

Introduzione

Lo scopo di questa tesi è definire un invariante importante di un campo, cioè il gruppo di Brauer, e mostrare che nel caso di un campo locale questo è isomorfo al gruppo additivo \mathbb{Q}/\mathbb{Z} .

Nel primo capitolo si vedrà innanzitutto il teorema di Wedderburn, che ci dice come sono fatte le algebre semplici centrali su un campo. Poi, dopo aver scorso le proprietà del prodotto tensoriale, definiremo il gruppo di Brauer di un campo come l'insieme delle algebre semplici centrali sul campo, a meno di una certa relazione d'equivalenza, con l'operazione di prodotto tensoriale.

La trattazione continuerà con due risultati fondamentali sulle algebre semplici che sono il teorema di Noether-Skolem ed il teorema del centralizzatore, di cui osserveremo un'applicazione immediata nel determinare il gruppo di Brauer di \mathbb{R} . Definiremo anche gli omomorfismi di norma ridotta e traccia ridotta da un'algebra semplice al suo centro, perché ci serviranno nell'ultima parte.

Vedremo poi un tipo molto importante di algebre semplici, che sono i prodotti incrociati; queste ci permetteranno anche di collegare il gruppo di Brauer con i gruppi di coomologia. Come caso particolare di prodotti incrociati, approfondiremo il discorso sulle algebre cicliche, che ci serviranno poi per determinare il gruppo di Brauer nel caso di un campo locale.

Nel secondo capitolo vedremo alcune proprietà degli anelli di valutazione discreta e dei campi locali, fino ad arrivare al risultato fondamentale che mette in corrispondenza le estensioni non ramificate di un campo locale con le estensioni separabili del suo campo dei residui.

Concluderemo mostrando come le algebre semplici centrali su un campo locale si possono scrivere sotto forma di algebre cicliche. Questo ci permetterà di definire l'invariante di Hasse, che vedremo essere un isomorfismo tra il gruppo di Brauer del campo locale e il gruppo additivo \mathbb{Q}/\mathbb{Z} .

Indice

Introduzione	ii
Convenzioni	iv
1 Gruppo di Brauer	1
1.1 Teorema di Wedderburn	2
1.2 Prodotto Tensoriale	10
1.2.1 Prodotto tensoriale di spazi vettoriali e di algebre	17
1.3 Gruppo di Brauer	22
1.4 Teorema di Noether-Skolem e Teorema del Centralizzatore	29
1.4.1 Il Gruppo di Brauer di \mathbb{R}	37
1.5 Norma e Traccia ridotta	43
1.6 Prodotti Incrociati	48
1.7 Algebre Cicliche	68
2 Campi Locali	73
2.1 Anelli di valutazione discreta e domini di Dedekind	74
2.1.1 Domini di Dedekind	79
2.2 Estensioni del campo dei quozienti	82
2.2.1 Estensioni nel caso locale	85
2.3 Completamento	88
2.3.1 Estensioni di campi completi	90
2.4 Gruppo di Brauer di un campo locale	98
Bibliografia	105

Convenzioni

Stabiliamo alcune convenzioni che valgono per tutta questa trattazione:

- Se $a, b \in \mathbb{Z}$, $a|b$ significa che a divide b .
- Se G è un gruppo, indichiamo con $|G|$ l'ordine di G . Se $g \in G$ indichiamo con $\langle g \rangle$ il sottogruppo generato da g .
- Tutti gli anelli considerati sono *unitari*.
- Un'*ideale minimale* (destro o sinistro) di un anello, è un ideale non nullo che è minimale per la relazione di inclusione.
- Se R è un anello, indichiamo con ${}_R R$, l'anello visto come modulo sinistro su sè stesso ed analogamente R_R sarà l'anello visto come modulo destro. Inoltre R^* indica il gruppo moltiplicativo degli elementi invertibili di R .
- Se F è un anello commutativo ed A è un anello, diciamo che A è una *F-algebra* se A è un F -modulo e vale $\alpha(ab) = (\alpha a)b = a(\alpha b)$ per ogni $\alpha \in F$, $a, b \in A$.
- Tutti gli spazi vettoriali hanno dimensione finita. Se V è uno spazio vettoriale sul campo F , indicheremo la dimensione di V su F con $[V : F]$.
- Se M ed N sono due R -moduli, indichiamo con $\text{Hom}_R(M, N)$ il gruppo degli R -omomorfismi da M in N .
- Se M è un R -modulo, indichiamo con $\text{End}_R(M)$ l'anello degli R -endomorfismi di M e con $\text{Aut}_R(M) \subset \text{End}_R(M)$ il gruppo moltiplicativo degli R -endomorfismi invertibili.
- Indichiamo con $M_n(R)$ l'anello delle matrici $n \times n$ ad elementi in R .

Capitolo 1

Gruppo di Brauer

1.1 Teorema di Wedderburn

Definizione 1.1.1. Un anello $R \neq 0$ è un *anello di divisione* se ogni elemento di R non nullo è invertibile.

Osservazione 1.1.2. Sia D un anello di divisione, e sia F il suo centro. Allora F è un campo e D è un'algebra su F .

