

[19] In particolare, L è sottocampo massimale di A. Mettiamo in evidenza che quest'ultimo fatto, però, non implica che $L = C_A(L)$ come si vede, per esempio, nel caso $D := \mathbb{C}$ in cui il centro dell'algebra matriciale è sottocampo massimale.

Dimostrazione. Sia D un corpo finito, $K := Z(D)$. Allora D è un'algebra di divisione (di dimensione) finita sul campo K. Sia $\mathfrak{M}$ l'insieme dei sottocampi massimali di D, $L \in \mathfrak{M}$. Per 1.3(1) vale $D = \bigcup \mathfrak{M}$, e $|L| = |L'|$ per un qualsiasi $L' \in \mathfrak{M}$ grazie a 2.4 (v. 2.6), quindi anche $L \cong L'$ per un risultato classico sui campi finiti. Ora 2.1 implica che $L' = L^y$ per un $y \in \dot{D}$. Ne segue che

$$\dot{D} = \bigcup_{y \in \dot{D}} \dot{L}^y.$$

Ma in un gruppo finito l'unione dei coniugati di un sottogruppo proprio è sempre una parte propria.[20] Allora $\dot{L} = \dot{D}$, quindi D è commutativo. □

Un campo finito è sempre un campo di ampliamento galoissiano su ogni sottocampo, con un gruppo di Galois ciclico. Quindi otteniamo il seguente risultato come conseguenza:

2.8. Corollario. *Se L è un campo finito, K un sottocampo di L, allora la norma $\mathcal{N} : \dot{L} \to \dot{K}$ è suriettiva.*

Dimostrazione. Sia σ un generatore di $\mathrm{Aut}_K L$, $z \in K$. Per 1.2(1) esiste un'algebra di divisione centrale D su K tale che $L_{\sigma,z} \cong D^{n\times n}$ per un $n \in \mathbb{N}$. Per 2.7 D è un campo. Quindi $K \cong Z(L_{\sigma,z}) \cong Z(D) = D$ e allora $n = o(\sigma)$, $L_{\sigma,z} \cong K^{n\times n}$. Ne segue che $z \in \dot{L}\mathcal{N}$ per 1.2(2). □

2.9. Corollario. *Sia D un corpo,* $\operatorname{char} D > 0$. *Allora ogni sottogruppo finito di $\dot{D}$ è ciclico.*

Per un *campo* D questo è un risultato classico che vale senza ipotesi sulla caratteristica e al quale ridurremo il corollario nella dimostrazione. Per un corpo D di caratteristica 0 invece abbiamo già visto un controesempio a p. 3.[21]

Dimostrazione. Sia $H \leq \dot{D}$, H finito, K il campo primo di D. Allora K è un sottocampo finito di $Z(D)$, $\langle H\rangle_K$ è sottoalgebra di D e finita, quindi sottoalgebra finita di divisione per 1.3(1) e di conseguenza un campo, per 2.7. Pertanto H è sottogruppo del gruppo moltiplicativo di un campo finito e quindi é ciclico. □

2.10. Teorema (Frobenius (1877)). *A meno di isomorfismi, $\mathbb{R}$ e $\mathbb{H}$ sono le uniche algebre di divisione centrali di dimensione finita su $\mathbb{R}$.*

In altre parole, $\mathcal{B}(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\}$.

Dimostrazione. Sia D un'algebra di divisione centrale di dimensione finita su $\mathbb{R}$, senza perdere di generalità $\mathbb{R} < D$. Per 1.3(1) ogni sottocampo massimale di D è un un'estensione propria di dimensione finita di $\mathbb{R}$ e allora isomorfa a $\mathbb{C}$. Allora possiamo assumere $\mathbb{R} < \mathbb{C} < D$. Da 2.4 segue che $\dim_{\mathbb{R}} D = 4$.

[20] Sia G un gruppo finito, $H \leq G$, $\bigcup_{y\in G} H^y = G$. Ogni sottogruppo contiene l'elemento 1_G, allora vale

$$|G| = |\bigcup_{y\in G} H^y| \leq 1 + |G : N_G(H)|(|H| - 1) \leq 1 + \frac{|G|}{|H|}(|H| - 1) = 1 + |G| - \frac{|G|}{|H|},$$

quindi $\frac{|G|}{|H|} = 1$, cioè, $H = G$.

