Università del Salento
Dipartimento di Matematica e Fisica
"Ennio de Giorgi"

Hartmut Laue

Algebre associative semplici di dimensione finita

Quaderno 1/2014
Università del Salento - Coordinamento SIBA

Quaderni di Matematica

Una pubblicazione a cura del

Dipartimento di Matematica e Fisica "Ennio de Giorgi"
Università del Salento

I Quaderni del Dipartimento di Matematica e Fisica "Ennio De Giorgi" della Università del Salento documentano gli aspetti di rilievo dell'attività di ricerca e didattica del Dipartimento. Nei Quaderni sono pubblicati articoli di carattere matematico che siano:

(1) lavori di rassegna e monografie su argomenti di ricerca;
(2) testi di seminari di interesse generale, tenuti da docenti o ricercatori del Dipartimento o esterni;
(3) lavori di specifico interesse didattico.

La pubblicazione dei lavori è soggetta all'approvazione del Comitato di Redazione, che decide tenendo conto del parere di un *referee*, nominato di volta in volta sulla base delle competenze specifiche.

Quaderno 1/2014: e-ISBN 978–88–8305–106–7

Università del Salento - Coordinamento SIBA

ALGEBRE ASSOCIATIVE SEMPLICI DI DIMENSIONE FINITA

Hartmut Laue

Università di Kiel - Germania

Prefazione

Nel periodo 1 settembre – 4 ottobre 2012 ho tenuto, presso il Dipartimento di Matematica dell'Università del Salento, una serie di 21 lezioni rivolte agli studenti del Dottorato in Matematica. Il corso ha avuto lo scopo di approfondire le conoscenze dei dottorandi su un argomento cruciale dell'algebra che riveste un'importanza fondamentale anche in altri rami della matematica. La teoria delle algebre associative semplici di dimensione finita è stato il tema scelto. Il fulcro del corso è stato una presentazione moderna dei risultati dovuti a Emmy Noether e Richard Brauer le cui ideee innovative hanno preparato e indirizzato la ricerca in quest'ambito e sono tutt'ora attuali.

Ringrazio i colleghi del Dipartimento di Matematica dell'Università del Salento per il gentile invito e la calorosa ospitalità. È stato un piacere enorme e un grande desiderio esporre l'argomento in modo tale che il corso desse un approccio adeguato all'importanza dell'area, mettendo in evidenza la sua attualità, la sua profondità e bellezza.

Il Dipartimento di Matematica dell'Università del Salento offre possibilità eccellenti per realizzare corsi avanzati di questo tipo, non solo nel senso organizzativo ma anche per il livello di preparazione nell'ambito dell'Algebra, raggiunto grazie a un impegno infaticabile da parte dei docenti. Per ogni studente interessato a fare ricerca in Algebra l'Università del Salento è un'ottima scelta. La mia speranza è che il mio corso sia stato un utile contributo all'alto livello di lavoro scientifico che è presente a Lecce.

Kiel (Germania), marzo 2013, Hartmut Laue

Indice

Prefazione v

Introduzione 1

Capitolo 1. Algebre di divisione e prodotti tensoriali 5

Capitolo 2. Automorfismi nella teoria delle algebre associative 15

Capitolo 3. Il gruppo di Brauer 23

Appendice A. 33

Bibliografia 37

Indice analitico 39

Introduzione

Il nucleo principale della teoria di base delle algebre associative semplici consiste nei tre seguenti risultati[1] dovuti a Wedderburn (1907):

(I) *Sia D un corpo, $n \in \mathbb{N}$. Allora $D^{n\times n}$ è un'algebra associativa semplice su $Z(D)$.*

(II) *Sia A un'algebra associativa unitaria semplice di dimensione finita su $Z(A)$. Allora esiste un corpo D e $n \in \mathbb{N}$ tale che $A \cong D^{n\times n}$.*

(III) *Siano $m, n \in \mathbb{N}$, D, E corpi tali che $D^{n\times n} \cong E^{m\times m}$. Allora vale $m = n$, $E \cong D$.*

Di conseguenza, le algebre associative semplici di dimensione finita su un campo K sono tutte e sole le algebre matriciali sulle algebre di divisione di dimensione finita su K, a meno di isomorfismi. Poi, a meno di isomorfismi, le algebre di divisione in una tale descrizione sono uniche. Questi risultati servono come punto di partenza per tutto quanto segue. Il risultato chiave della teoria scoperta da Wedderburn è la proposizione (II). Ricordiamo il punto saliente della dimostrazione:

Sia A un'algebra semplice di dimensione finita su un campo K. Giocherà un ruolo importante l'algebra opposta di A che denoteremo con A^-.[2] Per ogni ideale destro minimale R di A esiste un $n \in \mathbb{N}$ tale che $A \cong R^n$, come A-moduli, dove l'azione di A è data tramite la moltiplicazione a destra, cioè, mediante l'omomorfismo di algebre

$$\rho : A \to \mathrm{End}(A, +),\ x \mapsto \begin{bmatrix} A & \to & A \\ y & \mapsto & yx \end{bmatrix}.$$

Essendo R un A-modulo irriducibile, si ha allora che l'A-modulo A è omogeneo, $\mathrm{End}_A R$ è algebra di divisione su K (per il Lemma di Schur), $\mathrm{End}_A R^n \cong (\mathrm{End}_A R)^{n\times n}$. La moltiplicazione a sinistra,

$$\lambda : A \to \mathrm{End}(A, +),\ x \mapsto \begin{bmatrix} A & \to & A \\ y & \mapsto & xy \end{bmatrix}$$

invece è un antiomomorfismo di A, quindi un omomorfismo di A^-,[3] e si ha

$$A \cong (\mathrm{End}_A R^n)^- \cong D^{n\times n}$$

dove $D := (\mathrm{End}_A R)^-$.

Un dettaglio molto importante è il fatto che a meno di isomorfismi, R è l'unico A-modulo irriducibile. Poi, ogni A-modulo di dimensione finita è completamente

[1] Per ogni algebra A e $n \in \mathbb{N}$ denotiamo con $A^{n\times n}$ l'algebra delle matrici $n \times n$ su A, con $Z(A)$ il centro di A. Se A è associativa unitaria (cioè ha un elemento neutro rispetto alla moltiplicazione) e semplice, allora $Z(A)$ è un campo.

[2] Una scrittura diffusa per l'algebra opposta di A è A^{opp}, anche A^{op}. Tale algebra nasce da A considerando il nuovo prodotto $x \circ y := yx$ per ogni $x, y \in A$.

[3] Vale $(xx')\rho = (x\rho)(x'\rho)$, $(xx')\lambda = (x'\lambda)(x\lambda)$ per ogni $x, x' \in A$.

riducibile. In altre parole, le rappresentazioni di dimensione finita di A permettono una descrizione molto semplice:
Per ogni A-modulo V di dimensione finita su K esiste un $k \in \mathbb{N}_0$ tale che $V \underset{A}{\cong} R^k$.
Notiamo come conseguenza:

COROLLARIO. *Se V, W sono A-moduli tali che $\dim_K V = \dim_K W$, allora*

$$V \underset{A}{\cong} W.$$

Un esempio di ideale destro minimale di $D^{n\times n}$ è, per ogni $j \in \underline{n}_{,}$[4] l'insieme R_j delle matrici $n \times n$ su D in cui al più la j-esima riga contiene elementi non nulli:

$$R_j := \left\{ \begin{pmatrix} & O & \\ d_{j,1} & \dots & d_{j,n} \\ & O & \end{pmatrix} \Big| \, d_{jk} \in D \right\}.$$

Grazie ai risultati di Wedderburn, lo studio delle algebre associative semplici di dimensione finita su un campo K si concentra su due problemi seguenti:

Problema 1 Come si possono descrivere le algebre di divisione di dimensione finita?

Problema 2 Data un'algebra di divisione D di di dimensione finita e $n \in \mathbb{N}$, come si analizza l'interno dell'algebra $D^{n\times n}$? [5]

Per quanto riguarda il Problema 2, vedremo che il passaggio da A ad $A^{n\times n}$ comporta fenomeni strutturali nuovi che meritano uno studio approfondito. Per quanto riguarda il Problema 1, va detto che le algebre di divisione – se non sono campi – nascono sempre con costruzioni non banali e raramente studiate nei corsi introduttivi. Però, i risultati (I), (II), (III) mostrano che esse sono di importanza centrale per la teoria delle algebre associative: *La teoria stabilita da Wedderburn può essere interpretata come riduzione dello studio delle algebre semplici di dimensione finita allo studio delle algebre di divisione di dimensione finita.* Un esempio famoso di algebra di divisione non commutativa – frequentemente l'unica presentata nei corsi di base – è quella dei quaternioni. Ricordiamo la sua definizione: Per ogni campo K di caratteristica $\neq 2$ si dice algebra dei quaternioni su K un'algebra associativa unitaria A di dimensione 4 su K generata da due elementi i, j tali che $i^2 = -1_A = j^2$, $ij = -ji$. [6] Si ha:

---

[4] $\underline{n}_{,} := \{j | j \in \mathbb{N},\, j \leq n\}$ per ogni $n \in \mathbb{N}_0$.