Dimostrazione. E' chiaro che se due elementi stanno nel centro di D anche la loro somma e il loro prodotto ci stanno. E' altrettanto evidente che se un elemento commuta con tutti gli altri, anche il suo inverso farà lo stesso ($ad = da$ implica $da^{-1} = a^{-1}d$, moltiplicando a destra e a sinistra per a^{-1}), quindi F è un campo. Prendendo come moltiplicazione per scalare la moltiplicazione in D , si ha che D è uno spazio vettoriale su F , e si ha che

$$\alpha(ab) = (\alpha a)b = a(\alpha b) \quad \text{per ogni } a, b \in D, \alpha \in F$$

quindi è un'algebra. □

Per questo motivo useremo indifferentemente i termini *anello di divisione* e *algebra di divisione*.

Definizione 1.1.3. Sia R un anello, $M \neq 0$ un R -modulo. Diciamo che M è *semplice* (o *irriducibile*) se M non ha sottomoduli propri non nulli.

Per esempio un ideale minimale (destra o sinistra) di R è un modulo semplice.

Proposizione 1.1.4 (Lemma di Schur). *Sia M un modulo semplice sull'anello R , allora $\text{End}_R(M)$ è un'algebra di divisione.*

Dimostrazione. Sia $f \in \text{End}_R(M)$, $f \neq 0$. Allora $\text{Ker } f$ e $\text{Im } f$ sono sottomoduli di M , quindi per la semplicità di M e per il fatto che $f \neq 0$ si ha per forza $\text{Ker } f = 0$, $\text{Im } f = M$. Quindi f è 1-1 e su e ammette un inverso in $\text{End}_R(M)$. □

Definizione 1.1.5. Sia $R \neq 0$ un anello. Diciamo che R è un *anello semplice* se ${}_R R$ è Artiniano e R non ha ideali bilateri propri non nulli.

Proposizione 1.1.6. Sia D un anello di divisione, allora $M_n(D)$ è un anello semplice.

Dimostrazione. Chiaramente $M_n(D)$ è Artiniano perché gli ideali destri o sinistri di $M_n(D)$ sono sottospazi vettoriali di $M_n(D)$ e quindi la condizione della catena discendente è verificata per motivi di dimensione. Ora è sufficiente mostrare che se I è un ideale bilatero di $M_n(D)$, allora $1 \in I$. Per vederlo, prendiamo una matrice $0 \neq A \in I$, $A = (a_{ij})$, questa avrà almeno un elemento non nullo $(a_{i_0 j_0})$, se indichiamo con E_{ij} la matrice che ha tutti gli elementi nulli a parte 1 nella posizione (i, j) , un semplice calcolo mostra che

$$E_{kk} = a_{i_0 j_0}^{-1} E_{k i_0} A E_{j_0 k} \in I \quad \text{per ogni } k = 1, \dots, n.$$

Quindi

$$1 = \sum_{k=1}^n E_{kk} \in I.$$

□

Quello che vogliamo arrivare a vedere è che in realtà questo è l'unico esempio possibile, cioè un anello semplice è sempre un anello di matrici su un anello di divisione.

Teorema 1.1.7. Sia R un anello semplice e sia I un ideale minimale sinistro di R (un tale I esiste perché l'insieme degli ideali sinistri è non nullo, in quanto R è non nullo, e ammette un elemento minimale perché ${}_R R$ è Artiniano). Se $M \neq 0$ è un R -modulo sinistro Artiniano, allora esiste un n tale che

$$M \simeq \bigoplus_{i=1}^n I.$$

Dimostrazione. Consideriamo

$$0 \neq A = \sum_{r \in R} I r \subseteq R,$$

A è un ideale bilatero di R non nullo, quindi $A = R$, ne segue che

$$M = \sum_{m \in M} Rm = \sum_{m \in M} Am = \sum_{m \in M} \sum_{r \in R} Irm = \sum_{i \in J} Im_i$$

dove J è un insieme di indici, eventualmente infinito.

Definiamo $M_i := Im_i$; abbiamo che M_i è l'immagine dell'omomorfismo di R -moduli $\phi : I \rightarrow M$ dato da $x \mapsto xm_i$. Ma I è un modulo semplice, quindi $\text{Ker } \phi = 0$ oppure $\text{Ker } \phi = I$; abbiamo allora che $M_i \simeq I$ oppure $M_i = 0$. Possiamo quindi definire

$$\bar{J} := \{i \in J \mid M_i \simeq I\} \quad \text{così che} \quad M = \sum_{i \in \bar{J}} M_i.$$

Ora consideriamo Λ , l'insieme dei $J_\alpha \subset \bar{J}$ tali che

$$\sum_{i \in J_\alpha} M_i = \bigoplus_{i \in J_\alpha} M_i. \quad (1.1)$$

Questo insieme è non vuoto perché, se prendiamo J_α di cardinalità 1, la condizione (1.1) è verificata. Inoltre, se consideriamo una catena

$$J_\alpha^1 \subset J_\alpha^2 \subset \dots \subset J_\alpha^n \subset \dots$$

abbiamo che $\bigcup_n J_\alpha^n$ verifica ancora la condizione (1.1). Infatti, se così non fosse, avremmo che esistono M_{i_1}, \dots, M_{i_n} , $\{i_1, \dots, i_n\} \subset \bigcup_n J_\alpha^n$ tali che la somma $M_{i_1} + \dots + M_{i_n}$ non sia diretta. Ma ciascuno degli i_j sta in un J_α^j ; consideriamo il più grande di questi, diciamo che sia J_α^m , abbiamo allora $i_j \in J_\alpha^m$ per $j = 1, \dots, n$. Quindi per ipotesi la somma $M_{i_1} + \dots + M_{i_n}$ è diretta.