[21] Nel 1955, Amitsur [**Am**] descrisse i gruppi finiti che compaiono come sottogruppi di qualche algebra di divisione di caratteristica 0. Per esempio, $\langle a, b | a^7 = 1 = b^9, a^b = a^2\rangle$ e $\langle a, b | a^{13} = 1 = b^9, a^b = a^9\rangle$ sono tali gruppi non ciclici di ordini dispari (risp. 63, 117).

$\begin{matrix} D \\ | \\ \mathbb{C} \\ | \\ \mathbb{R} \end{matrix}$ *Per* 2.1*, l'automorfismo* $z \mapsto \overline{z}$ *di* $\mathbb{C}$ *si estende ad un automorfismo interno di* D*.*

Cioè, esiste un $y \in \dot{D}$ tale che $y^{-1}zy = \overline{z}$ per ogni $z \in \mathbb{C}$. Ne segue che $y^{-1}iy = \overline{i} = -i$ (quindi $y \notin \mathbb{C}$ e $\mathbb{C}[y] = D$ per 1.3(1)) e $(y^2)^{-1}iy^2 = y^{-1}(-i)y = i$, implicando che $y^2 \in Z(D) = \mathbb{R}$.

C'è una certa libertà nella scelta di y*:* Tutto questo vale anche per ogni elemento cy oppure yc al posto di y, dove $c \in \dot{\mathbb{C}}$. Pertanto possiamo assumere che $y^2 \in \{1, -1\}$ e quindi $y^2 = -1$ visto che $y^2 = 1$ vale solo per il caso escluso che $y \in \{1, -1\}$. Ora vale $i^2 = -1 = y^2$, $iy = -yi$. $\dim_{\mathbb{R}} D = 4$, quindi $D \cong \mathbb{H}$ (v. p. 2). □

Sono scritti in corsivo i due aspetti della dimostrazione che giocheranno il ruolo decisivo nello sviluppo della teoria. Adesso considereremo in generale i campi di ampliamento L di K che compaiono come sottocampi di una K-algebra associativa unitaria A e loro automorfismi. Come al solito (in teoria dei gruppi) scriviamo $N_{U(A)}(L)$, $C_{U(A)}(L)$ per il normalizzante, il centralizzante di L nel gruppo $U(A)$ degli elementi invertibili di A rispettivamente.

2.11. Lemma. *Sia* A *un'algebra associativa unitaria su* K *e* L *un sottocampo unitale di* A*. Assumiamo che* $K \leq L$ [22]*. Siano* $r \in \mathbb{N}$ *e* $y_1, \ldots, y_r$ *elementi a due a due distinti di un trasversale di* $C_{U(A)}(L)$ *in* $N_{U(A)}(L)$*. Sia* $J \leq (A, +)$ *tale che* JL*,* $LJ \subseteq J$ *e* $y_1, \ldots, y_r \notin J$*. Allora* $(J + y_1, \ldots, J + y_r)$ *è linearmente indipendente nel* L*-spazio (destro)* A/J*.*

Dimostrazione. Altrimenti si scelga un controesempio con r minimo. Allora esistono $b_1, \ldots, b_r \in \dot{L}$ tali che $\sum_{i \in \underline{r}\,'} y_i b_i \in J$. Vale $r \neq 1$. Sia α_i la coniugazione mediante y_i. Allora vale per ogni $b \in L$

$$\begin{array}{ccccccccc} y_1(b\alpha_1)b_1 & + & y_2(b\alpha_2)b_2 & + & \cdots & + & y_r(b\alpha_r)b_r & = & b\sum_{i \in \underline{r}\,'} y_i b_i \in J, \\ y_1(b\alpha_1)b_1 & + & y_2(b\alpha_1)b_2 & + & \cdots & + & y_r(b\alpha_1)b_r & = & \sum_{i \in \underline{r}\,'} y_i b_i\,(b\alpha_1) \in J. \end{array}$$

Di conseguenza, $\sum_{i=2}^{r} y_i(b\alpha_i - b\alpha_1)b_i \in J$. Siccome $b_i \neq 0_L$ e r è minimo ne segue $b\alpha_i = b\alpha_1$, quindi $C_{U(A)}y_i = C_{U(A)}y_1$ per ogni $i > 1$, assurdo. □