[5] Dipende dalle proprietà che si studiano se il passaggio da un'algebra A all'algebra matriciale $A^{n\times n}$ è banale o meno. Per esempio è banale l'implicazione

$$A \text{ nilpotente} \Rightarrow A^{2\times 2} \text{ nilpotente}$$

mentre l'implicazione

$$A \text{ nil} \Rightarrow A^{2\times 2} \text{ nil}$$

è una forma della congettura di Köthe, rimasta aperta da 80 anni. A si dice nil se ogni elemento di A è nilpotente, il che è naturalmente una condizione molto più debole della nilpotenza di A. Se A è una $\mathbb{Q}$-algebra ed esiste un $n \in \mathbb{N}$ tale che $x^n = 0_A$ per ogni $x \in A$, allora ogni prodotto di $2^n - 1$ fattori in A dà 0_A (Nagata-Higman 1952, in questa forma dovuto a Woo Lee [**WL**] che anche diede una dimostrazione semplificata.) Per ulteriori dettagli rispetto alla congettura di Köthe e i suoi legami con altre congetture nella teoria degli anelli, v. per esempio [**Sm**].

[6] L'ultima condizione può essere sostituita con $(i + j)^2 = -2_A$. – È anche possibile studiare il caso in cui $\operatorname{char} K = 2$ ma ciò comporta fenomeni speciali che non hanno importanza nel nostro contesto.

PROPOSIZIONE. *Per ogni campo K tale che* $\operatorname{char} K \neq 2$ *esiste a meno di isomorfismi un'unica algebra dei quaternioni $H(K)$ su K. Tale algebra è semplice e l'applicazione $K \to H(K)$, $c \mapsto c1_{H(K)}$, è un isomorfismo da K su $Z(H(K))$.*

Per (II), o $H(K) \cong K^{2\times 2}$ o $H(K)$ è un'algebra di divisione su K. Nel caso di un sottocampo K di $\mathbb{R}$, $H(K)$ è sempre un'algebra di divisione, mentre $H(\mathbb{C}) \cong \mathbb{C}^{2\times 2}$. Gli elementi i, j generano un sottogruppo moltiplicativo non abeliano di ordine 8, il cosiddetto gruppo dei quaternioni, in teoria dei gruppi normalmente denotato con Q_8. L'algebra di divisione $\mathbb{H} := H(\mathbb{R})$ è storicamente il primo esempio (1843) di algebra non commutativa e prende il suo nome, l'algebra di Hamilton, dal suo scopritore irlandese.

Per ogni K-algebra unitaria A poniamo

$$\iota : K \to A, \quad c \mapsto c1_A.$$

Allora ι è un monomorfismo e $K\iota \subseteq Z(A)$. L'algebra A si dice centrale su K se $K\iota = Z(A)$. Siccome ogni K-algebra è anche un'algebra su $Z(A)$ e, nel caso semplice, $Z(K)$ è un campo, *basta studiare le K-algebre centrali.* È facile vedere che per ogni corpo D e $n \in \mathbb{N}$

$$Z(D^{n\times n}) = \Big\{ \begin{pmatrix} c & & O \\ & \ddots & \\ O & & c \end{pmatrix} \Big| \, c \in Z(D) \Big\} \cong Z(D).$$

La nozione di algebra nel senso più generale richiede solo la struttura di gruppo abeliano $(A, +)$ nel quale è definita una seconda operazione (la moltiplicazione) tale che valgano le due leggi distributive. Un'algebra si dice unitaria se esiste un elemento neutro $1_A \neq 0_A$ rispetto alla moltiplicazione (dove 0_A è l'elemento neutro rispetto all'«addizione»+ data in A). Se $(A, +)$ è un K-modulo rispetto ad un anello commutativo unitario K e vale $c(xy) = (cx)y = x(cy)$ e $1_K x = x$ per ogni $x, y \in A$, $c \in K$, allora A si dice una K-algebra, e gli elementi di K si dicono scalari. Per ogni algebra A, $K := \mathbb{Z}$ è sempre una possibile scelta come anello di scalari.

E' restrittivo richiedere che A sia un'algebra su un *campo* K, cioè $(A, +)$ uno spazio vettoriale su K, – e questo è il caso al quale ci limiteremo in questa serie di lezioni.

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 σ. 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 σ 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 σ.

[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

$$\begin{aligned} t^n - z &= (a_{n-1}t^{n-1} + \cdots + a_1 t + a_0)(t - b) \\ &= (a_{n-1}t^n + \cdots + a_0 t) - (a_{n-1}t^{n-1}b + \cdots + a_1 tb + a_0 b) \\ &= a_{n-1}t^n + \sum_{j\in\underline{n-1}_1} \big(a_{j-1} - a_j(b\sigma^j)\big)t^j - a_0 b. \end{aligned}$$

[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 $a_{n-1} = 1_L$, $\forall j \in \underline{n-1}_1 \quad a_{j-1} = a_j(b\sigma^j)$, $a_0 b = z$, 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

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

$ya = b^{-1}xa = b^{-1}(a\sigma)x = (a\sigma)y$ 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 σ 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 σ 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 ρ_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 *δ-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 δ-endomorfismi. È utile notare che, per queste nozioni, basta che δ sia una *funzione lineare* (anziché, più strettamente, un omomorfismo di algebre), anche se nella maggioranza delle applicazioni in questa teoria δ sarà anche un omomorfismo moltiplicativo. Se δ è un omomorfismo di A *come algebra*, δ è detto unitale se $1_A\delta = \mathrm{id}_V$. Più in generale, se A, B sono algebre unitarie, un omomorfismo δ 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: λ e ρ; ricordiamo che di questi solo ρ 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 $\alpha \in \mathrm{End}(\mathrm{A}, \rho)$, $y \in A$, 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, φ, ψ) 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 $\varphi : (c_{ij}) \mapsto (c_{ij}1_A)$, $\psi : y \mapsto diag(y, \ldots, y)$.
(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 ∂ 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, φ, ψ) 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 σ 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 φ la funzione K-lineare da A in T tale che $x\varphi = (x, 1_B)$ per ogni $x \in X$. È facile vedere che φ 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, φ, ψ) 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 σ 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, ∂ 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, φ, ψ) 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, φ, ψ), $(\tilde{T}, \tilde{\varphi}, \tilde{\psi})$ sono prodotti tensoriali di A con B, allora l'omomorfismo σ 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 σ è un isomorfismo. □

Date A, B, fissiamo *una* terna (T, φ, ψ) 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 φ, ψ 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 σ 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 $Q = A' \underset{K}{\dot{\otimes}} B'$, 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) δ, 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,*

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

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 τ 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) τ 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, ρ), 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

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

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 ρ (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 $\operatorname{End}_K V$.

CAPITOLO 2

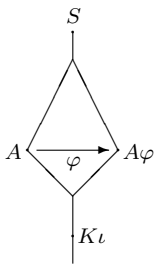
Automorfismi nella teoria delle algebre associative

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

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



Sia ψ un isomorfismo di K-algebre da $\operatorname{End}_{D^-} D^n$ 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]: $\operatorname{Aut}_K A = \operatorname{Inn}_K A$ *per ogni algebra associativa centrale semplice A di dimensione finita* (dove il gruppo degli automorfismi interni di A è denotato con $\operatorname{Inn}_K A$)[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 $\operatorname{Inn}_K A \cong U(A)/\dot{K}\iota$

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

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

(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 $E_1, \dots, E_k \in \mathcal{P}$ 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).

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.

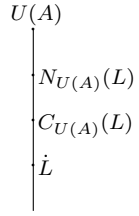
2.11. Lemma. *Sia* A *un'algebra associativa unitaria su* K *e* L *un sottocampo unitale di* A. *Assumiamo che* $K \leq L$ [22]. *Siano* $r \in \mathbb{N}$ *e* $y_1, \ldots, y_r$ *elementi a due a due distinti di un trasversale di* $C_{U(A)}(L)$ *in* $N_{U(A)}(L)$. *Sia* $J \leq (A, +)$ *tale che* JL,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



(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 $i, j \in \underline{n}_{\,|}$, $x \in A$, sia $b_{i,j}(x) \in L$ tale che vale $v_i x = \sum_{j \in \underline{n}_{\,|}} v_j b_{i,j}(x)$. Ne segue per ogni $\alpha, \beta \in G$, $i \in \underline{n}_{\,|}$

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

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

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

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 $y_{\sigma^i} a \mapsto ax^i$ 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.