Possiamo allora applicare il lemma di Zorn a Λ ed ottenere un elemento massimale $\hat{J} \subset \bar{J}$. Adesso vogliamo mostrare che

$$\bigoplus_{i \in \hat{J}} M_i = \sum_{i \in \bar{J}} M_i = M.$$

Se così non fosse, esisterebbe $j \in \bar{J}$ con $M_j \not\subset \bigoplus_{i \in \hat{J}} M_i$, quindi $j \notin \hat{J}$. Ma

$$M_j \cap \left(\bigoplus_{i \in \hat{J}} M_i \right) \subsetneq M_j$$

quindi $M_j \cap \left(\bigoplus_{i \in \hat{J}} M_i\right) = 0$, poiché M_j è un modulo semplice. Ma in questo caso avremmo la somma diretta

$$\bigoplus_{i \in \hat{J} \cup \{j\}} M_i \supsetneq \bigoplus_{i \in \hat{J}} M_i$$

che contraddice la massimalità di \hat{J} .

Per concludere, mostriamo che \hat{J} è un insieme finito. In caso contrario, sia $\{i_j\}_{j \geq 1} \subset \hat{J}$ una successione infinita di indici tutti diversi tra loro e sia per ogni $k \geq 1$, $\hat{J}_k = \hat{J} \setminus \{i_1, \dots, i_k\}$. Allora

$$M \supset \sum_{i \in \hat{J}_1} M_i \supset \dots \supset \sum_{i \in \hat{J}_k} M_i \supset \dots$$

sarebbe una catena strettamente discendente infinita il che è impossibile perché M è Artiniano. \square

Osservazione 1.1.8. Se R_R è artiniano, vale lo stesso risultato scegliendo dei moduli destri invece di quelli sinistri. Da questo teorema, prendendo come M un ideale minimale sinistro (destro) di R , si ottiene che tutti gli ideali minimali sinistri (destri) di un anello semplice sono isomorfi. Si ricava anche il fatto che ogni ideale sinistro (destro) di un anello semplice è somma diretta di ideali minimali sinistri (destri), prendendo come M un ideale sinistro (destro) qualunque.

Teorema 1.1.9. *Sia M un R -modulo sinistro, allora*

$$\text{End}_R \left(\bigoplus_{i=1}^n M \right) \simeq M_n(\text{End}_R(M)).$$

Dimostrazione. Poniamo $S = \bigoplus_{i=1}^n M$ e $s = (m_1, \dots, m_n)$ e siano $\pi_i : S \rightarrow M$ e $\iota_i : M \rightarrow S$ rispettivamente la proiezione e l'iniezione canonica sulla i -esima componente. Si ha chiaramente che:

$$\pi_i \iota_j = \begin{cases} id_M & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases} \quad \text{e} \quad \sum_{k=1}^n \iota_k \pi_k = id_S.$$

Ora, consideriamo una qualunque $f \in \text{End}_R(S)$, abbiamo che $\pi_i f \iota_j \in \text{End}(M)$ e quindi esiste una mappa additiva

$$\alpha : \text{End}_R(S) \rightarrow M_n(\text{End}_R(M)) \quad \text{con} \quad \alpha(f) = (\pi_i f \iota_j)_{1 \leq i, j \leq n}.$$

Questa è un omomorfismo di anelli, infatti

$$\alpha(id_S) = (\pi_i \iota_j)_{1 \leq i, j \leq n} = id_M I_n;$$

e

$$\begin{aligned} \alpha(fg) &= (\pi_i f g \iota_j) \\ &= \left(\pi_i f \left(\sum_{k=1}^n \iota_k \pi_k \right) g \iota_j \right) \\ &= \left(\sum_{k=1}^n (\pi_i f \iota_k) (\pi_k g \iota_j) \right)_{1 \leq i, j \leq n} \\ &= \alpha(f) \alpha(g). \end{aligned}$$

Viceversa, sia data $(f_{ij})_{1 \leq i, j \leq n} \in M_n(\text{End}_R(M))$ e consideriamo la mappa additiva

$$\beta : M_n(\text{End}_R(M)) \rightarrow \text{End}_R(S) \quad \text{data da} \quad (f_{ij}) \mapsto \sum_{1 \leq i, j \leq n} \iota_i f_{ij} \pi_j.$$

Anche questa è un omomorfismo di anelli, visto che

$$\beta(id_M I_n) = \sum_{1 \leq i, j \leq n} \iota_i id_M \delta_{ij} \pi_j = \sum_{k=1}^n \iota_k \pi_k = id_S$$

e

$$\begin{aligned}
 \beta((f_{ik})(g_{kj})) &= \beta\left(\left(\sum_{k=1}^n f_{ik}g_{kj}\right)\right) \\
 &= \left(\sum_{i,j,k} \iota_i f_{ik}g_{kj}\pi_j\right) \\
 &= \left(\sum_{i,j,k} \iota_i f_{ik}\pi_k \iota_k g_{kj}\pi_j\right) \\
 &= \left(\sum_{i,k} \iota_i f_{ik}\pi_k\right) \left(\sum_{k,j} \iota_k g_{kj}\pi_j\right) \\
 &= \beta(f)\beta(g).
 \end{aligned}$$