2.12. Proposizione. *Sia* A *un'algebra associativa unitaria di dimensione finita su* K*,* L *un sottocampo unitale di* A *tale che* $K \leq L$*. (Allora* $N_{U(A)}(L)$ *agisce mediante coniugazione su* L*.) Sia* $G \leq \mathrm{Aut}_K L$ *l'immagine di* $N_{U(A)}(L)$ *rispetto a quell'azione. Per ogni* $\alpha \in G$ *sia* $y_\alpha \in N_{U(A)}(L)$ *tale che* $b\alpha = y_\alpha^{-1} b y_\alpha$ *per ogni* $b \in L$*. Allora*

$\begin{matrix} U(A) \\ | \\ N_{U(A)}(L) \longrightarrow \\ | \\ C_{U(A)}(L) \longrightarrow \\ | \\ \dot{L} \end{matrix}$ $\begin{matrix} G \\ | \\ \{\mathrm{id}\} \end{matrix}$

(1) $\{y_\alpha | \alpha \in G\}$ *è una parte* L*-linearmente indipendente di* A*.*
(2) *Se* $\dim_L A = |G|$*, allora* $L = C_A(L)$*.*
(3) *Se* (K, L) *è galoissiana,* $G = \mathrm{Aut}_K L$ *e* $\dim_L A = |G|$*, allora* A *è centrale semplice.*

Dimostrazione. (1) è il caso speciale $J = \{0_A\}$ di 2.11.

(2) Banalmente, $y_\alpha \in C_A(L) \Leftrightarrow \alpha = \mathrm{id}_L$. Poniamo $J := C_A(L)$ e otteniamo da 2.11

$$|G| = \dim_L A = \dim_L J + \dim_L A/J \geq \dim_L J + |G| - 1,$$

[22] cioè, L è campo di ampliamento di K.

quindi $\dim_L J = 1$, cioè, $C_A(L) = L$.

(3) Sia $J \lhd A$. Allora $y_\alpha \notin J$ per ogni $\alpha \in G$, quindi $\dim_L A/J \geq |G|$ per 2.11 e conseguentemente $J = \{0_A\}$. Allora A è semplice.

Da (2) segue che $Z(A) \subseteq L$. Se $b \in Z(A)$, allora vale $b = y_\alpha^{-1} b y_\alpha = b\alpha$ per ogni $\alpha \in G$. Pertanto b appartiene al campo degli elementi fissati da G, cioè, a K. Allora $Z(A) = K$. □

La scelta dell'elemento y_α corrispondente ad $\alpha \in G$ non è unica, quindi non è detto che $y_{\alpha\beta}$ coincida con $y_\alpha y_\beta$. Lo studio della funzione data tramite il quoziente di tali elementi risulterà essere un passo significativo nella teoria:

2.13. Proposizione. *Siano soddisfatte le ipotesi di* 2.12 *e poniamo* $f(\alpha, \beta) := y_{\alpha\beta}^{-1} y_\alpha y_\beta$ *per ogni* $\alpha, \beta \in G$.

(1) *Per ogni* $\alpha, \beta, \gamma \in G$, $a, b \in L$ *vale* $f(\alpha, \beta) \in C_{U(A)}(L)$, $y_\alpha a \cdot y_\beta b = y_{\alpha\beta} f(\alpha, \beta)\, a\beta\, b$.

(2) *Sia* $L = C_A(L)$ *e* (M, δ) *un* A*-modulo unitale di dimensione finita. (In particolare,* M *è un* L*-spazio vettoriale destro.) Ponendo* $n := \dim_L M$ *si ha per ogni* $\alpha, \beta \in G$

$$f(\alpha, \beta)^n = (\det y_{\alpha\beta}\delta)^{-1} \cdot (\det y_\alpha \delta)\beta \cdot \det y_\beta \delta.$$

Dimostrazione. (1) Vale $y_{\alpha\beta} C_{U(A)}(L) = y_\alpha C_{U(A)}(L)\, y_\beta C_{U(A)}(L)$ per ogni α, β e γ elementi di G, quindi $f(\alpha, \beta) \in C_{U(A)}(L)$. Poi, per ogni $a \in L$ si ha $a\beta = y_\beta^{-1} a y_\beta$, allora l'equazione affermata.