CAPITOLO 3

Il gruppo di Brauer

3.1. Definizione. *Sia M un gruppo abeliano e sia data un'azione di G su M.*[26] *Poniamo*

$$Z^2(G,M) := \{f | f \in M^{G\times G},\ \forall \alpha,\beta,\gamma \in G \quad f(\alpha\beta,\gamma)\, f(\alpha,\beta)\gamma) = f(\alpha,\beta\gamma)\, f(\beta,\gamma)\},$$
$$N^2(G,M) := \{f | f \in Z^2(G,M),\ \forall \alpha \in G \quad f(\alpha,1_G) = 1_M = f(1_G,\alpha)\}.$$

*Gli elementi di $Z^2(G,M)$ si dicono i 2-*cocicli *di G rispetto a M. Specializzando la condizione nella definizione in maniera adatta si ottiene facilmente*

3.1.1.

$$\forall f \in Z^2(G,M)\, \forall \alpha \in G \quad f(\alpha,1_G) = f(1_G,1_G) = f(1_G,\alpha)\alpha^{-1},$$
$$\forall f \in N^2(G,M)\, \forall \alpha \in G \quad f(\alpha^{-1},\alpha) = f(\alpha,\alpha^{-1})\alpha. \qquad \square$$

3.1.2. *Per ogni $\nu \in M^G$, l'applicazione*

$$f : G\times G \to M,\ (\alpha,\beta) \mapsto \nu(\beta)\big(\nu(\alpha\beta)\big)^{-1}\big(\nu(\alpha)\big)\beta$$

è un 2-cociclo di G rispetto a M,

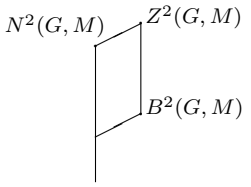
perché $f(\alpha\beta,\gamma)\, f(\alpha,\beta)\gamma = \nu(\gamma)\big(\nu(\alpha\beta\gamma)\big)^{-1}\big(\nu(\alpha\beta)\big)\gamma\,\big((\nu(\alpha\beta))\gamma\big)^{-1}\nu(\beta)\gamma\,\nu(\alpha)\beta\gamma = = \nu(\gamma)\big(\nu(\beta\gamma)\big)^{-1}\big(\nu(\beta)\big)\gamma\,\nu(\beta\gamma)\,\nu(\alpha\beta\gamma)^{-1}\,\nu(\alpha)\beta\gamma = f(\beta,\gamma)f(\alpha,\beta\gamma)$ *per* $\alpha,\beta,\gamma \in G$. $\square$

Poniamo

$$B^2(G,M) := \{f | f \in M^{G\times G},\ \exists \nu \in M^G\ \forall \alpha,\beta \in G \quad f(\alpha,\beta) = \nu(\beta)\big(\nu(\alpha\beta)\big)^{-1}\big(\nu(\alpha)\big)\beta\}$$

*e chiamiamo 2-*cobordi *di G rispetto a M gli elementi di $B^2(G,M)$. Il 2-cobordo f in* 3.1.2 *viene chiamato il 2-cobordo* associato a ν.

3.1.3. *$Z^2(G,M)$, $N^2(G,M)$, $B^2(G,M)$ sono sottogruppi*[27] *di $M^{G\times G}$, e vale $B^2(G,M)N^2(G,M) = Z^2(G,M)$.*



Dimostrazione. Sia $f \in Z^2(G,M)$ e ν un'applicazione qualsiasi da G in M tale che $\nu(1_G) = \big(f(1_G,1_G)\big)^{-1}$. Sia g_ν il 2-cobordo associato a ν. Otteniamo da 3.1.1 che $(fg_\nu)(\alpha,1_G) = 1_M = (fg_\nu)(1_G,\alpha)$ per ogni $\alpha \in G$, cioè: $fg_\nu \in N^2(G,M)$, $f \in N^2(G,M)B^2(G,M)$. $\square$

Il quoziente $H^2(G,M) := Z^2(G,M)/B^2(G,M)$ si dice il 2^o gruppo di coomologia *di G rispetto a M.*

[26] Per ogni $v \in M$, $\gamma \in G$, scriviamo $v\gamma$ per l'immagine di v sotto l'azione di γ.

[27] Ricordiamo che, per ogni isieme X, M^X è un gruppo abeliano rispetto all'usuale addizione di funzioni.

3.1.4. *Se valgono le ipotesi di* 2.13(2)*, allora* $f^n \in B^2(G, \dot{L})$.

Come dimostrazione basta porre $\nu(\alpha) := \det y_\alpha \delta$ per ogni $\alpha \in G$ e applicare 2.13(2). □

Ora sia (K, L) un'estensione di campi, $G \leq \mathrm{Aut}_K L$. Allora G agisce su $\dot{L}$. Chiamiamo sistemi noetheriani di fattori per (K, L) e G gli elementi $f \in N^2(G, \dot{L})$, nel caso che $G = \mathrm{Aut}_K L$ più brevemente *sistemi noetheriani di fattori per* (K, L).

3.2. 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* $f \in N^2(G, \dot{L})$*. Allora si ha*

(1) V_f *è una* K*-algebra associativa unitaria,* $L \cong y_{\mathrm{id}_L} L = C_{V_f}(y_{\mathrm{id}_L} L)$*,*

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

(2) *Se* (K, L) *è galoissiana e* $G = \mathrm{Aut}_K L$*, allora* V_f *è centrale semplice.*

Dimostrazione. (1) Per 2.15.1 sappiamo che V_f è una K-algebra associativa unitaria e ι_L è un monomorfismo del campo L in V_f. È banale la prima delle due equazioni affermate per ogni $\alpha \in G$, mentre la seconda consegue dalla 2^a parte di 3.1.1: $y_{\alpha^{-1}} f(\alpha, \alpha^{-1})^{-1} \bullet y_\alpha = y_{\mathrm{id}_L} f(\alpha^{-1}, \alpha)\, f(\alpha, \alpha^{-1})^{-1} \alpha = y_{\mathrm{id}_L}$. Allora ogni y_α è invertibile in V_f, e per ogni $\alpha \in G$, $b \in L$ vale

$$\begin{aligned} y_\alpha^{-1} \bullet y_{\mathrm{id}_L} b \bullet y_\alpha &= y_{\alpha^{-1}} f(\alpha, \alpha^{-1})^{-1} \bullet y_{\mathrm{id}_L} b \bullet y_\alpha = y_{\alpha^{-1}} f(\alpha, \alpha^{-1})^{-1} b \bullet y_\alpha \\ &= y_{\mathrm{id}_L} f(\alpha^{-1}, \alpha)(f(\alpha, \alpha^{-1})^{-1} b)\alpha = y_{\mathrm{id}_L} b\alpha. \end{aligned}$$

Allora possiamo applicare 2.12 e otteniamo sia l'affermazione sul centralizzante di $y_{\mathrm{id}_L} L$ in (1) che (2). □

Applichiamo 3.2(2) al sistema noetheriano f_z di fattori (con $z \in \dot{K}$) per un'estensione galoissiana (K, L) con un gruppo di Galois ciclico $\langle \sigma \rangle$. Conseguentemente V_{f_z}, dunque per 2.16 anche $L_{\sigma,z}$ è centrale semplice. Abbiamo così dimostrato la prima affermazione in 1.2(1). Per 3.2(1) vale anche la seconda parte, e la dimostrazione di 1.2 è completa.

Uno spazio V come in 3.2 è spazio di sostegno per tutti i prodotti incrociati V_f, $f \in \dot{L}^{G \times G}$. Come in 3.2 prendiamo in considerazione nel seguito solo sistemi *noetheriani* f di fattori. Allora y_{id_L} è sempre neutro in V_f per cui scriveremo solo 1_V per tale elemento. Inoltre fissiamo anche la biiezione $\alpha \mapsto y_\alpha$ da G su una L-base di V. Notiamo che vale sempre

$$\begin{aligned} L \cong 1_V L = C_V(1_V L) \qquad & \text{per 3.2(1)}, \\ \dim_K V = \dim_K L \dim_L V &= \dim_K L \cdot |G|, \end{aligned}$$

nel caso di un'estensione galoissiana (K, L) quindi $\dim_K V = (\dim_K L)^2$.

3.3. Teorema. *Sia* (K, L) *un'estensione galoissiana,* A *un'algebra associativa unitaria su* K*. Sono equivalenti*

(i) A *è centrale semplice con un sottocampo unitale isomorfo a* L*,* $\dim_K A = (\dim_K L)^2$*,*

(ii) *Esiste un sistema noetheriano* f *di fattori per* (K, L) *tale che* $A \cong V_f$*.*

DIMOSTRAZIONE. (i)⇒(ii): Sia $G := \mathrm{Aut}_K L$. Senza perdita di generalità assumiamo che L sia sottocampo unitale di A. Le nostre ipotesi implicano che $\dim_L A = \dim_K L = |G| = |N_{U(A)}(L)/C_{(U(A)}(L)|$, quest'ultimo per 2.1. Ne segue (ii) per 2.15.2.

(ii)⇒(i): Se vale (ii), allora $\dim_K A = \dim_K L \cdot \dim_L V_f = (\dim_K L)^2$ perché (K, L) è galoissiana. Le altre parti della tesi seguono da 3.2. □

Essendo centrale semplice nel caso di un'estensione galoissiana (K, L), un prodotto incrociato V_f (con un sistema noetheriano f di fattori) è isomorfo ad un'algebra matriciale su un corpo $D \in \mathcal{B}(K)$. Adesso caratterizzeremo i sistemi noetheriani f tali che vale $D \cong K$.