Ora,

$$\begin{aligned}
 \alpha(\beta((f_{ij}))) &= \alpha\left(\sum_{1 \leq i,j \leq n} \iota_i f_{ij}\pi_j\right) \\
 &= \left(\pi_k \sum_{1 \leq i,j \leq n} \iota_i f_{ij}\pi_j \iota_l\right)_{1 \leq k,l \leq n} \\
 &= \left(\sum_{1 \leq i,j \leq n} \pi_k \iota_i f_{ij}\pi_j \iota_l\right) \\
 &= (f_{kl});
 \end{aligned}$$

e

$$\beta(\alpha(f)) = \beta((\pi_i f \iota_j)) = \left(\sum_{1 \leq i,j \leq n} \iota_i \pi_i f \iota_j \pi_j\right) = f.$$

In conclusione, α e β sono omomorfismi e sono uno l'inverso dell'altro, quindi sono isomorfismi. \square

Definizione 1.1.10. Sia R un anello. Un elemento $e \in R$ si dice *idempotente* se $e^2 = e$.

Osservazione 1.1.11. Se e è un idempotente di R , ovviamente Re ed eR sono rispettivamente un ideale sinistro e destro di R e si vede facilmente che

$eRe \subset Re \cap eR$ è un anello a sua volta, con elemento neutro e . E' contenuto in R ma non è un suo sottoanello, a meno che $e = 1$.

Lemma 1.1.12. *Sia R un anello, $e \in R$ un idempotente e sia $L_x : R \rightarrow R$ la moltiplicazione a sinistra definita da $L_x(r) = xr$. Allora c'è un isomorfismo di anelli*

$$L : eRe \rightarrow \text{End}_R(eR) \quad eae \mapsto L_{eae}$$

Dimostrazione. L è chiaramente un isomorfismo di anelli, infatti sia $eae \in eRe$ e sia $re \in eR$, allora

$$L_{eae+ebe}(er) = (eae + ebe)er = eaeer + ebeer = L_{eae}(er) + L_{ebe}(er),$$

$$L_e(er) = eer = er,$$

$$L_{eaeebe}er = eaebeer = L_{eae}L_{ebe}r.$$

L è iniettivo perchè se $L_{eae} = 0$, cioè $eaeer = 0$ per ogni $r \in R$, allora prendendo $r = e$ abbiamo $eaeer = eae = 0$, ma è anche suriettivo perchè se $f \in \text{End}_R(eR)$, allora abbiamo che $f(e) = ea$ per un certo $a \in R$ e abbiamo che

$$f(er) = f(eer) = f(e)er = eaer = eaeer = L_{eae}(er) \quad \text{per ogni } r \in R.$$

□

Teorema 1.1.13 (Wedderburn). *Sia A un anello semplice. Allora esiste un unico anello di divisione D (a meno di isomorfismo) ed un unico $n \in \mathbb{N}$ tale che $A \simeq M_n(D)$.*

Dimostrazione. Innanzitutto dimostriamo l'esistenza. Scegliamo un idempotente $0 \neq e \in A$ (ad esempio 1), sia I un qualunque ideale minimale di A (sappiamo già che sono tutti isomorfi tra loro) e sia $D = \text{End}_A(I)$ (per il Lemma di Schur è un anello di divisione), allora, usando il lemma appena dimostrato, insieme all'osservazione che segue il teorema 1.1.7 e al teorema 1.1.9 si ha:

$$eAe \simeq \text{End}_A(eA) \simeq \text{End}_A \left(\bigoplus_{i=1}^n I \right) \simeq M_n(D).$$

Per vedere l'unicità, mostriamo che $M_n(D) \simeq M_m(E)$ con D ed E anelli di divisione, implica $m = n$ e $D \simeq E$.

Consideriamo l'idempotente $0 \neq E_{11} \in M_n(D)$, un calcolo semplice mostra che $E_{11}M_n(D)E_{11} \simeq D$ e ne deduciamo che $E_{11}M_n(D)$ è un ideale minimale di $M_n(D)$.

Infatti, se così non fosse, dal momento che $M_n(D)$ è un anello semplice, avremmo $E_{11}M_n(D) \simeq \bigoplus_{i=1}^k I$ con I ideale minimale di $M_n(D)$ e $k \geq 2$, da cui usando 1.1.7 e 1.1.9 si avrebbe

$$\begin{aligned} D &\simeq E_{11}M_n(D)E_{11} \\ &\simeq \text{End}(E_{11}M_n(D)) \\ &\simeq \text{End}\left(\bigoplus_{i=1}^k I\right) \\ &\simeq M_k(\text{End}(I)) \end{aligned}$$

con $k \geq 2$, che è impossibile (ad esempio perché D non ha zero-divisori). Allo stesso modo $E_{11}M_m(E)$ è un ideale minimale di $M_m(E)$, quindi per il fatto che $M_n(D) \simeq M_m(E)$ si ha

$$D \simeq \text{End}(E_{11}M_n(D)) \simeq \text{End}(E_{11}M_m(E)) \simeq E.$$

Ne segue poi che $n = m$ per motivi di dimensione. □

Osservazione 1.1.14. Se $A \simeq M_n(D)$ è un anello semplice, avremo allora che il centro di A è il centro di D , cioè è un campo e A è un'algebra su tale campo. Si può quindi anche dire che A è un'algebra semplice.

