CAPITOLO 1

# Algebre di divisione e prodotti tensoriali

Prima di iniziare lo studio delle algebre semplici di dimensione finita in generale vogliamo dare una costruzione di un tipo di algebra che, come nel caso dei quaternioni, in molti casi risulta essere un'algebra di divisione :

1.1. DEFINIZIONE. *Sia $L$ un ampliamento di un campo $K$, $\sigma \in \mathrm{Aut}_K L$. Consideriamo lo spazio vettoriale $L[t]$ dei polinomi su $L$ e definiamo la seguente operazione:*

$$\forall a, b \in L\ \forall i, j \in \mathbb{N}_0 \quad at^i \cdot bt^j := a(b\sigma^i)t^{i+j},$$

*estesa secondo la legge distributiva alla chiusura additiva degli elementi $at^i$, cioè, a $L[t]$. Siccome $c\sigma = c$ per ogni $c \in K$, sono soddisfatti gli assiomi di una $K$-algebra. Poi, la operazione è associativa e $1_L t^0$ è neutro. Scriviamo $L[t, \sigma]$ per l'algebra associativa unitaria ottenuta in questo modo, detta il* twist di Hilbert [7] *di $L$ tramite $\sigma$. Come nel caso classico di un anello dei polinomi su un campo si dimostra*

1.1.1. *$L[t, \sigma]$ è un anello ad ideali sinistri principali,*

*cioè, per ogni ideale sinistro $J$ di $L[t, \sigma]$ esiste un $f \in L[t]$ tale che $J = L[t, \sigma] \cdot f$. Ora sia $\sigma$ di ordine finito $n$. Allora $t^n \in Z(L[t, \sigma])$. Per ogni $z \in \dot{K}$* [8] *anche $t^n - z \in Z(L[t, \sigma])$ e $J_z := (t^n - z) \cdot L[t, \sigma]$ è un ideale di $L[t, \sigma]$. Poniamo*

$$L_{\sigma,z} := L[t, \sigma]/J_z, \quad x := J_z + t.$$

*Allora $x^n = J_z + z = z \cdot x^0$, e gli elementi di $L_{\sigma,z}$ hanno un'unica rappresentazione nella forma*

$$\sum_{i=0}^{n-1} b_i x^i \quad (b_i \in L).$$

*L'applicazione $L \to L_{\sigma,z}$, $a \mapsto a \cdot x^0$, è un'immersione. È comodo scrivere $a$ al posto di $a \cdot x^0$ (quindi $1_L = x^0$). Un'algebra $A$ si dice* ciclica *su $K$ se $A \cong L_{\sigma,z}$ per un ampliamento galoissiano $L$ di $K$ tale che $\mathrm{Aut}_K L = \langle \sigma \rangle$ e un elemento $z \in \dot{K}$ (Dickson 1906).*

1.1.2. *Se $(K, L)$ è galoissiana, $\mathrm{Aut}_K L = \langle \sigma \rangle$, allora $\dim_K L_{\sigma,z} = o(\sigma)$,*

*perché $\dim_K L = |\langle \sigma \rangle|$.*

1.2. TEOREMA. *Sia $(K, L)$ un'estensione galoissiana, $n := \dim_K L$, $z \in \dot{K}$, $\mathrm{Aut}_K L = \langle \sigma \rangle$ ciclico, $A := L_{\sigma,z}$. Allora si ha*

(1) *$A$ è centrale semplice, $L\iota = C_A(L\iota)$,*
(2) *$A \cong K^{n \times n} \Leftrightarrow \exists b \in \dot{L} \quad \prod_{i=0}^{n-1} b\sigma^i = z$,*

[7] Il *twist* non è solo una danza degli anni 60 del tipo rock and roll ma ha anche il significato dello ≪storcere≫: L'anello ordinario dei polinomi su $L$ viene ≪storto≫ mediante $\sigma$.

[8] Per ogni corpo $D$ poniamo $\dot{D} := D \setminus \{0_D\}$.

(3) *Se $n$ è un numero primo, o $A \cong K^{n\times n}$ o $A$ è un'algebra di divisione su $K$.*

Ogni costruzione di un'algebra centrale semplice $A$ di dimensione finita su un campo $K$ porta in modo unico (a meno di isomorfismi) ad un'algebra di divisione centrale $D$ su $K$ tramite l'isomorfismo $A \cong D^{m\times m}$ che si ottiene dai risultati di Wedderburn (v. Introduzione). In particolare, con riferimento a (1), questo vale per la costruzione dell'algebra ciclica. La parte (2) esprime un criterio per decidere se l'algebra di divisione $D$ ottenuta in quella maniera è «noiosa» (cioè, $\cong K$) o meno. Data un'estensione $(K, L)$ galoissiana con gruppo di Galois $G$, per ogni $b \in L$ si dice norma di $b$ il prodotto $b\mathcal{N} := \prod_{\varphi\in G} b\varphi$. Evidentemente $\mathcal{N}$ è un omomorfismo moltiplicativo da $L$ nel campo degli elementi fissati da $G$, cioè, in $K$. Secondo (2) la scelta di $z$ decide se l'algebra di divisione che si ottiene mediante la costruzione di $L_{\sigma,z}$ risulta essere banale ($\cong K$) o interessante, un esempio *proprio*: quest'ultimo è il caso se e solo se $z$ *non* è norma di un elemento di $L$, cioè, se e solo se $z \notin \dot{L}\mathcal{N}$. Nel caso di un primo $n$, secondo (3) ci sono soltanto due alternative: O si tratta di un caso banale nel senso di cui sopra oppure l'algebra $L_{\sigma,z}$ stessa è già un'algebra di divisione. Questa parte del teorema è un caso speciale di un risultato molto più generale in cui l'ordine della classe laterale di $z$ nel gruppo quoziente $\dot{K}/\dot{L}\mathcal{N}$ gioca un ruolo importante.[9]