3.4. PROPOSIZIONE. *Sia (K, L) un'estensione galoissiana, $G = \mathrm{Aut}_K L$, $n := |G|$, $f \in N^2(G, \dot{L})$, V_f il prodotto incrociato relativo. Sono equivalenti*

(i) $V_f \cong K^{n\times n}$,
(ii) V_f *ha un ideale destro* R *tale che* $\dim_L R = 1$,
(iii) $f \in B^2(G, \dot{L})$.

DIMOSTRAZIONE. (i)⇔(ii): Se vale (i), un ideale destro minimale della K-algebra V_f è di dimensione n su K, quindi di dimensione 1 su L. Vice versa sia R un ideale destro di V_f tale che $\dim_L R = 1$. Allora R è un ideale destro minimale della K-algebra V_f e di dimensione n su K. Tramite la rappresentazione relativa (indotta dalla moltiplicazione a destra) otteniamo un omomorfismo iniettivo (per 3.3) da V_f in $K^{n\times n}$ che deve essere un isomorfismo perché $\dim_K V_f = n^2 = \dim_K K^{n\times n}$.

Se $\beta \in G$ e $v = \sum_{\alpha\in G} y_\alpha b_\alpha \in V_f$ (dove $b_\alpha \in L$ per ogni $\alpha \in G$) vale

$$v \bullet y_\beta = \sum_{\alpha\in G} y_{\alpha\beta} f(\alpha, \beta)\, b_\alpha \beta = \sum_{\gamma\in G} y_\gamma f(\gamma\beta^{-1}, \beta) b_{\gamma\beta^{-1}}\beta. \qquad (*)$$

(ii)⇒(iii): Se $v \in V_f$ tale che $R = \langle v\rangle_L$ allora $v \bullet y_\beta = vc_\beta = \sum_{\alpha\in G} y_\alpha b_\alpha c_\beta$ per un $c_\beta \in \dot{L}$. Segue che

$$\forall \alpha, \beta \in G \quad b_\alpha c_\beta = f(\alpha\beta^{-1}, \beta) b_{\alpha\beta^{-1}}\beta. \qquad (**)$$

Se fosse $b_\alpha = 0_L$ per un $\alpha \in G$, allora $(*)$ implicherebbe $b_\alpha = 0_L$ per *ogni* $\alpha \in G$, assurdo perché $v \neq 0_{V_f}$. Allora vale $b_\alpha \neq 0_L$ per ogni $\alpha \in G$, e possiamo assumere che $b_{\mathrm{id}_L} = 1_L$. Ora mostriamo che f è il 2-cobordo associato all'applicazione $\nu : G \to \dot{L}$, $\alpha \mapsto b_\alpha^{-1}$: Per ogni $\beta \in G$ otteniamo come caso speciale di $(**)$ che $b_\beta c_\beta = f(\mathrm{id}_L, \beta)\, 1_L\beta = 1_L$, cioè, $c_\beta = b_\beta^{-1}$. Con questa, sempre grazie a $(**)$, vediamo che $b_\alpha b_\beta^{-1}(b_{\alpha\beta^{-1}}^{-1}\beta) = f(\alpha\beta^{-1}, \beta)$, quindi $\nu(\beta)\big(\nu(\alpha\beta)\big)^{-1}\big(\nu(\alpha)\big)\beta = f(\alpha, \beta)$ per ogni $\alpha, \beta \in G$.

(iii)⇒(ii): Sia $f \in B^2(G, \dot{L})$, $\nu \in \dot{L}^G$ tale che $f(\alpha, \beta) = \nu(\beta)\,\nu(\alpha\beta)^{-1}\,\big(\nu(\alpha)\big)\beta$ per ogni $\alpha, \beta \in G$. Siccome $f(\mathrm{id}_L, \beta) = 1_L$ vale $\nu(\mathrm{id}_L)\beta = 1_L$, quindi $\nu(\mathrm{id}_L) = 1_L$. Sia $b_\alpha := \nu(\alpha)^{-1}$ per ogni $\alpha \in G$ e $v := \sum_{\alpha\in G} y_\alpha b_\alpha$. Allora $v \neq 0_{V_f}$, e per ogni $\beta \in G$ otteniamo tramite $(*)$

$$\begin{aligned} v \bullet y_\beta = \sum_{\alpha\in G} y_\alpha\, f(\alpha\beta^{-1}, \beta)\, b_{\alpha\beta^{-1}}\beta &= \sum_{\alpha\in G} y_\alpha \nu(\beta)\nu(\alpha)^{-1}\big(\nu(\alpha\beta^{-1})\big)\beta\,\nu(\alpha\beta^{-1})^{-1}\beta \\ &= (\sum_{\alpha\in G} y_\alpha b_\alpha) b_\beta^{-1} \in \langle v\rangle_L. \end{aligned}$$

Allora $\langle v\rangle_L$ è ideale destro di V_f. □

3.5. Definizione. *Sia A un'algebra centrale semplice di dimensione finita su K. Un ampliamento L di K si dice un* campo di spezzamento *di A se esiste un $n \in \mathbb{N}$ tale che $A_L \cong L^{n\times n}$ (v. p. 11). Per esempio, $\mathbb{H}_{\mathbb{C}} \cong \mathbb{C}^{2\times 2}$. Generalmente vale*

3.5.1. *Ogni ampliamento L di K tale che $\mathcal{B}(L) = \{L\}$ è campo di spezzamento di A.*

Dimostrazione. A_L è L-algebra centrale semplice per 1.9 e il caso speciale (2) dopo 1.10. □

3.5.2. *Se $D \in \mathcal{B}(K)$, $m \in \mathbb{N}$ e $A \cong D^{m\times m}$, allora A, D hanno gli stessi campi di spezzamento.*

Dimostrazione. Sia L campo di ampliamento di K. Vale $A_L \cong (D^{m\times m})_L \cong (D_L)^{m\times m}$, quindi la tesi. □

3.5.3. *A^- e A hanno gli stessi campi di spezzamento,*

perché $(L^{n\times n})^- \cong L^{n\times n}$ per ogni campo L, $n \in \mathbb{N}$. □

Per 2.4 *vale*

3.5.4. *Se $D \in \mathcal{B}(K)$ e L è sottocampo massimale di D, allora L è un campo di spezzamento di D.*

In particolare, ogni algebra centrale semplice di dimensione finita ha un campo di spezzamento di dimensione finita su K. Per ogni estensione (K, L) poniamo

$$\mathcal{B}_L(K) := \{D | D \in \mathcal{B}(K),\ L \text{ è campo di spezzamento di } D\}.$$

Allora vale:

3.5.5. $\mathcal{B}(K) = \bigcup_{\dim_K L<\infty} \mathcal{B}_L(K)$. □

3.5.6. *Ogni ampliamento di un campo di spezzamento di A è un campo di spezzamento di A.*

Dimostrazione. Sia L un campo di spezzamento di A, M un ampliamento di L. Allora $A \underset{K}{\otimes} M \cong (A \underset{K}{\otimes} L) \underset{L}{\otimes} M \cong L^{n\times n} \underset{L}{\otimes} M \cong M^{n\times n}$ per un $n \in \mathbb{N}$. □

Sia L un ampliamento di K. Per ogni $D \in \mathcal{B}(K)$ la L-algebra D_L è centrale semplice per 1.9 *e il caso speciale* (2) *dopo* 1.10. *Scriviamo $D(L)$ per l'algebra in $\mathcal{B}(L)$ tale che $D_L \cong D(L)^{n\times n}$ per un $n \in \mathbb{N}$. Se $D, E \in \mathcal{B}(K)$, allora le L-algebre $(D \underset{K}{\otimes} E) \underset{K}{\otimes} L$ e $(D \underset{K}{\otimes} L) \underset{L}{\otimes} (E \underset{K}{\otimes} L)$ sono isomorfe come L-algebre. Ne segue:*

3.5.7. *Se L è un ampliamento di K, allora $\varphi : \mathcal{B}(K) \to \mathcal{B}(L)$, $D \mapsto D(L)$, è un omomorfismo, e $\ker\varphi = \mathcal{B}_L(K)$.* □

Per ogni $D \in \mathcal{B}(K)$ vale la seguente caratterizzazione dei campi di ampliamento di dimensione finita su K che sono campi di spezzamento di D:

3.6. Proposizione. *Sia $D \in \mathcal{B}(K)$, $n := \operatorname{ind} D$, L un campo di ampliamento di dimensione finita su K. Sono equivalenti*

(i) *L è un campo di spezzamento di D,*

(ii) *$n | \dim_K L$ ed esiste un monomorfismo unitale da L in $D^{m\times m}$, dove $m = \frac{\dim_K L}{n}$,*