Osservazione 1.1.15. Abbiamo visto nella dimostrazione di 1.1.13 che un ideale minimale di $A \simeq M_n(D)$ è $E_{11}M_n(D)$; per 1.1.8 sappiamo che sono tutti isomorfi tra loro. Per un qualunque ideale minimale I di A abbiamo allora

$$[I : D] = n.$$

1.2 Prodotto Tensoriale

Il prodotto tensoriale è una costruzione algebrica molto naturale: è ciò che si fa moltiplicando un vettore colonna per un vettore riga per ottenere una matrice, ma per adesso non limitiamoci al caso degli spazi vettoriali e vediamo la costruzione generale.

Definizione 1.2.1. Sia R un anello; siano M ed N rispettivamente un modulo destro ed un modulo sinistro su R e sia P un gruppo abeliano, scritto additivamente. $f : M \times N \rightarrow P$ è una *mappa bilanciata* se f è \mathbb{Z} -bilineare e

$$f(m, rn) = f(mr, n) \quad \text{per ogni } r \in R, m \in M, n \in N.$$

Definizione 1.2.2. Siano $f : M \times N \rightarrow P$ e $\varphi : M \times N \rightarrow T$ due mappe bilanciate di $M \times N$ nei gruppi abeliani additivi P e T . Diciamo che f può essere *fattorizzata* attraverso T se esiste un omomorfismo $f^* : T \rightarrow P$ tale che $f = f^* \varphi$.

Teorema 1.2.3. *Siano R , M ed N come sopra, allora esiste un gruppo abeliano T e una mappa bilanciata $t : M \times N \rightarrow T$ tale che*

$$(i) \text{ per ogni } x \in T, x = \sum t(m_i, n_i) \text{ con } m_i \in M \text{ e } n_i \in N,$$

(ii) ogni mappa bilanciata da $M \times N$ in un qualunque gruppo abeliano P si può fattorizzare in modo unico attraverso T .

Inoltre, la coppia (T, t) è unica a meno di isomorfismo, cioè se anche (T', t') verificano (i) e (ii), esiste $\lambda : T \rightarrow T'$ isomorfismo di gruppi e $t' = \lambda t$.

Dimostrazione. Cominciando definendo F come lo \mathbb{Z} -modulo libero che ha come base gli elementi di $M \times N$, in modo che F sia il gruppo abeliano additivo che consiste di tutte le somme formali finite

$$\sum z_{ij}(m_i, n_j), \quad z_{ij} \in \mathbb{Z} \quad m_i \in M \quad n_j \in N.$$

Ora, sia H il sottogruppo di F generato dalle somme formali

$$\begin{cases} (m_1 + m_2, n) - (m_1, n) - (m_2, n), \\ (m, n_1 + n_2) - (m, n_1) - (m, n_2), \\ (m, rn) - (mr, n) \end{cases} \quad (1.2)$$

per tutti gli $m_i \in M$, $n_i \in N$ e $r \in R$. Sia T il gruppo quoziente F/H e definiamo

$$t : M \times N \rightarrow T$$

tramite

$$t(m, n) = (m, n) + H.$$

Visto che tutte le somme indicate in (1.2) stanno in H , si ha immediatamente che t è \mathbb{Z} -bilineare e che

$$t(m, rn) - t(mr, n) = 0 \quad \text{per ogni } m \in M, n \in N, r \in R. \quad (1.3)$$

che mostra che t è una mappa bilanciata. Dal fatto che ogni elemento di F è combinazione \mathbb{Z} -lineare di coppie ordinate, ne segue che possiamo scrivere ogni elemento di T come

$$\sum z_i t(m_i, n_i) \quad \text{con } m_i \in M, n_i \in N \text{ e } z_i \in \mathbb{Z}.$$

Da qui, per ottenere (i) basta osservare che la \mathbb{Z} -bilinearità di t e (1.3) implicano che

$$t(zm, n) = t(m, zn) = zt(m, n) \quad \text{per ogni } m \in M, n \in N \text{ e } z \in \mathbb{Z}.$$

Ora, sia $\varphi : M \times N \rightarrow P$ una qualunque mappa bilanciata. Visto che gli elementi (m, n) formano una \mathbb{Z} base di F , possiamo definire un omomorfismo φ' di F in P tramite

$$\varphi' \left(\sum z_{ij} (m_i, n_j) \right) = \sum z_{ij} \varphi(m_i, n_j).$$

Osserviamo che $\varphi'(H) = 0$ perchè φ è bilanciata, quindi φ' induce un omomorfismo φ^* dal quoziente $F/H = T$ in P tale che

$$\varphi^*((m, n) + H) = \varphi(m, n) \quad \text{per ogni } (m, n) \in M \times N$$