Spostiamo la dimostrazione di (1) perché si tratta di un caso speciale di un risultato generale che dimostreremo più tardi (v. p. 24). Però, faremo uso di (1) nelle dimostrazioni delle altre parti del teorema. Come preparazione dimostriamo il seguente caso speciale di (2):

1.2.1. *Sia $(K, L)$ un'estensione galoissiana, $n := \dim_K L$, $\mathrm{Aut}_K L = \langle\sigma\rangle$ ciclico. Allora $L_{\sigma,1_K} \cong K^{n\times n}$.*

Dimostrazione. L'ideale destro $(t - 1_K)L[t,\sigma]$ di $L[t,\sigma]$ è di co-dimensione $n$ su $K$ e contiene $J_{1_K}$ perché $t^n - 1_K = (t - 1_K)(t^{n-1} + \cdots + t + 1_K)$. Il quoziente è un modulo unitale dell'algebra $L_{\sigma,1_K}$. Ne segue che esiste un omomorfismo unitale da $L_{\sigma,1_K}$ in $K^{n\times n}$ che, per (1), deve essere iniettivo. Ma $\dim_K L_{\sigma,1_K} = n^2 = \dim_K K^{n\times n}$, allora vale la tesi. □

Dimostrazione. (2) $\Rightarrow$: Sia $A \cong K^{n\times n}$. Siccome ogni ideale sinistro massimale di $K^{n\times n}$ è di co-dimensione $n$ troviamo un ideale sinistro $Q$ di $L[t,\sigma]$ tale che

$$L[t,\sigma](t^n - z) \subseteq Q,\ \dim_K L[t,\sigma]/Q = n.$$

Per 1.1.1 esiste un polinomio normato $f \in L[t,\sigma]$ tale che $Q = L[t,\sigma]f$. Le potenze di $t$ di grado $< \deg f$ formano una $L$-base di $L[t,\sigma]$ modulo $Q$ e allora $n = \dim_K L \cdot \deg f$. Ne segue che $\deg f = 1$, $f = t - b$ per un $b \in L$. Siccome $t^n - z \in Q$ esistono $a_0, \ldots, a_{n-1} \in L$ tali che

$$\begin{aligned} t^n - z &= (a_{n-1}t^{n-1} + \cdots + a_1 t + a_0)(t - b) \\ &= (a_{n-1}t^n + \cdots + a_0 t) - (a_{n-1}t^{n-1}b + \cdots + a_1 tb + a_0 b) \\ &= a_{n-1}t^n + \sum_{j\in\underline{n-1}} \big(a_{j-1} - a_j(b\sigma^j)\big)t^j - a_0 b. \end{aligned}$$

[9] **Teorema** (Wedderburn 1914) *Siano soddisfatte le ipotesi di* 1.2. *Se, nel gruppo $\dot{K}/\dot{L}\mathcal{N}$, vale $o((\dot{L}\mathcal{N})z) = n$, allora $A$ è un'algebra di divisione su $K$.*

L'ipotesi sull'ordine di $(\dot{L}\mathcal{N})z$ è sufficiente, ma necessaria solo sotto ipotesi adatte su $K$, per esempio, se $K$ è un campo numerico (v. [**L**], 5.§14).

Consegue che $a_{n-1} = 1_L$, $\forall j \in \underline{n-1}_{\mid}$ $a_{j-1} = a_j(b\sigma^j)$, $a_0 b = z$, allora $b \in \dot{L}$ e inoltre

$$a_0 = a_1(b\sigma) = a_2(b\sigma^2)(b\sigma) = \cdots = \underset{=1_L}{a_{n-1}}(b\sigma^{n-1})\cdots(b\sigma^2)(b\sigma),$$

quindi $z = a_0 b = \prod_{i=0}^{n-1} b\sigma^i$.

$\Leftarrow$: Sia $b \in \dot{L}$ tale che $\prod_{i=0}^{n-1} b\sigma^i = z$. Poniamo $y := b^{-1}x$. Allora

$$y^n = \underset{n}{(b^{-1}x)\cdots(b^{-1}x_n)} = \underbrace{(b^{-1}\sigma^{n-1})\cdots(b^{-1}\sigma)b^{-1}}_{=z^{-1}} \underset{=z}{x^n} = 1_A,$$

$ya = b^{-1}xa = b^{-1}(a\sigma)x = (a\sigma)y$ per ogni $a \in L$. Ne segue che esiste un omomorfismo da $L_{\sigma,1_K}$ in $A$ che manda $x$ in $y$. Grazie a 1.2.1 e alla semplicità di $K^{n\times n}$ ne segue che $A \cong K^{n\times n}$.

(3) Per (1) sappiamo che $A \cong D^{m\times m}$ per un'algebra centrale di divisione $D$ e un $m \in \mathbb{N}$, quindi vale $n^2 = \dim_K A = (\dim_K D)m^2$. Essendo $n$ un primo ne segue che o $\dim_K D = 1$, $A \cong K^{n\times n}$, oppure $m = 1$, $A \cong D$. □

Per esempio, se $L$ è il campo di riducibilità completa del polinomio $t^3+t^2-2t-1$ su $\mathbb{Q}$ in $\mathbb{C}$ e $a \in L$ è uno dei suoi zeri, allora vale[10] : $\operatorname{Aut} L$ è ciclico, generato da un automorfismo $\sigma$ che porta $a$ in $a^2-2$, $\dim_{\mathbb{Q}} L = 3$, $\forall b \in L \quad b \cdot b\sigma \cdot b\sigma^2 \neq 2$. Per 1.2(2), $L_{\sigma,2} \ncong \mathbb{Q}^{2\times 2}$. Allora $L_{\sigma,2}$ è algebra di divisione, per 1.2(3), e $\dim_{\mathbb{Q}} L_{\sigma,2} = 9$.