(iii) *Esiste un monomorfismo φ da L in un'algebra matriciale A su D tale che vale $C_A(L\varphi) = L\varphi$.*

Prima della dimostrazione notiamo una conseguenza importante riguardante la portata del concetto di prodotto incrociato:

3.7. Corollario. *Se (K, L) è un'estensione galoissiana, allora per ogni $D \in \mathcal{B}_L(K)$ esiste un $f \in N^2(G, \dot{L})$ tale che $V_f \cong D^{m\times m}$ per un $m \in \mathbb{N}$ (isomorfismo di L-algebre).*

Dimostrazione. Sia $D \in \mathcal{B}_L(K)$. Allora vale 3.6(i), quindi anche 3.6(iii). Sia A come in 3.6(iii). Per 2.2(2) si ha $\dim_K A = (\dim_K L)^2$, quindi vale 3.3(i). Essendo l'estensione (K, L) galoissiana, ne segue 3.3(ii), quindi la tesi. □

Dimostrazione di 3.6. (i)⇒(ii): Se vale (i), allora L è campo di spezzamento anche per D^- (v. 3.5.3). Allora esiste un $k \in \mathbb{N}$ tale che $D^- \underset{K}{\otimes} L \cong L^{k\times k}$. Ne segue che $\dim_K D \cdot \dim_K L = k^2 \dim_K L$, quindi $k = n$. Essendo semplice, $D^- \underset{K}{\otimes} L$ ha (a meno di isomorfismi) un unico modulo irriducibile unitale (V, δ), dato tramite un ideale destro minimale di $L^{n\times n}$. D'altra parte vale $V \cong (D^m, +)$ come D^--modulo, per un $m \in \mathbb{N}$, perché $(D, +)$ è l'unico D^--modulo irriducibile a meno di isomorfismi. Pertanto si ha $mn^2 = \dim_K V = n \dim_K L$, quindi $mn = \dim_K L$. Vale $\mathrm{End}_{D^-} V \cong \big(\mathrm{End}_{D^-}(D, +)\big)^{m\times m} \cong D^{m\times m}$ per 1.4(1). Per 1.7.1 otteniamo quindi un monomorfismo unitale da L in $D^{m\times m}$.

(ii)⇒(iii): Sia $m \in \mathbb{N}$ secondo (ii), $A := D^{m\times m}$ e assumiamo che L sia sottocampo unitale di A. Vale $C_A(L) \geq L$ e, per 2.2(2),

$$m^2n^2 = \dim_K A = \dim_K L \dim_K C_A(L) = mn \dim_K C_A(L),$$

quindi $\dim_K C_A(L) = mn = \dim_K L$ e consegue $C_A(L) = L$.

(iii)⇒(i): Possiamo assumere di nuovo che L sia sottocampo unitale di A, e per ipotesi $L = C_A(L) \cong C_A(L)\rho = \mathrm{End}_{A^-\underset{K}{\otimes}L}(A, +)$, grazie a 2.1.1. In particolare, id_A è l'unico elemento idempotente non nullo di quest'ultimo anello. Ne segue che lo $A^- \underset{K}{\otimes} L$-modulo $(A, +)$ è direttamente scomponibile perché ogni proiezione su un suo addendo diretto (come $A^- \underset{K}{\otimes} L$-modulo) è idempotente e appartiene a $\mathrm{End}_{A^-\underset{K}{\otimes}L}(A, +)$, quindi $\{0_A\}$, A sono gli unici tali addendi diretti. D'altra parte, essendo $A^- \underset{K}{\otimes} L$ essendo semplice, il modulo $(A, +)$ è completamente riducibile. Ne segue che $(A, +)$ è irriducibile. Pertanto (v. p. 1) si hanno i seguenti isomorfismi di L-algebre:

$$A^- \underset{K}{\otimes} L \cong \big(\mathrm{End}_{A^-\underset{K}{\otimes}L}(A, +)^-\big)^{k\times k} \cong L^{k\times k} \text{ per un } k \in \mathbb{N}.$$

Per 3.5.3 ne segue (i). □

Ci stiamo avvicinando allo scopo di questo capitolo per quanto riguarda l'esame del ruolo dei prodotti incrociati. Manca un'ultima preparazione per poter dare il teorema principale:

3.8. Lemma. *Siano L un ampliamento di K, G un sottogruppo finito di $\mathrm{Aut}_K L$, $n := |G|$, $f, g \in N^2(G, \dot{L})$, V_f, V_g i relativi prodotti incrociati. Sia $T := V_f \underset{K}{\otimes} V_g$ e R l'ideale destro di T generato dagli elementi*

$$\Delta(c) := 1_V c \otimes 1_V - 1_V \otimes 1_V c \qquad (c \in L).$$

Sia Λ l'omomorfismo additivo da $(V,+)$ in $(\mathrm{End}_K(T,+),+)$ tale che

$$(y_\alpha a)\Lambda = (y_\alpha a \otimes y_\alpha)\lambda \quad \text{per ogni } \alpha \in G,\ a \in L.$$

$T = V_f \underset{K}{\otimes} V_g$
R
o

Allora

(1) $\dim_K T/R \le n^2 \dim_K L$,

(2) $1_V\Lambda = \mathrm{id}_T$, *$\Lambda$ è una rappresentazione di V come K-spazio vettoriale*[28], *R è un sottomodulo di T rispetto a Λ,*

(3) $\Lambda_{T/R}$ [29] *è una rappresentazione unitale della K-algebra V_{fg}^-.*

Dimostrazione. Per ogni $\alpha, \beta \in G$, $a, b, c \in L$ vale

$$y_\alpha(c\alpha)a \otimes y_\beta b - y_\alpha a \otimes y_\beta(c\beta)b = \Delta(c)(y_\alpha a \otimes y_\beta b) \in R. \qquad (*)$$

(1) Ponendo $d := c\alpha$, $a := 1_L$, si ha $y_\alpha d \otimes y_\beta b - y_\alpha \otimes y_\beta(d\alpha^{-1}\beta)b \in R$ per $(*)$, quindi $R + y_\alpha d \otimes y_\beta b = R + y_\alpha \otimes y_\beta(d\alpha^{-1}\beta)b$ per ogni $\alpha, \beta \in G$, $b, d \in L$. Se B è una K-base di L, allora gli elementi $R + y_{\alpha \otimes y_\beta c}$ $(\alpha, \beta \in G,\ c \in B)$ formano un sistema di generatori di T/R come K-spazio vettoriale. Ne segue (1).

(2) V_f e V_g sono K-algebre per cui Λ è K-lineare, e $1_V\Lambda = (1_V \otimes 1_V)\lambda = \mathrm{id}_T$. Scegliendo $\alpha = \beta$, $b = 1_L$ in $(*)$ e scrivendo $c\alpha^{-1}$ al posto di c otteniamo

$$\Delta(c)\big((y_\alpha a)\Lambda\big) = (y_\alpha a \otimes y_\alpha)\Delta(c) = y_\alpha(ca) \otimes y_\alpha - y_\alpha a \otimes y_\alpha c \in R$$

per ogni $\alpha \in G$, $a, c \in L$. Allora, tramite le azioni degli elementi di V (che sono certe moltiplicazioni a sinistra), i generatori $\Delta(c)$ dell'ideale destro R vengono mandati in R. Ne segue (2).

(3) Siano $\bullet$ la moltiplicazione in V_{fg} e $\alpha, \delta \in G$, $a, d \in L$, $\gamma := \delta\alpha$, $c := g(\delta, \alpha)\gamma^{-1}$, $a^* := f(\delta, \alpha)\, d\alpha\, a$. L'endomorfismo di $(T,+)$

$$\begin{aligned}(y_\delta d \bullet y_\alpha a)\Lambda - (y_\alpha a)\Lambda(y_\delta d)\Lambda \\ &= \big(y_{\delta\alpha} g(\delta,\alpha) f(\delta,\alpha) d\alpha a \otimes y_{\delta\alpha} - y_{\delta\alpha} f(\delta,\alpha) d\alpha a \otimes y_{\delta\alpha} g(\delta,\alpha)\big)\lambda \\ &= \big(y_\gamma(c\gamma)a^* \otimes y_\gamma - y_\gamma a^* \otimes y_\gamma(c\gamma)\big)\lambda,\end{aligned}$$

è la moltiplicazione a sinistra per un elemento di R, come mostra $(*)$. Allora manda T in R, quindi lascia R invariante e induce su T/R l'endomorfismo zero. Pertanto $\Lambda_{T/R}$ è un anti-omomorfismo unitale della K-algebra V_{fg} in $\mathrm{End}_K(T/R,+)$. Ne segue (3). □

3.9. Corollario. *Supponiamo le ipotesi di* 3.8. *Allora*

(1) *T/R è un modulo unitale della K-algebra $V_{fg}^- \underset{K}{\otimes} V_f \underset{K}{\otimes} V_g$.*

(2) *Se (K, L) è galoissiana e $G = \mathrm{Aut}_K L$, allora $V_{fg}^- \underset{K}{\otimes} V_f \underset{K}{\otimes} V_g \cong K^{n^3 \times n^3}$.*

[28] cioè, Λ è un'applicazione K-lineare da V nel K-spazio $\mathrm{End}_K(T,+)$, cfr. p. 8.