Possiamo quindi fattorizzare φ attraverso T , infatti

$$\varphi(m, n) = \varphi^*((m, n) + H) = \varphi^*(t(m, n)).$$

Con questo abbiamo concluso l'esistenza, passiamo ora all'unicità. Supponiamo che T' sia un gruppo abeliano e t' sia una mappa bilanciata che verificano (i) e (ii), allora possiamo fattorizzare t attraverso T' e t' attraverso T . Otteniamo dunque due omomorfismi $\lambda : T \rightarrow T'$ e $\mu : T' \rightarrow T$ tali che

$$\lambda(t(m, n)) = t'(m, n) \quad \text{e}$$

$$\mu(t'(m, n)) = t(m, n) \quad \text{per ogni } (m, n) \in M \times N.$$

Poiché gli elementi $\{t(m, n)\}$ e $\{t'(m, n)\}$ generano rispettivamente i gruppi T e T' , ne segue che $\lambda\mu$ e $\mu\lambda$ sono l'identità su T e T' , quindi λ e μ sono isomorfismi. \square

Definizione 1.2.4. Il gruppo T che abbiamo appena costruito si chiama il *prodotto tensoriale* di M ed N su R e si indica $M \otimes_R N$. L'immagine di (m, n) tramite la mappa bilanciata $M \times N \rightarrow M \otimes_R N$ si indica con $m \otimes n$.

Dal teorema 1.2.3, si vede che il prodotto $m \otimes n$ è \mathbb{Z} -bilineare e che

$$mr \otimes n = m \otimes rn, \text{ per ogni } m \in M, n \in N \text{ e } r \in R.$$

Osservazione 1.2.5. Ogni mappa bilanciata $f : M \times N \rightarrow P$ può essere fattorizzata in un solo modo attraverso $M \otimes_R N$ perché se $f(m, n) = f^*(m \otimes n)$, il fatto che ogni elemento di $M \otimes_R N$ si può esprimere come $\sum m_i \otimes n_i$ ci dice che in realtà f^* è determinata univocamente da f .

Proposizione 1.2.6. Siano M ed M' R -moduli destri, N ed N' R -moduli sinistri e siano $f : M \rightarrow M'$ e $g : N \rightarrow N'$ degli R -omomorfismi. Allora esiste un unico omomorfismo $f \otimes g : M \otimes_R N \rightarrow M' \otimes N'$ tale che

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

Dimostrazione. La mappa $(m, n) \mapsto f(m) \otimes g(n)$ è bilanciata perché f e g sono R -omomorfismi, quindi per il teorema 1.2.3 esiste $f \otimes g$, l'unicità segue dall'osservazione appena fatta. \square

Osservazione 1.2.7. Se f e g sono come sopra e se $f' : M' \rightarrow M''$ e $g' : N' \rightarrow N''$ sono R -omomorfismi, usando due volte la proposizione appena vista, si ha che

$$(f' \otimes g')(f \otimes g) = f'f \otimes g'g.$$

Proposizione 1.2.8. Siano M_1 ed M_2 R -moduli destri e N un R -modulo sinistro, allora

$$(M_1 \oplus M_2) \otimes_R N \simeq (M_1 \otimes_R N) \oplus (M_2 \otimes_R N).$$

Dimostrazione. Consideriamo la mappa da $(M_1 \oplus M_2) \times N$ in $(M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$ data da

$$(m_1 + m_2, n) \mapsto m_1 \otimes n + m_2 \otimes n \quad m_i \in M, n \in N.$$

E' una mappa bilanciata, quindi per 1.2.3 induce un omomorfismo $f : (M_1 \oplus M_2) \otimes_R N \rightarrow (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$ tale che

$$f((m_1 + m_2) \otimes n) = m_1 \otimes n + m_2 \otimes n.$$

Ora, consideriamo per $j = 1, 2$ le mappe $g'_j : M_j \times N \rightarrow (M_1 \oplus M_2) \otimes_R N$ date da

$$g'_j(m_j, n) = i_j(m_j) \otimes n \quad m_j \in M_j, n \in N,$$

dove $i_j : M_j \rightarrow M_1 \oplus M_2$ è l'iniezione canonica nell' i -esima componente. le g'_j sono mappe bilanciate, quindi per 1.2.3 esistono $g_j : M_j \otimes_R N \rightarrow (M_1 \oplus M_2) \otimes_R N$ con

$$g_j(m_j \otimes n) = i_j(m_j) \otimes n \quad m_j \in M_j, n \in N.$$

Siano ora $\pi_j : (M_1 \otimes_R N) \oplus (M_2 \otimes_R N) \rightarrow M_j \otimes_R N$ le proiezioni sulle componenti j -esime, abbiamo la mappa $g : (M_1 \otimes_R N) \oplus (M_2 \otimes_R N) \rightarrow (M_1 \oplus M_2) \otimes_R N$, data da

$$g = g_1\pi_1 + g_2\pi_2.$$

Ora,

$$\begin{aligned}
 g(f((m_1 + m_2) \otimes n)) &= (g_1\pi_1 + g_2\pi_2)(m_1 \otimes n + m_2 \otimes n) \\
 &= g_1\pi_1(m_1 \otimes n + m_2 \otimes n) + g_2\pi_2(m_1 \otimes n + m_2 \otimes n) \\
 &= g_1(m_1 \otimes n) + g_2(m_2 \otimes n) \\
 &= i_1(m_1) \otimes n + i_2(m_2) \otimes n \\
 &= (i_1(m_1) + i_2(m_2)) \otimes n \\
 &= (m_1 + m_2) \otimes n.
 \end{aligned}$$

Viceversa,

$$\begin{aligned}
 f(g(m_1 \otimes n + m_2 \otimes n)) &= f(i_1(m_1) \otimes n + i_2(m_2) \otimes n) \\
 &= f((m_1 + m_2) \otimes n) \\
 &= m_1 \otimes n + m_2 \otimes n.
 \end{aligned}$$

Quindi f e g , essendo uno l'inverso dell'altro, sono isomorfismi. □

Chiaramente questo risultato implica anche la generalizzazione alla somma diretta finita di moduli.