(2) Per ogni $v \in M$, $x \in A$ scriviamo vx invece di $v(x\delta)$. Sia $(v_1, \ldots, v_n)$ un'upla base di M come L-spazio vettoriale. Per ogni $i, j \in \underline{n}_{\text{ı}}$, $x \in A$, sia $b_{i,j}(x) \in L$ tale che vale $v_i x = \sum_{j \in \underline{n}_{\text{ı}}} v_j b_{i,j}(x)$. Ne segue per ogni $\alpha, \beta \in G$, $i \in \underline{n}_{\text{ı}}$

$$\sum_{j \in \underline{n}_{\text{ı}}} v_j b_{i,j}(y_{\alpha\beta}) f(\alpha, \beta) = v_i y_{\alpha\beta} f(\alpha, \beta) = v_i y_\alpha y_\beta = \sum_{j \in \underline{n}_{\text{ı}}} v_j b_{i,j}(y_\alpha) y_\beta$$
$$= \sum_{j \in \underline{n}_{\text{ı}}} v_j y_\beta \big(b_{i.j}(y_\alpha)\big)\beta = \sum_{j,k \in \underline{n}_{\text{ı}}} v_j b_{k,j}(y_\beta) \big(b_{i,k}(y_\alpha)\big)\beta.$$

L'ipotesi e (1) implicano che $f(\alpha, \beta) \in L$, quindi

$$\forall i, j \in \underline{n}_{\text{ı}} \quad b_{i,j}(y_{\alpha\beta}) f(\alpha, \beta) = \sum_{k \in \underline{n}_{\text{ı}}} \big(b_{i,k}(y_\alpha)\big)\beta\, b_{k,j}(y_\beta),$$

ossia l'equazione di matrici $\big(b_{i,j}(y_{\alpha\beta})\big)_{i,j} \cdot f(\alpha, \beta) = \big((b_{i,j}(y_\alpha))\beta\big)_{i,j} \cdot \big(b_{i,j}(y_\beta)\big)_{i,j}$. Applicando il determinante otteniamo $(\det y_{\alpha\beta}\delta) f(\alpha, \beta)^n = (\det y_\alpha \delta)\beta \cdot (\det y_\beta \delta)$. □

In 2.11, 2.12, 2.13 abbiamo *analizzato* la situazione di un'algebra associativa unitaria A contenente un campo di ampliamento del campo di base K. L'equazione ottenuta in 2.13(1) mostra che, nel caso che $f(\alpha, \beta) \in L$ per ogni $\alpha, \beta \in G$, lo L-spazio vettoriale destro generato dagli elementi y_α è moltiplicativamente chiuso, quindi una sottoalgebra di A. Adesso prendiamo la strada opposta e *partiamo* da uno spazio vettoriale destro su L nel quale *definiamo* un prodotto tramite tale equazione, all'inizio rispetto a una funzione f arbitraria da $G \times G$ in $\dot{L}$. Lo scopo sarà arrivare in questo modo ad una costruzione di un'algebra associativa unitaria contenente L e ad un criterio quando tale algebra sia centrale semplice. Così l'analisi viene completata con una *sintesi*:

2.14. PROPOSIZIONE. *Sia L un campo di ampliamento di K, $G \leq \mathrm{Aut}_K L$, V uno spazio vettoriale destro su L di dimensione $|G|$, e sia data una biiezione $\alpha \mapsto y_\alpha$ da G su una L-base di V. Sia f un'applicazione da $G \times G$ in $\dot{L}$. Estendiamo distributivamente su tutto V il seguente prodotto:*

$$\forall \alpha, \beta \in G \; \forall a, b \in L \quad y_\alpha a \bullet y_\beta b := y_{\alpha\beta} f(\alpha, \beta)\, a\beta\, b.$$

(1) *La funzione $\iota_L : L \to V$, $b \mapsto y_{\mathrm{id}_L} b$, è un omomorfismo moltiplicativo unitale se e solo se $f(\mathrm{id}_L, \mathrm{id}_L) = 1_L$.*

(2) *y_{id_L} è neutro rispetto a $\bullet$ se e solo se*

$$\forall \alpha \in G \quad f(\alpha, \mathrm{id}_L) = 1_L = f(\mathrm{id}_L, \alpha).$$

Se vale questa condizione, allora $(V, +, \bullet)$ è una K-algebra.[23]

(3) *$\bullet$ è associativa se e solo se*

$$\forall \alpha, \beta, \gamma \in G \quad f(\alpha\beta, \gamma) f(\alpha, \beta)\gamma = f(\alpha, \beta\gamma) f(\beta, \gamma).$$

DIMOSTRAZIONE. (1) $y_{\mathrm{id}_L} a \bullet y_{\mathrm{id}_L} b = y_{\mathrm{id}_L} f(\mathrm{id}_L, \mathrm{id}_L) ab$ per ogni $a, b \in L$, quindi la tesi.