Come caso speciale della costruzione di $L_{\sigma,z}$ consideriamo poi un campo $K$ tale che il polinomio $t^2+1_K$ sia irriducibile in $K[t]$, e sia $L$ un campo di riducibilità completa su $K$, $i \in L$ tale che $i^2 = -1_K$. Allora $\operatorname{Aut}_K L = \{\mathrm{id}_L, \sigma\}$ dove $\sigma$ è l'automorfismo di $L$ che porta $a+bi$ in $a-bi$, per ogni $a, b \in K$. Sia $A := L_{\sigma,-1_K}$. Allora $\dim_K A = 4$ e $i^2 = -1_A = x^2$, $i \cdot x = ix = -x \cdot i$. Ne segue che $A \cong H(K)$. *L' algebra dei quaternioni su $K$ è un'algebra ciclica se $t^2+1$ è irriducibile su $K$.* Il caso classico studiato da Hamilton è $K = \mathbb{R}$.

1.2.2. *Sia $a$ un elemento di un'algebra associativa su un anello commutativo unitario $K$. Allora la sottoalgebra generata da $a$ è $\langle a, a^2, a^3, \dots\rangle_K$, in particolare è commutativa.* □

1.3. Proposizione. *Sia $K$ un campo, $D$ un'algebra di divisione su $K$.*

(1) *Se $a \in \dot{D}$ è algebrico su $K$ e $T$ è l'algebra generata da $a$, allora $T$ è un campo di dimensione finita su $K$. Ogni sottoalgebra algebrica $\neq \{0_D\}$ di $D$ è un'algebra di divisione.*

(2) *Se $K$ è algebricamente chiuso, allora ogni elemento di $D \setminus K\iota$ è trascendente su $K$. In particolare, se $D$ è algebrica su $K$, allora $D = K\iota$.*

Dimostrazione. (1) Siccome $a$ è algebrico su $K$, $T$ è di dimensione finita su $K$, per 1.2.2. La moltiplicazione a destra $\rho_a : T \to T$, $x \mapsto xa$, essendo $K$-lineare e iniettiva, deve quindi essere anche suriettiva. In particolare esiste $x \in T$ tale che $xa = a$. Siccome $a$ è invertibile, consegue che $x = 1_D$. Allora $1_D \in T$ e, di nuovo per la suriettività di $\rho_a$, esiste $y \in T$ tale che $ya = 1_D$, cioè, $a^{-1} \in T$.

(2) Per ogni $a \in D$ algebrico su $K$ la sottoalgebra unitaria generata da $a$ è un campo, per 1.2.2 e (1). Ma il suo sottocampo $K\iota \cong K$ è algebricamente chiuso, implicando che $a \in K\iota$. Ne segue che $K\iota = D$. □

[10] da verificarsi!

Si vede allora: Su un campo algebricamente chiuso $K$ non esiste alcun'algebra di divisione di dimensione finita tranne $K$, a meno di isomorfismi. Sul campo $\mathbb{R}$ si hanno, come algebre di divisione *centrali* di dimensione finita, almeno $\mathbb{R}$ e $\mathbb{H}$. Su $\mathbb{Q}$ invece conosciamo $\mathbb{Q}$, $H(\mathbb{Q})$, l'algebra di divisione di dimensione 9 costruita come esempio dopo 1.2, e tale costruzione evidentemente lascia molto spazio per esempi simili. Pertanto non si può aspettare una soluzione facile del Problema 1 nel caso generale. La descrizione delle algebre di divisione centrali di dimensione finita su $\mathbb{Q}$ è stato uno degli argomenti principali della teoria intorno al 1930. Il problema è stato risolto grazie agli sforzi dei grandi del tempo: Albert, Brauer, Hasse, Noether. Un risultato bellissimo in questo ambito è il seguente famoso teorema che, però, non dimostreremo:

**Teorema** (Hasse-Brauer-Noether, Albert (1931)) *Ogni algebra di divisione centrale di dimensione finita su un campo numerico $K$ è un'algebra ciclica su $K$.*

Il metodo per studiare il nostro argomento farà un uso esteso del concetto di prodotto tensoriale di algebre associative unitarie che tratteremo nel seguito.

Sia $A$ un'algebra associativa unitaria su un campo $K$, $V$ uno spazio vettoriale su $K$. Per ogni rappresentazione $\delta : A \to \mathrm{End}_K V$ poniamo

$$\mathrm{End}(V, \delta) := C_{\mathrm{End}_K V}(A\delta),$$

la sottoalgebra di $\mathrm{End}_K V$ degli elementi di $V$ che commutano con ogni endomorfismo indotto da $A$. Gli elementi di $\mathrm{End}(V, \delta)$ vengono chiamati *$\delta$-endomorfismi* di $V$. Se viene discussa un'unica rappresentazione di $A$ (con il modulo $V$), allora si usa la scrittura $\mathrm{End}_A V$ al posto di $\mathrm{End}(V, \delta)$ e si parla di $A$-endomorfismi invece di $\delta$-endomorfismi. È utile notare che, per queste nozioni, basta che $\delta$ sia una *funzione lineare* (anziché, più strettamente, un omomorfismo di algebre), anche se nella maggioranza delle applicazioni in questa teoria $\delta$ sarà anche un omomorfismo moltiplicativo. Se $\delta$ è un omomorfismo di $A$ *come algebra*, $\delta$ è detto unitale se $1_A\delta = \mathrm{id}_V$. Più in generale, se $A$, $B$ sono algebre unitarie, un omomorfismo $\delta$ da $A$ in $B$ viene chiamato unitale se $1_A\delta = 1_B$. Nello stesso spirito[11] una sottoalgebra unitaria $T$ di $A$ è detta unitale se $1_T = 1_A$.