Fino ad adesso abbiamo dato al prodotto tensoriale solamente la struttura di gruppo abeliano, ma possiamo spingerci più in là: vediamo per esempio in quali casi $M \otimes_R N$ è un modulo.

Definizione 1.2.9. Diciamo che un gruppo abeliano M è un (S, R) -bimodulo sugli anelli R ed S , se M è un S -modulo sinistro ed un R -modulo destro e si ha:

$$(sm)r = s(mr) \quad \text{per ogni } s \in S, m \in M, r \in R.$$

Per esempio se R è un anello commutativo, un R -modulo sinistro M è un (R, R) -bimodulo se definiamo $mr = rm$, $m \in M$, $r \in R$.

Proposizione 1.2.10. Sia M è un (S, R) -bimodulo e sia N è un R -modulo sinistro. Esiste un'unica struttura di S -modulo sinistro su $M \otimes_R N$ tale che $s(m \otimes n) = (sm) \otimes n$.

Dimostrazione. Fissiamo $s \in S$ e consideriamo la mappa $(m, n) \mapsto sm \otimes n$ da $M \times N$ in $M \otimes_R N$. E' una mappa bilanciata, quindi per il teorema 1.2.3 esiste ψ_s endomorfismo di $M \otimes_R N$ tale che $\psi_s(m \otimes n) = sm \otimes n$. Definiamo allora $\forall s \in S$

$$s \left(\sum m_i \otimes n_i \right) = \psi_s \left(\sum m_i \otimes n_i \right) = \sum sm_i \otimes n_i.$$

Si vede chiaramente che $M \otimes_R N$ è un modulo rispetto a questa operazione. \square

Analogamente, se M è un S -modulo destro e N è un (S, R) -bimodulo, $M \otimes_S N$ sarà un R -modulo destro.

Con le ipotesi di quest'ultima proposizione, si generalizza facilmente l'isomorfismo in 1.2.8 ad un isomorfismo di moduli.

Se N è un R -modulo sinistro, dal momento che R è evidentemente un (R, R) -bimodulo, abbiamo che $R \otimes_R N$ è un R -modulo sinistro.

Proposizione 1.2.11. $R \otimes_R N \simeq N$ come R -moduli sinistri.

Dimostrazione. La mappa $(r, n) \mapsto rn$ è una mappa bilanciata da $R \times N$ in N , quindi per 1.2.3 esiste un omomorfismo $\varphi : R \otimes_R N \rightarrow N$ tale che

$$\varphi(r \otimes n) = rn.$$

D'altra parte, possiamo definire un omomorfismo $\psi : N \rightarrow R \otimes_R N$ tramite

$$\psi(n) = 1 \otimes n \quad n \in N.$$

Chiaramente $\varphi\psi$ è l'identità su N , inoltre

$$\psi(\varphi(r \otimes n)) = \psi(rn) = 1 \otimes rn = r \otimes n,$$

quindi $\psi\varphi$ è l'identità su $R \otimes_R N$. Ciò significa che φ è un isomorfismo di gruppi e si vede facilmente che è anche un R -omomorfismo. \square

Allo stesso modo, con N modulo destro, $N \otimes_R R \simeq N$ come R -modulo destro.

Osservazione 1.2.12. Se R è commutativo, non c'è differenza tra moduli destri e sinistri, quindi, se M ed N sono entrambi R -moduli, sono anche (R, R) -bimoduli ed esistono sia $M \otimes_R N$ che $N \otimes_R M$ e sono chiaramente isomorfi.

Teorema 1.2.13 (Associatività del Prodotto Tensoriale). *Sia L un R -modulo destro, sia M un (R, S) -bimodulo e sia N un S -modulo sinistro, dove R ed S sono anelli. Allora $L \otimes_R M$ è un S -modulo destro, $M \otimes_S N$ è un R -modulo sinistro e*

$$(L \otimes_R M) \otimes_S N \simeq L \otimes_R (M \otimes_S N).$$

Dimostrazione. Abbiamo già visto che $L \otimes_R M$ è un S -modulo destro e $M \otimes_S N$ è un R -modulo sinistro, sono quindi ben definiti $(L \otimes_R M) \otimes_S N$ e $L \otimes_R (M \otimes_S N)$. Ora, fissiamo $n \in N$ e consideriamo $\lambda_n : L \times N \rightarrow L \otimes_R (M \otimes_S N)$ definita da

$$(l, m) \mapsto l \otimes (m \otimes n) \quad l \in L, m \in M.$$

Questa è R -bilanciata, quindi per 1.2.3 induce un'unica mappa da $L \otimes_R M$ in $L \otimes_R (M \otimes_S N)$ con

$$l \otimes m \mapsto l \otimes (m \otimes n) \quad l \in L, m \in M.$$

Possiamo allora definire $\lambda : (L \otimes_R M) \times N \rightarrow L \otimes_R (M \otimes_S N)$ tramite

$$(l \otimes m, n) \mapsto l \otimes (m \otimes n) \quad l \in L, m \in M, n \in N.$$