[29] la rappresentazione K-lineare di V indotta da Λ rispetto al modulo T/R

DIMOSTRAZIONE. (1) L'azione standard di T su $(T,+)$, quindi anche su T/R, è data mediante moltiplicazione a destra. Siccome Λ induce soltanto molteplicazioni a sinistra, $\Lambda_{T/R}$ è una T-rappresentazione unitale di V_{fg}^-. Per 1.7.1, ne segue che T/R è un modulo unitale dell'algebra $V_{fg}^- \underset{K}{\otimes} T$.

(2) Se (K,L) è galoissiana, $G = \mathrm{Aut}_K L$, allora V_{fg}, V_f, V_g sono centrali semplici per 3.3. Per il caso speciale (3) dopo 1.10 anche $V_{fg}^- \underset{K}{\otimes} V_f \underset{K}{\otimes} V_g$ è centrale semplice. Allora la rappresentazione di $V_{fg}^- \underset{K}{\otimes} T$ in (1) deve essere iniettiva. Per 3.8(2),

$$\dim_K \mathrm{End}_K(T/R,+) = (\dim_K T/R)^2 \leq n^6 = \dim_K V_{fg}^- \underset{K}{\otimes} V_f \underset{K}{\otimes} V_g.$$

Allora la rappresentazione in (1) è un isomorfismo da $V_{fg}^- \underset{K}{\otimes} V_f \underset{K}{\otimes} V_g$ su $\mathrm{End}_K(T/R,+)$, $\dim_K \mathrm{End}_K(T/R,+) = n^6$, $\mathrm{End}_K(T/R,+) \cong K^{n^3 \times n^3}$. □

3.10. TEOREMA PRINCIPALE. *Sia (K,L) un'estensione galoissiana e $G := \mathrm{Aut}_K L$. Allora*

$$\mathcal{B}_L(K) \cong H^2(G, \dot{L}).$$

DIMOSTRAZIONE. Per ogni $f \in N^2(G,\dot{L})$ sia D_f l'elemento di $\mathcal{B}_L(K)$ per il quale esiste, per 3.3, un $m \in \mathbb{N}$ tale che $V_f \cong D_f^{m\times m}$. Sia

$$\varphi : N^2(G,\dot{L}) \to \mathcal{B}_L(K), \quad f \mapsto D_f.$$

Per 3.7 φ è suriettiva. Per 3.9(2) vale $D_{fg}^- \odot D_f \odot D_g = K$, quindi φ è un omomorfismo. Per 3.4, $\ker\varphi = N^2(G,\dot{L}) \cap B^2(G,\dot{L})$. Ora 3.1.3 implica che $H^2(G,\dot{L}) \cong N^2(G,\dot{L})/\ker\varphi \cong \mathcal{B}_L(K)$. □

Torniamo per un momento al caso di un gruppo di Galois G *ciclico*, $G = \langle\sigma\rangle$. Per ogni $z \in \dot{K}$ scriviamo D_z per l'elemento di $\mathcal{B}_L(K)$ tale che $L_{\sigma,z}$ è isomorfa all'algebra matriciale $D_z^{m\times m}$ per un $m \in \mathbb{N}$. Per ogni $z, z' \in K$ vale (ove $f_z \in N^2(G,\dot{L}$ come in 2.16):

$$D_z^- \odot D_{z'} = D_{f_z} \odot D_{f_{z'}}^- = D_{f_z f_{z'}^{-1}} = D_{z^{-1}z'}$$

per 2.16 e 3.10. Per 1.2(2), $D_{z^{-1}z'} = K$ se e solo se $z^{-1}z' \in \mathcal{N}(\dot{L})$. Allora vale

$$D_z = D_{z'} \Leftrightarrow \mathcal{N}(\dot{L})z = \mathcal{N}(\dot{L})z'.$$

Se $\mathcal{R}$ è un trasversale di $\mathcal{N}(\dot{L})$ in $\dot{K}$, allora le algebre cicliche $L_{\sigma,z}$ ($z \in \mathcal{R}$) danno origine a un sottogruppo di ordine $|\mathcal{R}|$ di $\mathcal{B}_L(K)$. Un risultato ben noto (v., per esempio, [**G**], §8) della teoria della coomologia dei gruppi ciclici finiti afferma che, per ogni G-modulo M, $H^2(G,M)$ è isomorfo al gruppo quoziente del gruppo degli elementi di M fissati da ogni elemento di G modulo il sottogruppo delle norme[30]. Nel nostro contesto quindi vale $\dot{K}/\mathcal{N}(\dot{L}) \cong \mathcal{B}_L(K)$ e allora $\mathcal{B}_L(K) = \{D_z | z \in \mathcal{R}\}$: Se G è ciclico, allora ogni elemento di $\mathcal{B}_L(K)$ nasce tramite una K-algebra ciclica.

Allora gli elementi di $\mathcal{B}(K)$ che hanno un campo di spezzamento che è un ampliamento *galoissiano* di K permettono una descrizione soddisfacente tramite i prodotti incrociati V_f. Il gruppo $\mathcal{B}_L(K)$ ha una struttura che si inquadra nel capitolo della

[30]Tale gruppo quoziente viene anche chiamato lo zeresimo gruppo di coomologia (di Tate) del gruppo G rispetto al modulo M, $H^0(G,M)$.

coomologia per il gruppo di Galois G con il gruppo moltiplicativo di L come G-modulo.

Ma lo corona di questa teoria è il suo ultimo pezzo: Vedremo che *ogni* elemento di $\mathcal{B}(K)$ ha un campo di spezzamento che è ampliamento galoissiano di K! Grazie a 3.5.6 basta mostrare che ogni elemento di $\mathcal{B}(K)$ ha un campo di spezzamento che è *separabile* e di dimensione finita su K il che è ovvio se $\operatorname{char} K = 0$. Per il caso $\operatorname{char} K \neq 0$ avremo bisogno della seguente osservazione. Scriviamo $\min_{x,K}$ per il polinomio minimo di un elemento algebrico x su K:

3.10.1. *Se y è un elemento algebrico di una K-algebra associativa e $p = \operatorname{char} K$, allora esiste un $n \in \mathbb{N}_0$ tale che y^{p^n} è separabile su K.*

Dimostrazione. Se y è separabile su K, la tesi è banale. Altrimenti vale $\min'_{y,K} = 0_K$. Sia $n \in \mathbb{N}_0$ massimale tale che p^n divide ogni esponente delle potenze della indeterminata t in $\min_{y,K}$. Allora $\min_{y^{p^n},K}(t^{p^n}) = \min_{y,K}$ e quindi $\min'_{y^{p^n},K} \neq 0_K$. Ne segue la tesi. □

La nostra strada per ottenere il risultato già indicato sulla separabilità toccherà l'area dei criteri di commutatività (per algebre di divisione) e farà uso dei commutatori di Lie in un'algebra A associativa:

$$\forall x, y \in A \quad [x, y] := xy - yx = x(y\rho - y\lambda).$$

Poniamo induttivamente $[x_1, \ldots, x_n] := [[x_1, \ldots, x_{n-1}], x_n]$ per ogni $n \in \mathbb{N}_{>1}$, $x_i \in A$.

3.11. Proposizione. *Sia D un corpo tale che per ogni $x, y \in D$ esiste un $m \in \mathbb{N}$ tale che $[x, y, \underset{m}{\ldots}, y] = 0_D$. Allora D è commutativo.*

Come preparazione osserviamo che, qualunque siano x, y elementi di un'algebra associativa A,

3.11.1. $\forall z \in C_A(y) \quad z[x, y] = [zx, y],\ [y, x]z = [y, xz]$. □

3.11.2. $\forall n \in \mathbb{N} \quad [x, y, \underset{n}{\ldots}, y] = \sum_{k=0}^{n} \binom{n}{k} (-1)^k y^k x y^{n-k}$,

perchè $[x, y, \underset{n}{\ldots}, y] = x(y\rho - y\lambda)^n = x \sum_{k=0}^{n} \binom{n}{k} (y\rho)^{n-k}((-y)\lambda)^k$ per il fatto che $y\lambda$, $y\rho$ commutano tra loro. □

Dimostrazione di 3.11. Assumiamo per assurdo che ci siano $x, y \in D$ tali che $[x, y] \neq 0_D$. Poniamo $z_0 := x$, $z_n := [x, y, \underset{n}{\ldots}, y]$ per ogni $n \in \mathbb{N}$. Sia $k \in \mathbb{N}$ minimale tale che $z_k = 0_D$. Allora vale $k \geq 2$ e $y, z_{k-1} \in C_D(y) \setminus \{0_D\}$. Ponendo $u := -y z_{k-1}^{-1} z_{k-2}$ si ha, per 3.11.1,

$$y = y z_{k-1}^{-1} z_{k-1} = y z_{k-1}^{-1} [z_{k-2}, y] = [y z_{k-1}^{-1} z_{k-2}, y] = [y, u].$$