Come «caso di base» può essere considerato lo spazio $V = A$ nel quale, però, ci vuole una specificazione dell'azione di $A$ perché abbiamo già incontrato due candidati naturali: $\lambda$ e $\rho$; ricordiamo che di questi solo $\rho$ è una rappresentazione di $A$ come algebra.

1.4. Proposizione. *Per ogni $K$-algebra associativa unitaria $A$ vale*

(1) $\mathrm{End}(A, \rho) = A\lambda \cong A^-$, $\mathrm{End}(A, \lambda) = A\rho \cong A$,
(2) $Z(A)\lambda = A\lambda \cap A\rho = Z(A)\rho$.

Dimostrazione. Per ogni $\alpha \in \mathrm{End}\, A$ poniamo $a_\alpha := 1_A\alpha$. Se $\alpha \in \mathrm{End(A}, \rho)$, $y \in A$, si ha $y\alpha = (1_A y)\alpha = (1_A\alpha)y = a_\alpha y$, quindi vale $\alpha = a_\alpha\lambda \in A\lambda$. Se $\alpha \in A\lambda \cap A\rho$, allora $y(a_\alpha\lambda) = a_\alpha y = (1_A\alpha)(y\rho) = \big(1_A(y\rho)\big)\alpha = y\alpha$ perché $\alpha \in A\lambda \subseteq \mathrm{End}(A, \rho)$, e similmente $y(a_\alpha\rho) = y\alpha$. Osservando che per ogni $a, b \in A$ vale $a\lambda = b\rho$ se e solo se $a = b \in Z(A)$, ne seguono facilmente le tesi. □

Se $T, T'$ sono sottospazi di un'algebra, denotiamo con $TT'$ la chiusura additiva dell'insieme dei prodotti $xx'$ ($x \in T$, $x' \in T'$).

[11] visto che non faremo uso del linguaggio delle categorie

1.4.1. *Siano $A, B$ sottoalgebre di un'algebra associativa $Q$ tali che $xy = yx$ per ogni $x \in A$, $y \in B$. Allora $AB$ è una sottoalgebra di $Q$. In particolare, per ogni algebra associativa $A$, $(A\lambda)(A\rho)$ è una sottoalgebra di* $\mathrm{End}_K(A,+)$,

perché $xyx'y' = xx'yy'$ per ogni $x, x' \in A$, $y, y' \in B$. □

1.5. Definizione. *Siano $A, B$ $K$-algebre associative unitarie. Una* realizzazione prodotto *per $(A,B)$ è una terna $(Q, \varphi, \psi)$ dove $Q$ è un'algebra associativa unitaria e $\varphi : A \to Q$, $\psi : B \to Q$ sono omomorfismi unitali tali che $(x\varphi)(y\psi) = (y\psi)(x\varphi)$ per ogni $x \in A$, $y \in B$.*

Esempi:

(1) $(\mathrm{End}_K(A,+), \lambda, \rho)$ è una realizzazione prodotto per $(A^-, A)$.
(2) $(A^{n\times n}, \varphi, \psi)$ è una realizzazione prodotto per $(K^{n\times n}, A)$ dove $\varphi : (c_{ij}) \mapsto (c_{ij}1_A)$, $\psi : y \mapsto diag(y, \dots, y)$.
(3) Siano $A$, $B$ sottoalgebre unitali di un'algebra associativa unitaria $S$ tali che $xy = yx$ per ogni $x \in A$, $y \in B$. Sia $\partial$ una derivazione $A \to C_S(B)$. [12] Allora $(S^{2\times 2}, \varphi, \psi)$ è realizzazione prodotto per $(A, B)$ dove

$$\varphi : x \mapsto \begin{pmatrix} x & x\partial \\ 0_S & x \end{pmatrix}, \quad \psi : y \mapsto \begin{pmatrix} y & 0_S \\ 0_S & y \end{pmatrix}$$

1.6. Proposizione. *Siano $K$ un campo e $A$, $B$, $K$-algebre associative unitarie. Allora esiste una realizzazione prodotto $(T, \varphi, \psi)$ per $(A, B)$ con le seguenti proprietà:*

(i) $(A\varphi)(B\psi) = T$,
(ii) *Se $(Q, \tilde{\varphi}, \tilde{\psi})$ è una realizzazione prodotto per $(A, B)$, allora esiste un omomorfismo unitale $\sigma$ da $T$ in $Q$ tale che $\varphi\sigma = \tilde{\varphi}$, $\psi\sigma = \tilde{\psi}$.*

*Costruzione di $T$*: Sia $X$ una $K$-base di $A$, $1_A \in X$, $Y$ una $K$-base di $B$, $1_B \in Y$. Poniamo $Z := X \times Y$. Sia $T$ un $K$-spazio con base $Z$. Definiamo un prodotto in $T$ tramite estensione distributiva del seguente prodotto per gli elementi di $Z$:

$$(x_1, y_1) \cdot (x_2, y_2) := \sum_x \sum_y c_{x_1x_2x} d_{y_1y_2y}(x, y)$$

dove $c_{x_1x_2x}, d_{y_1y_2y} \in \dot{K}$ sono tali che $x_1x_2 = \sum_x c_{x_1x_2x}x$, $y_1y_2 = \sum_y d_{y_1y_2y}y$ ( dove $x$ trascorre una parte finita di $X$, similmente $y$ una parte finita di $Y$). Allora $T$ è un'algebra associativa unitaria ($1_T = (1_A, 1_B) \in Z$).