(2) Siano $\alpha, \beta \in G$. Vale $y_\alpha a \bullet y_{\mathrm{id}_L} = y_\alpha f(\alpha, \mathrm{id}_L) a$, $y_{\mathrm{id}_L} \bullet y_\alpha a = y_\alpha f(\mathrm{id}_L, \alpha) a$ per ogni $a \in L$. Quindi vale la prima affermazione. Inoltre, per ogni $a, b \in L$, $c \in K$ si ha

$$\begin{aligned}
(y_\alpha a \bullet y_\beta b) \bullet \mathrm{id}_L c &= y_{\alpha\beta} f(\alpha\beta, \mathrm{id}_L) f(\alpha, \beta)\, a\beta\, bc \\
y_\alpha a \bullet (y_\beta b \bullet \mathrm{id}_L c) &= y_{\alpha\beta} f(\alpha, \beta)\, a\beta\, f(\beta, \mathrm{id}_L)\, bc \\
(y_\alpha a \bullet \mathrm{id}_L c) \bullet y_\beta b &= y_{\alpha\beta} f(\alpha, \beta) f(\alpha, \mathrm{id}_L)\beta\, a\beta\, cb
\end{aligned}$$

Dunque $(V, +, \bullet)$ è una K-algebra se e solo se $f(\alpha\beta, \mathrm{id}_L) = f(\beta, \mathrm{id}_L) = f(\alpha, \mathrm{id}_L)\beta$ per ogni $\alpha, \beta \in G$. Banalmente questa condizione è soddisfatta se $f(\alpha, \mathrm{id}_L) = 1_L$ per ogni $\alpha \in G$.

(3) Per ogni $\alpha, \beta, \gamma \in G$, $a, b, c \in L$ valgono le equazioni

$$\begin{aligned}
(y_\alpha a \bullet y_\beta b) \bullet y_\gamma c &= y_{\alpha\beta\gamma} f(\alpha\beta, \gamma) f(\alpha, \beta)\gamma\; a\beta\gamma\; b\gamma\, c, \\
y_\alpha a \bullet (y_\beta b \bullet y_\gamma c) &= y_{\alpha\beta\gamma} f(\alpha, \beta\gamma)\; a\beta\gamma\, f(\beta, \gamma)\; b\gamma\, c,
\end{aligned}$$

quindi la tesi. □

2.15. DEFINIZIONE. *Siano date le ipotesi di* 2.14. *L'algebra $(V, +, \bullet)$ si chiama il* prodotto incrociato *di L con G rispetto all'applicazione $f \in \dot{L}^{G\times G}$, in breve denotato V_f.*[24] *Da* 2.14(1),(2) *otteniamo*

2.15.1. *Per ogni $f \in \dot{L}^{G\times G}$ tale che $f(\alpha, \mathrm{id}_L) = 1_L = f(\mathrm{id}_L, \alpha)$ per ogni $\alpha \in G$, V_f è una K-algebra unitaria e ι_L un monomorfismo unitale da L in V_f.* □

Poi, 2.14(3) è un criterio per l'associatività di V_f. Viceversa vale:

[23] È facile vedere che, più precisamente, $e \in V$ è neutro rispetto a $\bullet$ se e solo se $e = y_{\mathrm{id}_L} f(\mathrm{id}_L, \mathrm{id}_L)^{-1}$ e $f(\alpha, \mathrm{id}_L) = f(\mathrm{id}_L, \mathrm{id}_L) = f(\mathrm{id}_L, \alpha)\alpha^{-1}$ per ogni $\alpha \in G$. Inoltre, $(V, +, \bullet)$ è una K-algebra se e solo se $f(\alpha, \mathrm{id}_L) = f(\mathrm{id}_L, \mathrm{id}_L) = f(\mathrm{id}_L, \mathrm{id}_L)\alpha$ per ogni $\alpha \in G$.