Allora $y = [y, u, \underset{n}{\ldots}, u]$ per ogni $n \in \mathbb{N}$, quindi $y = 0_D$, assurdo. □

3.12. Corollario. *Se D è un corpo, $p := \operatorname{char} D > 0$ ed esiste per ogni $x, y \in D$ un $n \in \mathbb{N}$ tale che $[x, y^{p^n}] = 0_D$, allora D è commutativo.*

Dimostrazione. Per 3.11 basta dimostrare che per ogni $x, y \in D$ vale $[x, y^{p^k}] = [x, y, \underset{p^k}{\ldots}, y]$ per ogni $k \in \mathbb{N}$. Per $k = 1$ questa equazione segue da 3.11.2. Applicando la regola all'elemento y^p e induttivamente per $k - 1$ al posto di k otteniamo

$$[x, y^{p^k}] = [x, (y^p)^{p^{k-1}}] = [x, y^p, \underset{p^{k-1}}{\ldots}, y^p] = [x, y, \underset{p}{\ldots}, y,\ \ldots\ , y, \underset{p}{\ldots}, y],$$

applicando nell'ultimo passo p^{k-1} volte il caso iniziale dell'induzione. □

3.13. Lemma (Noether-Jacobson). *Sia D un'algebra di divisione algebrica su K. Se D non è commutativa, allora $D \setminus Z(D)$ contiene un elemento separabile su K.*

Dimostrazione. Supponiamo che ogni elemento di D separabile su K sia centrale. Sia $p := \operatorname{char} K > 0$, $y \in D$. Per 3.10.1 esiste un $n \in \mathbb{N}_0$ tale che y^{p^n} è separabile su K e quindi $y^{p^n} \in Z(D)$. Segue da 3.12 che D è commutativa. □

3.14. Teorema (Köthe (1932)). [31] *Sia $D \in \mathcal{B}(K)$. Allora esiste un sottocampo massimale di D che è separabile su K.*

Di conseguenza esiste un campo di spezzamento di D che è galoissiano su K.

Dimostrazione. Sia L sottocampo di D, $K \leq L$, e L massimale tra i sottocampi di D contenenti K e separabili su K. Sia $B := C_D(L)$. Per 2.2(3) vale $C_D(B) = L$. Allora (o per 1.3(1) o per dimostrazione diretta) B è algebra di divisione centrale su L. Se B non fosse commutativa, allora per 3.13 esisterebbe un elemento $y \in B \setminus L$ separabile su L. Allora $L(y)$ sarebbe un ampliamento proprio di L e separabile su K, assurdo. Allora B è commutativa, $L = C_D(B) \geq B = C_D(L)$, quindi $L = C_D(L)$ e L è sottocampo unitale massimale di D.

Per 3.5.4, un sottocampo massimale è un campo di spezzamento di D. Per quanto abbiamo dimostrato, possiamo scegliere un tale sottocampo che è separabile su K. Quindi esiste un ampliamento galoissiano di esso, e per 3.5.6 ne segue l'ultima tesi del teorema. □

Con 3.14 abbiamo il seguente raffinamento di 3.5.5:

3.14.1. $\mathcal{B}(K) = \bigcup_{(K,L)\ gal.} \mathcal{B}_L(K)$. □

Il teorema di Hasse-Brauer-Noether e Albert (v. p. 8) può essere espresso in questa forma:

Se K è un campo numerico, allora $\mathcal{B}(K) = \bigcup_{\substack{(K,L)\,gal. \\ \mathrm{Aut}_K L\ ciclico}} \mathcal{B}_L(K)$.

È noto, però, che un tale raffinamento di 3.14.1 non vale per campi K in generale (Albert 1932).

La prima parte del teorema seguente implica, in particolare, che ogni gruppo di Brauer è un gruppo di torsione:

3.15. Teorema (Brauer (1930)). *Per ogni $D \in \mathcal{B}(K)$ vale*

(1) *$o(D) | \operatorname{ind} D$.*
(2) *Ogni divisore primo di $\operatorname{ind} D$ divide $o(D)$.*

Dimostrazione. Sia $n := \operatorname{ind} D$. Per 3.14.1 D ha un campo di spezzamento L galoissiano su K.

(1) Dobbiamo dimostrare che vale $D^n = K$ (in $\mathcal{B}(K)$). Per 3.6 possiamo assumere che L sia sottocampo di un'algebra matriciale A su D tale che $C_A(L) = L$. Per 2.2(2) ne segue che $\dim_K A = (\dim_K L)^2$. Per 3.3 esiste un $f \in N^2(G, \dot{L})$ tale che $A \cong V_f$. Per 2.6.1 lo (a meno di isomorfismi unico) A-modulo unitale irriducibile ha

[31] Questo importante teorema viene anche attribuito a E. Noether che nel 1933 pubblicò una dimostrazione diversa da quella del suo allievo Köthe.

dimensione n su L. Ora 3.1.4 mostra che $f^n \in B^2(G, \dot{L})$. Ne segue la tesi per 3.10.

(2) Sia p un divisore primo di n, P un p-sottogruppo di Sylow di G, K' il sottocampo di L degli elementi fissati da ogni $\alpha \in P$. Nella notazione di 3.5.7 vale $D_{K'} \cong D(K')^{m\times m}$ per un $m \in \mathbb{N}$. L è campo di spezzamento della K-algebra D, allora anche della K'-algebra $D(K')$. Per 3.6 vale $\operatorname{ind} D(K') | \dim_{K'} L = p^j$ per un $j \in \mathbb{N}$. Mostriamo che

$$o(D(K')) \neq 1$$

(l'ordine nel gruppo $\mathcal{B}(K')$): Altrimenti varrebbe $D_{K'} = K'$, K' sarebbe un campo di spezzamento di D. Ma $p|n$, $p \nmid \dim_K K'$, assurdo per 3.6.

Per (1) vale $1 \neq o(D(K'))|\operatorname{ind} D(K')|p^j$, allora $p|o(D(K'))$. Ne segue $p|o(D)$ per 3.5.7. □

APPENDICE A

Il teorema principale 3.10 permette una descrizione degli elementi del gruppo di Brauer $\mathcal{B}(K)$ mediante i prodotti incrociati nel caso che tali elementi abbiano un campo di spezzamento L galoissiano su K. Più esattamente, tale teorema collega strutturalmente il sottogruppo $\mathcal{B}_L(K)$ e la coomologia per l'azione del gruppo di Galois di (K, L) su $\dot{L}$. Inoltre, grazie al teorema di Köthe 3.14, si ha una riduzione del caso arbitrario al caso galoissiano trattato in 3.10. Molto più tardi si è visto che i sottocampi massimali separabili in un'algebra di divisione centrale di dimensione finita (v. 3.14) permettono una caratterizzazione molto soddisfacente in termini della teoria delle algebre di Lie. Tale risultato sarà lo scopo di questa aggiunta all'esposizione nei capitoli precedenti.

Mettiamo in evidenza che la nostra dimostrazione del Lemma di Noether 3.13 (nella forma generalizzata successivamente da Jacobson[32]) utilizza soltanto poche regole elementari del ≪Lie bracket≫ che la rendono molto trasparente. Così non vogliamo nascondere la speranza che ci saranno da scoprire altri legami tra le teorie delle algebre associative e di Lie.[33] Già la base storica, la dimostrazione che l'algebra dei quaternioni sia centrale semplice, può essere vista in questa luce: In [**P**], 1.6, si lavora vantaggiosamente con la struttura di Lie dell'algebra per ottenere il risultato in maniera elegante.

Ci serviremo del risultato seguente che diamo senza dimostrazione.[34]

Proposizione. *Sia (K, L) un'estensione di campi di dimensione finita. Sono equivalenti:*

(i) *(K, L) è separabile.*
(ii) *La K-algebra $L \underset{K}{\otimes} L$ è semisemplice.*[35]

A.1. Proposizione. *Se (K, L) è un'estensione di campi separabile di dimensione finita, allora l'applicazione $L \to \{0_K\}$ è l'unica derivazione K-lineare di L.*

Dimostrazione. Sia ∂ una derivazione di L. Applichiamo l'esempio (3) in 1.5 (con $S = A = B = L$). Cioè otteniamo una realizzazione prodotto $(L^{2\times 2}, \varphi, \psi)$ per (L, L) tramite

$$\varphi : x \mapsto \begin{pmatrix} x & x\partial \\ 0_L & x \end{pmatrix}, \qquad \psi : y \mapsto \begin{pmatrix} y & 0_L \\ 0_L & y \end{pmatrix} \qquad (x, y \in L).$$

[32] La formulazione in 3.13 è di nuovo più generale di una piccolezza.

[33] Non sarà sfuggito al lettore attento che la dimostrazione di 3.12 e quindi di 3.13 è collegata alla nozione di algebra di Lie ristretta.