Sia $\varphi$ la funzione $K$-lineare da $A$ in $T$ tale che $x\varphi = (x, 1_B)$ per ogni $x \in X$. È facile vedere che $\varphi$ è un monomorfismo unitale dell'*algebra* $A$ in $T$. Similmente, questo vale per $\psi : B \to T$, $y \mapsto (1_A, y)$, e si ha

$$\forall x \in X \, \forall y \in Y \quad (x, 1_B) \cdot (1_A, y) = (x, y) = (1_A, y) \cdot (x, 1_B),$$

quindi $(x\varphi)(y\psi) = (y\psi)(x\varphi)$. Pertanto $(T, \varphi, \psi)$ è una realizzazione prodotto per $(A, B)$ e vale (i). Inoltre siano $Q$ un'algebra associativa unitaria, $\tilde{\varphi} : A \to Q$, $\tilde{\psi} : B \to Q$ omomorfismi unitali (di algebre) tali che $(a\tilde{\varphi})(b\tilde{\psi}) = (b\tilde{\psi})(a\tilde{\varphi})$. La funzione lineare $\sigma$ da $T$ in $Q$ tale che $(x, y)\sigma = (x\tilde{\varphi})(y\tilde{\psi})$ per ogni $x \in X$, $y \in Y$,

[12] cioè, $\partial$ è lineare e $(xx')\partial = x(x'\partial) + (x\partial)x'$ per ogni $x, x' \in A$.

risulta essere un omomorfismo unitale di algebre e $\varphi\sigma = \tilde{\varphi}$, $\psi\sigma = \tilde{\psi}$: Per ogni $x_1, x_2 \in X$, $y_1, y_2 \in Y$ vale

$$(x_1, y_1)\sigma \cdot (x_2, y_2)\sigma = (x_1\tilde{\varphi})(y_1\tilde{\psi})(x_2\tilde{\varphi})(y_2\tilde{\psi}) = (x_1\tilde{\varphi})(x_2\tilde{\varphi})(y_1\tilde{\psi})(y_2\tilde{\psi})$$
$$= (x_1x_2)\tilde{\varphi}(y_1y_2)\tilde{\psi} = \sum_x \sum_y c_{x_1x_2x} d_{y_1y_2y} (x\tilde{\varphi})(y\tilde{\psi}) = \big((x_1, y_1) \cdot (x_2, y_2)\big)\sigma.$$

Una terna $(T, \varphi, \psi)$ come in 1.6 si dice un prodotto tensoriale esterno di $A$ con $B$, la proprietà (ii) si dice la proprietà universale di $T$. Applicandola vediamo che un prodotto tensoriale non solo esiste, come appena dimostrato tramite la costruzione, ma è anche unico a meno di isomorfismi:

1.6.1. *Se $(T, \varphi, \psi)$, $(\tilde{T}, \tilde{\varphi}, \tilde{\psi})$ sono prodotti tensoriali di $A$ con $B$, allora l'omomorfismo $\sigma$ in* 1.6(ii) *(con $Q := \tilde{T}$) è un isomorfismo,*

perchè esiste, per la proprietà universale di $(\tilde{T}, \tilde{\varphi}, \tilde{\psi})$, un omomorfismo $\tilde{\sigma}$ da $\tilde{T}$ in $T$ tale che $\tilde{\varphi}\tilde{\sigma} = \varphi$, $\tilde{\psi}\tilde{\sigma} = \psi$. Allora $\sigma\tilde{\sigma} = \mathrm{id}_T$, $\tilde{\sigma}\sigma = \mathrm{id}_{\tilde{T}}$, e $\sigma$ è un isomorfismo. □

Date $A$, $B$, fissiamo *una* terna $(T, \varphi, \psi)$ come in 1.6 e, tenuto conto di 1.6.1, chiamiamola *il* prodotto tensoriale di $A$ con $B$. Per avere un riferimento diretto ad $A$, $B$ nella denotazione si scrive

$$A \underset{K}{\otimes} B \text{ per il prodotto tensoriale di } A \text{ con } B,$$
$$a \otimes b \text{ per i suoi generatori } (a\varphi)(b\psi) \quad (a \in A,\ b \in B).$$

$A \underset{K}{\otimes} B$ è la chiusura *additiva* degli elementi $a \otimes b$ ($a \in A$, $b \in B$), anche la chiusura *$K$-lineare* degli elementi $x \otimes y$ ($x \in X$, $y \in Y$). Se $\dim_K A$, $\dim_K B$ sono finite, allora si ottiene direttamente dalla costruzione in 1.6:

1.6.2. $\dim_K A \underset{K}{\otimes} B = \dim_K A \dim_K B$. □

Le proprietà di $\varphi$, $\psi$ implicano le seguenti regole per ogni $c \in K$, $a, a' \in A$, $b, b' \in B$:

$$c(a \otimes b) = (ca) \otimes b = a \otimes (cb)$$
$$(a + a') \otimes (b + b') = a \otimes b + a \otimes b' + a' \otimes b + a' \otimes b'$$
$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

Poi vale $K^{n\times n} \underset{K}{\otimes} A \cong A^{n\times n}$ (v. Esempio (2) in 1.5, $A \underset{K}{\otimes} B \cong B \underset{K}{\otimes} A$, $(A \underset{K}{\otimes} B) \underset{K}{\otimes} C \cong A \underset{K}{\otimes} (B \underset{K}{\otimes} C)$, regole che, però, sono un po' meno banali di quanto sembrano. Abbiamo già notato che le funzioni $A \to A \underset{K}{\otimes} B$, $a \mapsto a \otimes 1_B$, e $B \to A \underset{K}{\otimes} B$, $b \mapsto 1_A \otimes b$, sono immersioni, cioè, monomorfismi (unitali) di algebre.