[24] Per fare la costruzione in 2.14 basterebbe avere un'*azione* di G su L al posto dell'ipotesi che $G \leq \mathrm{Aut}_K L$. Se allora si sceglie l'azione banale ($a\beta = a$ per ogni $a \in L$, $\beta \in G$) e $f(\alpha, \beta) = 1_L$ per ogni $\alpha, \beta \in G$, nasce una L-algebra isomorfa all'anello gruppale LG di G su L. Il prodotto incrociato quindi può essere visto come una generalizzazione dell'anello gruppale in due direzioni: da una parte gioca un ruolo un'azione del gruppo sul campo L, dall'altra parte anche un sistema di fattori, l'applicazione $f : G \times G \to \dot{L}$.

2.15.2. *Sia A un'algebra associativa unitaria, L un sottocampo unitale di A tale che $K \leq L$, G come in* 2.12 *e* $\dim_L A = |G|$ [25]*. Allora A è isomorfa ad un prodotto incrociato V_f di L con G rispetto a un'applicazione $f \in \dot{L}^{G\times G}$ tale che*

$$f(\alpha, \mathrm{id_L}) = 1_L = f(\mathrm{id}_L, \alpha), \quad f(\alpha\beta, \gamma)f(\alpha, \beta)\gamma = f(\alpha, \beta\gamma)f(\beta, \gamma)$$

per ogni $\alpha, \beta, \gamma \in G$.

Dimostrazione. Per ogni $\alpha \in G$ scegliamo y_α come in 2.12 e specialmente $y_{\mathrm{id}_L} := 1_A$. Se ora f è come in 2.13, sono soddisfatte le ipotesi di 2.14, per 2.12(2) e 2.13(1). Ne segue la tesi. □

Nel caso di un'estensione galoissiana (K, L) e $G := \mathrm{Aut}_K L$, il prodotto incrociato per la scelta banale $f(\alpha, \beta) = 1_L$ per ogni $\alpha, \beta \in G$ è isomorfo all'algebra matriciale $K^{n\times n}$ (dove $n = \dim_K L$), come seguirà da un risultato generale nel capitolo successivo (3.4). Ora consideriamo un esempio che in un certo senso è «il minimo caso non banale».

Esempio. Sia L un campo di ampliamento di K, $\sigma \in \mathrm{Aut}_K L$ di ordine finito n, $G = \langle\sigma\rangle$. Consideriamo un elemento $z \in \dot{L}$ tale che $z\sigma = z$ e poniamo

$$f_z : G \times G \to L, \quad (\sigma^i, \sigma^j) \mapsto \begin{cases} 1_L & \text{se } i + j < n \\ z & \text{se } i + j \geq n \end{cases} \quad (0 \leq i, j < n).$$

Sia φ l'isomorfismo dell'L-spazio vettoriale destro V_{f_z} sull'L-spazio vettoriale sinistro $L_{\sigma,z}$ (v. p. 5) tale che $y_{\sigma^i} a \mapsto a x^i$ per ogni $i \in \underline{n-1}_{\,|} \cup \{0\}$, $a \in L$. Per la definizione della moltiplicazione in $L_{\sigma,z}$ si ha, per ogni $a, b \in L$, $i, j \in \underline{n-1}_{\,|} \cup \{0\}$,

$$(y_{\sigma^i} a \bullet y_{\sigma^j} b)\varphi = (y_{\sigma^{i+j}} f_z(\sigma^i, \sigma^j)\, a\sigma^j\, b)\varphi = \begin{cases} b\, a\sigma^j\, x^{i+j} & \text{se } i + j < n \\ b\, a\sigma^j\, z\, x^{i+j-n} & \text{se } i + j \geq n \end{cases}$$
$$= bx^j \cdot ax^i = (y_{\sigma^j} b)\varphi \cdot (y_{\sigma^i} a)\varphi.$$

Pertanto vale

2.16. Proposizione. *Sia (K, L) un'estensione di campi di dimensione finita, $\sigma \in \mathrm{Aut}_K L$, $z \in \dot{K}$ e f_z come sopra. Allora vale $V_{f_z}^- \cong L_{\sigma,z}$.* □

In particolare, V_{f_z} è associativa, cioè, soddisfa alla condizione in 2.14(3). Nel seguito consideremo tale condizione in una veste più generale.

[25] Senza quest'ipotesi possiamo sempre fare le scelte di y_α e f come nella dimostrazione e, per 2.12(1), applicare l'osservazione alla K-sottoalgebra $\langle y_\alpha | \alpha \in G\rangle_L$ al posto di A.