[34] In una forma più generale si trova una dimostrazione per esempio in [**DK**], 6.1.2.

[35] $L \underset{K}{\otimes} L$ è commutativa, allora è semisemplice se e solo se non ha elementi nilpotenti non nulli.

Allora la sottoalgebra $(L\varphi)(L\psi)$ di $L^{2\times 2}$ è immagine epimorfa di $L \underset{K}{\otimes} L$ e contiene le matrici

$$\begin{pmatrix} 0_L & x\partial \\ 0_L & 0_L \end{pmatrix} = x\varphi - x\psi \qquad (x \in L)$$

che generano un'ideale di $(L\varphi)(L\psi)$ nel quale ogni prodotto è zero. Per la separabilità di (K, L) la proposizione precedente mostra che $L \underset{K}{\otimes} L$, quindi anche ogni sua immagine epimorfa, è semisemplice. Ne segue che ∂ è l'applicazione zero. □

Per ogni K-sottospazio T di una K-algebra $(A, +, \circ)$ poniamo

$$N_A(T) := \{x | x \in A,\, T \circ x \subseteq T\},$$

detto il normalizzante di T in A. Se A è associativa o un'algebra di Lie, allora $N_A(T)$ è una sottoalgebra di A. Nella teoria delle algebre di Lie sono di massima importanza le sottoalgebre di Cartan che sono le sottoalgebre (Lie-)nilpotenti T tali che $N_A(T) = T$.

Se A è un'algebra di Lie e L un campo di ampliamento del campo di base K, allora lo L-spazio vettoriale destro $A \underset{K}{\otimes} L$ è un'algebra di Lie su L dove si pone

$$[x \otimes a, y \otimes b] := [x, y] \otimes ab$$

per elementi arbitrari x, y di una K-base di A, $a, b \in L$. Quindi si ottiene, come nel caso dell'algebra associativa unitaria, un ampliamento del campo di base anche per le algebre di Lie, e l'algebra di Lie che nasce così viene anche denotata con A_L. Si ha

Proposizione. *Se H è una sottoalgebra di Cartan dell'algebra di Lie A, allora H_L è una sottoalgebra di Cartan di A_L, per ogni ampliamento L di K.*

Per noi sarà interessante il caso di un'algebra *associativa* A, considerata come algebra di Lie con il ≪Lie bracket≫ come prodotto di Lie. Per esempio vale

Proposizione. *Se K è algebricamente chiuso, $n \in \mathbb{N}$, allora le sottoalgebre di Cartan dell'algebra di Lie $K^{n\times n}$ sono la sottoalgebra $\{diag[x_1, \ldots, x_n] | x_i \in K\}$ e le sue coniugate tramite automorfismi dell'algebra associativa $K^{n\times n}$.*[36]

Dati $x, y, z_1, \ldots, z_n$ elementi di un'algebra associativa, si dimostra induttivamente che

$$[xy, z_1, \ldots, z_n] = \sum [x, z_{i_1}, \ldots, z_{i_r}][y, z_{i_{r+1}}, \ldots, z_{i_n}]$$

dove la sommatoria si estende su tutte le coppie $((i_1, \ldots, i_r), (i_{r+1}, \ldots, i_n))$ tali che $0 \le r \le n$, $i_1 < \cdots < i_r$, $i_{r+1} < \cdots < i_n$, $i_j \ne i_k$ se $j \ne k$.[37] Delle molte applicazioni di questa formula una utile è questa: Se T è una sottoalgebra nilpotente di Lie e $k \in \mathbb{N}$ tale che $[T, \underset{k}{\ldots}, T] = \{0_A\}$, $n \ge 2k$, allora $[xy, z_1, \ldots, z_n] = 0_A$ per ogni $x, y, z_1, \ldots, z_n \in T$. Ora sia $m \in \mathbb{N}_0$ minimale tale che $[xy, T, \underset{m}{\ldots}, T] \subseteq T$. Segue che, se $m > 0$, allora $[xy, T, \underset{m-1}{\ldots}, T] \subseteq N_A(T)$. Nel caso di una sottoalgebra *di Cartan* T quest'ultimo implicherebbe che $[xy, T, \underset{m-1}{\ldots}, T] \subseteq T$, assurdo per la definizione di m. Concludiamo allora che $m = 0$, cioè, che $ab \in T$. Abbiamo dimostrato:

[36] v. il caso speciale di 2.1

[37] Il caso $n = 1$ esprime il fatto che per ogni elemento z l'applicazione $y \mapsto [y, z]$ è una derivazione dell'algebra associativa data.

A.2. Proposizione. *Se A è un'algebra associativa, allora ogni sottoalgebra di Cartan di A è una sottoalgebra associativa di A.* □

A.3. Teorema (Siciliano (2006)). *Sia $D \in \mathcal{B}(K)$, $L \subseteq D$. Sono equivalenti*

(i) *L è un sottocampo massimale di D e separabile su K.*
(ii) *L è un sottocampo di D tale che $L = N_D(L)$.*[38]
(iii) *L è una sottoalgebra di Cartan di D* [38].

Dimostrazione. (i)⇒(ii) Se $x \in N_D(L)$, allora l'applicazione $L \to L$, $y \mapsto [y, x]$, è una derivazione K-lineare di L. Per A.1 ne segue che $x \in C_D(L)$, quindi $x \in L$ per 2.4.

(ii)⇒(iii) è banale.

(iii)⇒(i) Se vale (iii), allora L è sottoalgebra associativa di D per A.2, quindi un'algebra di divisione per 1.3(1) e per 3.11 commutativa. Pertanto L è un sottocampo di A che deve essere massimale per (iii). Per dimostrare la separabilità consideriamo un'estensione algebricamente chiusa $\bar{L}$ di L. Allora vale $L \underset{K}{\otimes} \bar{L} \cong \{diag[x_1, \ldots, x_n] | x_i \in \bar{L}\}$ per 3.5.1 e 1.13.2, applicando le due proposizioni riportate prima di A.2. Evidentemente $L \underset{K}{\otimes} L$ è L-sottoalgebra di $L \underset{K}{\otimes} \bar{L}$, quindi è priva di elementi nilpotenti non nulli. Ne segue che $L \underset{K}{\otimes} L$ è semisemplice, e per la proposizione prima di A.1 la dimostrazione è completa. □

È ben noto che ogni algebra di Lie associata ad un'algebra associativa di dimensione finita ha una sottoalgebra di Cartan. Dunque il risultato A.3 (più precisamente: la implicazione (iii)⇒(i)) comporta una dimostrazione alternativa – tramite alcuni risultati della teoria delle algebre di Lie – di 3.14. È da notare, però, che si basa sulla parte meno banale di A.3, e ulteriormente che fa uso della proposizione 3.11 che può essere vista come il nocciolo dell'idea della dimostrazione presentata nel 3^o capitolo. Nonostante ciò, il legame stabilito in A.3 (v. [**Sic**]) certamente merita riconoscimento. Si tratta di una scoperta che senza dubbio sarebbe piaciuta molto a Emmy Noether.

[38] D come algebra di Lie, con il ≪Lie bracket≫ come moltiplicazione.

Bibliografia

[Am] Amitsur, S. A., Finite subgroups of division rings, Trans. Amer. Math. Soc. 80 (1955), 361-386

[DK] Drozd, Yu. A. e Kirichenko, V. V., *Finite Dimensional Algebras*, Berlin Heidelberg New York 1994

[G] Gaschütz, W., *Lezioni sulla coomologia dei gruppi finiti*, in: Quaderni C.N.R., a. a. 1971-72, Padova 1973

[L] Lam, T. Y., *A First Course in Noncommutative Rings*, New York Berlin Heidelberg 2001[2]

[P] Pierce, R. S., *Associative Algebras*, New York Heidelberg Berlin 1982

[Sic] Siciliano, S., Cartan subalgebras in Lie algebras of associative algebras, Comm. Algebra 34 (2006), 4513-4522

[Sm] Smoktunowicz, A., On some results related to Köthe's conjecture, Serdica Math. J. 27 (2001), 159-170

[WL] Woo Lee, On Nagata-Higman theorem, J. Appl. Math. & Informatics 27 (2009), 1489-1492

Indice analitico

algebra
  K-, 3
  centrale, 3
  ciclica, 5
  dei quaternioni, 2
  di Hamilton, 3
automorfismo interno, 15

cobordo, 23
cociclo, 23
commutatore di Lie, 30

derivazione, 9

gruppo di coomologia, 2^o, 23

indice di Schur, 17

modulo libero, 11

nil, 2
norma, 6
normalizzante, 34

prodotto incrociato, 21
prodotto tensoriale
  esterno, 10
  interno, 10
proprietà universale, 10

quaternioni
  algebra, 2
  gruppo, 3

realizzazione prodotto, 9

scalari, 3
sistema noetheriano di fattori, 24
sottoalgebra di Cartan, 34

twist di Hilbert, 5

unitale
  omomorfismo, 8
  sottoalgebra, 8