Se $Q$ è un'algebra associativa unitaria con sottoalgebre $A'$, $B'$ tale che esiste un isomorfismo $\sigma$ da $A \underset{K}{\otimes} B$ su $Q$ con $(A \underset{K}{\otimes} 1_B)\sigma = A'$, $(1_A \underset{K}{\otimes} B)\sigma = B'$, allora scriviamo $Q = A' \dot{\underset{K}{\otimes}} B'$, detto prodotto tensoriale interno di $A'$ con $B'$. Vale $A' \cap B' = K\iota$. Dall'Esempio (1) in 1.5 si ottiene

1.6.3. *Sia $A$ un'algebra associativa unitaria su $K$ e $C := (A\lambda)(A\rho)$. Allora esiste un epimorfismo da $A^- \underset{K}{\otimes} A$ su $C$.* □

1.7. Proposizione. *Sia $A$ un'algebra associativa unitaria di dimensione finita su $K$. Sono equivalenti*

(i) $(A\lambda)(A\rho) = \mathrm{End}_K(A,+)$,
(ii) $\mathrm{End}_K(A,+) \cong A^- \underset{K}{\otimes} A$,
(iii) $A^- \underset{K}{\otimes} A$ *è semplice.*

Dimostrazione. Sia $n := \dim_K A$, $C := (A\lambda)(A\rho)$. Se vale (i), allora

$$\dim_K C = \dim_K \mathrm{End}_K(A,+) = n^2 \underset{1.6.2}{=} \dim_K A^- \underset{K}{\otimes} A.$$

Ne segue (ii) per 1.6.3. L'implicazione (ii)⇒(iii) vale perché $\mathrm{End}_K(A,+) \cong K^{n\times n}$. Se vale (iii), allora l'epimorfismo in 1.6.3 è un isomorfismo e consegue (i): Ambedue le algebre hanno la stessa dimensione. □

Siano $A$, $B$ sottoalgebre di un'algebra associativa unitaria $T$ tali che $T = A\dot{\underset{K}{\otimes}}B$. Allora ogni $K$-base $X$ di $A$ è una $B$-base di $T$: Se $Y$ è una $K$-base di $B$, allora $XY$ è una $K$-base di $T$ (v. la costruzione in 1.6). Per prima cosa, $T = \langle XY\rangle_K = \langle X\rangle_K\langle Y\rangle_K = \langle X\rangle_B$. In secondo luogo, se per un sottoinsieme finito di elementi $x \in X$ vale $\sum_x xb_x = 0_A$ (con $b_x \in B$), allora scriviamo ogni $b_x$ come combinazione $K$-lineare su $Y$ e otteniamo così una combinazione $K$-lineare di prodotti $xy$ che dà $0_A$. Ne segue che tutti gli scalari sono $0_K$, cioè, $b_x = 0_B$ per ogni $x$. Avendo una $B$-base, il $B$-modulo $T$ viene detto $B$-modulo libero. Mettiamo in evidenza due aspetti di questa considerazione:

1° aspetto. Se $K$, $B$ sono *campi*, allora $T$ risulta essere uno spazio vettoriale su $B$, e $B$ un campo di ampliamento di $K\iota$ ($\cong K$). Gli elementi di $B$ vengono così considerati come scalari, e $T$ nasce da $A$ tramite un ampliamento del campo di base, passando da $K$ a $B$. Il prodotto tensoriale $A\underset{K}{\otimes}B$, visto come $B$-algebra, viene anche denotato con $A_B$.

2° aspetto. Se $V$ è un $T$-modulo unitale tramite una rappresentazione (di algebre) $\delta$, allora $\delta_{|A}$ è una rappresentazione unitale di $A$ che porta $A$ in $\mathrm{End}_B V (= C_{\mathrm{End_K V}}(B\delta))$. Un omomorfismo da $A$ (come algebra) in $\mathrm{End}_B V$ si dice una $B$-rappresentazione di $A$. Vice versa, se $V$ è un $B$-modulo unitale, ogni omomorfismo unitale da $A$ (come algebra) in $\mathrm{End}_B V$ induce una rappresentazione unitale di $T$: Le due rappresentazioni $A \to \mathrm{End}_K V$, $B \to \mathrm{End}_K V$ definiscono una realizzazione prodotto per $(A,B)$, e quindi sono estendibili ad una rappresentazione di $T$.

1.7.1. *Siano $A$, $B$ algebre associative unitarie su un campo $K$. Ogni $B$-rappresentazione unitale di $A$ induce una rappresentazione unitale di $A\underset{K}{\otimes}B$ e viceversa.*□

1.8. Proposizione. *Siano $A$, $B$ sottoalgebre di un'algebra associativa unitaria $T$ tali che $T = A\dot{\underset{K}{\otimes}}B$. Allora valgono*

(1) $C_T(B) = A\,Z(B)$
(2) $I \trianglelefteq A$, $J \trianglelefteq B \Rightarrow IJ \trianglelefteq T$, $A \cap IB = I$.

Dimostrazione. (1) Sia $y \in C_T(B)$, $X$ una $K$-base di $A$, e sia dato un insieme finito di elementi $x \in X$ e $b_x \in B$ tali che $y = \sum_x xb_x$. Per ogni $b \in B$ vale

$$\sum_x xb_xb = yb = by = \sum_x bxb_x = \sum_x xbb_x,$$

perché $X \subseteq A \subseteq C_T(B)$. $X$ é $B$-base di $T$, quindi $b_x b = b b_x$, cioè, $b_x \in Z(B)$ per ogni $x$.

