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,

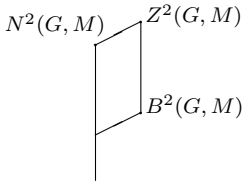
perché $f(\alpha\beta,\gamma)\, f(\alpha,\beta)\gamma = \nu(\gamma)\big(\nu(\alpha\beta\gamma)\big)^{-1}\big(\nu(\alpha\beta)\big)\gamma\,\big((\nu(\alpha\beta))\gamma\big)^{-1}\nu(\beta)\gamma\,\nu(\alpha)\beta\gamma =$
$= \nu(\gamma)\big(\nu(\beta\gamma)\big)^{-1}\big(\nu(\beta)\big)\gamma\,\nu(\beta\gamma)\,\nu(\alpha\beta\gamma)^{-1}\,\nu(\alpha)\beta\gamma = f(\beta,\gamma)f(\alpha,\beta\gamma)$ *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 $\operatorname{End}_{D^-} V \cong \big(\operatorname{End}_{D^-}(D, +)\big)^{m\times m} \cong D^{m\times m}$ 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 $L = C_A(L) \cong C_A(L)\rho = \operatorname{End}_{A^-\underset{K}{\otimes}L}(A, +)$, 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 $\operatorname{End}_{A^-\underset{K}{\otimes}L}(A, +)$, 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:

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

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) $1_V\Lambda = \mathrm{id}_T$, Λ *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. □