(2) Siano $I \trianglelefteq A$, $J \trianglelefteq B$. Per ogni $a \in A$, $b \in B$ si ha $abIJ = aIbJ \subseteq IJ$, similmente $IJab \subseteq IJ$, quindi $IJ \trianglelefteq T$. Poi è ovvio che $I \subseteq A \cap IB$. Per dimostrare l'inclusione opposta sia $y \in A \cap IB$ e $X$ una $K$-base di $A$ contenente una $K$-base $X_I$ di $I$. Scriviamo $y$ come combinazione $K$-lineare di un insieme finito $X'$ di elementi $x \in X$. Siano allora $c_x \in \dot{K}$ tali che

$$y = \sum_{x \in X'} c_x x = \sum_{x \in X'} x(c_x 1_T) \qquad (*)$$

e notiamo che, banalmente, $c_x 1_T \in B$, quindi $(*)$ esprime anche la rappresentazione di $y$ tramite $X$ come $B$-base di $T$. Siccome $y \in IB$ esiste anche una parte finita $X'_I$ di $X_I$ e per ogni $x \in X'_I$ un elemento $b_x \in B \setminus \{0_B\}$ tale che $y = \sum_{x \in X'_I} x b_x$. Ne segue che $X' = X'_I$ e $b_x = c_x 1_T$ per ogni $x \in X'$, allora $y \in \langle X_I \rangle_K = I$. □

1.9. Corollario. *Se $A$ è una $K$-algebra associativa unitaria centrale e $L$ è campo di ampliamento di $K$, allora $A_L$ è una $L$-algebra centrale,*

$$\text{perché } Z(A \underset{K}{\otimes} L) = C_{A \underset{K}{\otimes} L}(A) \cap C_{A \underset{K}{\otimes} L}(L) = LZ(A) \cap AZ(L) = L \cap AL = L. \quad \square$$

Ora sia $\mathcal{I}(A) := \{I | I \trianglelefteq A\}$, $\mathcal{I}(T) := \{J | J \trianglelefteq T\}$. Per 1.8(2) è iniettiva la funzione

$$\tau : \mathcal{I}(A) \to \mathcal{I}(T), \quad I \mapsto IB.$$

1.10. Proposizione. *Siano $A$, $B$ sottoalgebre di un'algebra associativa unitaria $T$ tali che $T = A \underset{K}{\dot{\otimes}} B$. Se $B$ è centrale semplice, allora $\tau$ è biiettiva.*

**Casi speciali**

(1) *$A, B$ centrali $\Rightarrow T$ centrale,*
(2) *$A, B$ semplici, $B$ centrale $\Rightarrow T$ semplice,*
(3) *$A, B$ centrali semplici $\Rightarrow T$ centrale semplice.*

Dimostrazione. Per 1.8(2) $\tau$ è iniettiva. Sia $J \in \mathcal{I}(T)$, $I := A \cap J$. Allora $I \in \mathcal{I}(A)$, $IB \subseteq J$, e il nostro scopo è mostrare che $IB = J$.

Sia $X$ una $K$-base di $A$ contenente una $K$-base $X_I$ di $I$. Assumiamo per assurdo che $IB \subset J$. Allora esiste una combinazione $B$-lineare su $X$ appartenente a $J$ ma non a $IB$. Per ogni $x \in X_I$ vale $xB \subseteq IB \subseteq J$. Sottraendo la combinazione $B$-lineare parziale sugli $x \in X_I$ otteniamo una combinazione $B$-lineare su $X \setminus X_I$ appartenente a $J \setminus \{0_T\}$. Sia $Y$ una parte *minimale* (rispetto a $\subseteq$) di $X \setminus X_I$ tale che $\left(\sum_{x \in Y} xB\right) \cap J \neq \{0_T\}$. Sia $z$ un elemento dell'insieme finito non vuoto $Y$. Per la minimalità di $Y$ si ha

$$\{0_T\} \neq \{b | b \in B,\ \forall y \in Y \setminus \{z\}\ \exists b_y \in B \quad zb + \sum_{y \in Y \setminus \{z\}} y b_y \in J\} \trianglelefteq B.$$

La semplicità di $B$ implica che tale ideale è tutto $B$, quindi

$$\forall b \in B\, \forall y \in Y \setminus \{z\}\, \exists b_y \in B \quad zb + \sum_{y \in Y \setminus \{z\}} y b_y \in J.$$

In particolare ($b := 1_B$) esistono elementi $\tilde{b}_y \in B$ tali che $z + \sum_{y\in Y\smallsetminus\{z\}} y\tilde{b}_y \in J$. Siccome $J \trianglelefteq T$ ne segue, per ogni $b \in B$,

$$\sum_{y\in Y\smallsetminus\{z\}} y(\tilde{b}_y b - b\tilde{b}_y) = \big(z + \sum_{y\in Y\smallsetminus\{z\}} yb_y\big)b - b\big(z + \sum_{y\in Y\smallsetminus\{z\}} yb_y\big) \in J,$$

perché $yb = by$ per ogni $y \in Y$. Concludiamo, per la minimalità di $Y$, che $\tilde{b}_y b - b\tilde{b}_y = 0_T$ per ogni $b \in B$, $y \in Y \smallsetminus \{z\}$, cioé, $\tilde{b}_y \in Z(B)$ per ogni $y \in Y \smallsetminus \{z\}$. Siccome $B$ è centrale ne segue, per ogni $y \in Y \smallsetminus \{z\}$, che $\tilde{b}_y = c_y 1_B$ per un $c_y \in K$. Allora

$$z + \sum_{y\in Y\smallsetminus\{z\}} y\tilde{b}_y = z + \sum_{y\in Y\smallsetminus\{z\}} c_y y \in A \cap J = I = \langle X_I\rangle_K,$$

implicando che $z \in \langle X \smallsetminus \{z\}\rangle_K$, assurdo.

I casi speciali si vedono facilmente: Facendo uso di 1.8(1) otteniamo

$$Z(T) = C_T(B) \cap C_T(A) = A\,Z(B) \cap B\,Z(A) = A \cap B = K\iota,$$

quindi la (1). (2) vale per 1.10, (3) per (1) e (2). □

1.11. Corollario. *Sia $n \in \mathbb{N}$, $A$ un'algebra associativa centrale semplice, $\dim_K A = n$. Allora vale $A^- \underset{K}{\otimes} A \cong K^{n\times n}$.*

Dimostrazione. Per (2) o (3), $A^- \underset{K}{\otimes} A$ è semplice, quindi $A^- \underset{K}{\otimes} A \cong K^{n\times n}$ per 1.7. □

Se $D$, $D'$ sono algebre di divisione su $K$ e almeno una di loro è centrale, allora $D \otimes D'$ è semplice per (2). Per (II),(III) esiste un'algebra di divisione $E$ tale che

$$D \underset{K}{\otimes} D' \cong E^{n\times n} \quad \text{per un } n \in \mathbb{N}, \tag{$*$}$$

ed $n$ è unico, $E$ è unica a meno di isomorfismi. Già nel caso dell'algebra dei quaternioni (v. p. 2) si vede che $D \underset{K}{\otimes} D'$ non è sempre un'algebra di divisione: in quell'esempio ($D := D' := H(K)$) ciò dipende dal campo di base $K$. Vale, però, il seguente risultato:

1.12. Proposizione. *Siano $D$, $D'$ algebre di dimensione finita su $K$, $D$ centrale. Se $\operatorname{mcd}(\dim_K D, \dim_K D') = 1$, allora $D \underset{K}{\otimes} D'$ è un'algebra di divisione.*

Dimostrazione. Dobbiamo dimostrare che in ($*$) vale $n = 1$. Sia $R$ un ideale destro minimale di $E^{n\times n}$. Allora $\dim_K R = n \dim_K E$, e $R$ è sia $D$-modulo che $D'$-modulo unitale completamente riducibile. A meno di isomorfismi, l'unico $D$-modulo irriducibile è $(D, \rho)$, quindi $R \underset{D}{\cong} D^k$ per un $k \in \mathbb{N}$. Ne segue che $\dim_K D | \dim_K R = n \dim_K E$. Nello stesso modo si ha $\dim_K D' | n \dim_K E$. Consegue per l'ipotesi sulle dimensioni che

$$\dim_K E^{n\times n} = \dim_K D \dim_K D' \,|\, n \dim_K E$$

implicando che $n = 1$. □

Ora scegliamo un sistema $\mathcal{B}(K)$ di rappresentanti per le classi di isomorfismo delle algebre di divisione centrali di dimensione finita su $K$, $K \in \mathcal{B}$.[13] Allora per ogni algebra di divisione $A$ centrale di dimensione finita su $K$ esiste un unico elemento $D \in \mathcal{B}(K)$ tale che $D \cong A$.

Se $D, D' \in \mathcal{B}(K)$, allora l'algebra $E$ in $(*)$ è centrale semplice, per il caso speciale (3) dopo 1.10. Per (III) esiste un'unico elemento $E \in \mathcal{B}(K)$ tale che vale $(*)$. Poniamo $D \odot D' := E$ e abbiamo definito così un'operazione $\odot$ su $\mathcal{B}(K)$.

Le proprietà del prodotto tensoriale menzionate dopo 1.6.2 implicano che $\odot$ è commutativa e associativa, e $K$ è elemento neutro. Per ogni $D \in \mathcal{B}(K)$ esiste $E \in \mathcal{B}(K)$ tale che $E \cong D^-$. Per 1.11 vale $D \odot E = K$. Allora, rispetto a $\odot$, $\mathcal{B}(K)$ è un gruppo abeliano con elemento neutro $K$.

1.13. Definizione. $(\mathcal{B}(K), \odot)$ *si dice il* gruppo di Brauer *di* $K$. *Applicando* 1.12 *a due elementi di* $\mathcal{B}(K)$ *otteniamo*

1.13.1. *Siano* $D, D' \in \mathcal{B}(K)$ *e* $\operatorname{mcd}(\dim_K D, \dim_K D') = 1$. *Allora*

$$\dim_K(D \odot D') = \dim_K D \, \dim_K D'.$$

□

*Essendo di dimensione finita, ogni algebra in* $\mathcal{B}(K)$ *è algebrica su* $K$, *quindi otteniamo direttamente da* 1.3(2)*:*

1.13.2. *Se* $K$ *è algebricamente chiuso allora* $\mathcal{B}(K) = \{K\}$. □

In particolare, $\mathcal{B}(\mathbb{C}) = \{\mathbb{C}\}$. Al gruppo $\mathcal{B}(\mathbb{R})$ invece appartengono almeno due elementi: $\{\mathbb{R}, \mathbb{H}\} \subseteq \mathcal{B}(\mathbb{R})$. Vedremo fra poco che vale l'uguglianza (v. 2.10). Studieremo nel prossimo capitolo le algebre di divisione su un campo arbitrario, con lo scopo di una descrizione di tutti gli elementi di $\mathcal{B}(K)$. Nel caso di un campo numerico $K$, tale descrizione viene sostanzialmente fornita dal teorema di Hasse-Brauer-Noether e Albert (p. 8) che riduce il problema alle algebre di divisione cicliche su $K$ e quindi a un tipo di algebra ben capito grazie agli studi di Wedderburn (v. la nota 9 a piè di pagina). Le principali idee ingenose per affrontare il caso generale tramite una generalizzazione della nozione di algebra ciclica sono dovute ad Emmy Noether che insieme a Richard Brauer creò i concetti decisivi della teoria negli anni intorno al 1930.

[13] Se $V$ è uno spazio vettoriale di dimensione contabile sul campo $K$, allora ogni algebra associativa unitaria di dimensione finita su $K$ è isomorfa ad una sottoalgebra di $\operatorname{End}_K V$: la rappresentazione $\rho$ (v. p. 1) è un monomorfismo dell'algebra $A$ in $\operatorname{End}_K A$ e quest'ultima è isomorfa ad una sottoalgebra di $\operatorname{End}_K V$ perché $\dim_K A \leq \dim_K V$. La relazione di isomorfismo è un'equivalenza sull'insieme delle sottoalgebre di $\operatorname{End}_K V$. Quindi è possibile scegliere gli elementi di $\mathcal{B}(K)$ di dimensione $> 1$ come rappresentanti delle classi di equivalenza rispettive in $\operatorname{End}_K V$.