λ è S -bilanciata, quindi per 1.2.3 esiste un'unica $\lambda' : (L \otimes_R M) \otimes_S N \rightarrow L \otimes_R (M \otimes_S N)$ con

$$\lambda'((l \otimes m) \otimes n) = l \otimes (m \otimes n) \quad l \in L, m \in M, n \in N.$$

Analogamente possiamo fare la stessa costruzione partendo da un $l \in L$ fissato e ottenere la mappa

$$m \otimes n \mapsto (l \otimes m) \otimes n,$$

quindi

$$(l, m \otimes n) \mapsto (l \otimes m) \otimes n,$$

per arrivare infine a $\mu' : L \otimes_R (M \otimes_S N) \rightarrow (L \otimes_R M) \otimes_S N$ con

$$\mu'(l \otimes (m \otimes n)) = (l \otimes m) \otimes n.$$

Abbiamo così costruito due omomorfismi λ' e μ' che sono l'uno l'inverso dell'altro e quindi sono isomorfismi. \square

1.2.1 Prodotto tensoriale di spazi vettoriali e di algebre

Vediamo ora il caso degli spazi vettoriali: siano M e N spazi vettoriali di dimensione rispettivamente m ed n su un campo F . Allora per 1.2.10, $M \otimes_F N$ è un F -modulo, cioè è ancora uno spazio vettoriale su F , e, usando 1.2.8 e 1.2.11 si vede che

$$M \otimes_F N \simeq \left(\bigoplus_1^m F \right) \otimes_F N \simeq \bigoplus_1^m F \otimes_F N \simeq \bigoplus_1^m N$$

come F -spazi, quindi $[M \otimes_F N : F] = mn = [M : F][N : F]$. Ora supponiamo che

$$M = Fv_1 \oplus \cdots \oplus Fv_m, \quad N = Fu_1 \oplus \cdots \oplus Fu_n$$

e che $x \otimes y \in M \otimes_F N$, allora

$$x \otimes y = \left(\sum_{i=1}^m x_i v_i \right) \otimes \left(\sum_{j=1}^n y_j u_j \right) = \sum_{i,j} \alpha_{ij} (v_i \otimes u_j) \quad \alpha_{ij} \in F$$

quindi, visto che ogni elemento di $M \otimes_F N$ può essere scritto come somma di elementi del tipo $x \otimes y$, si ha che gli $\{(v_i \otimes u_j)\}_{i,j}$ generano $M \otimes_F N$, di conseguenza ne sono una base poichè sono esattamente mn .

Da questo si deduce anche che se $m \neq 0_M$ e $n \neq 0_N$, allora $m \otimes n \neq 0$ in $M \otimes_F N$. Infatti possiamo scegliere delle basi di M e di N in modo che m ed n siano elementi delle rispettive basi, quindi $m \otimes n$ sarà un elemento di una base di $M \otimes_F N$ e perciò non nullo.

Aggiungiamo ancora un po' di struttura e passiamo al caso delle algebre.

Teorema 1.2.14. *Siano A e B due algebre su un campo F , allora $A \otimes_F B$ è ancora un'algebra su F se definiamo il prodotto come*

$$\left(\sum_i a_i \otimes b_i \right) \left(\sum_l a'_l \otimes b'_l \right) = \sum_{i,l} a_i a'_l \otimes b_i b'_l.$$

Dimostrazione. Innanzitutto dimostriamo che la moltiplicazione è ben definita, per fare ciò ci basta vedere che se $\sum_i a_i \otimes b_i = 0$ allora

$$\left(\sum_i a_i \otimes b_i \right) \left(\sum_j a'_j \otimes b'_j \right) = 0 \quad \text{per ogni } a'_i \in A, b'_j \in B.$$

Prendiamo $\{u_j\}_{j=1}^m$ base di A e $\{v_k\}_{k=1}^n$ base di B , allora

$$\begin{aligned} 0 &= \sum_i a_i \otimes b_i \\ &= \sum_i \left(\sum_j \alpha_{ij} u_j \right) \otimes \left(\sum_k \beta_{ik} v_k \right) \\ &= \sum_{i,j,k} \alpha_{ij} \beta_{ik} u_j \otimes v_k, \end{aligned}$$

quindi, visto che $(u_j \otimes v_k)$ sono una base, tutte le componenti devono essere nulle, cioè

$$\sum_i \alpha_{ij} \beta_{ik} = 0 \quad \text{per ogni } (j, k).$$

Allora

$$\begin{aligned} \sum_{i,l} a_i a'_l \otimes b_i b'_l &= \sum_{i,j,k,l} \alpha_{ij} \beta_{ik} u_j a'_l \otimes v_k b'_l \\ &= \sum_{j,k,l} \left(\sum_i \alpha_{ij} \beta_{ik} \right) u_j a'_l \otimes v_k b'_l \\ &= 0. \end{aligned}$$

Ora, avendo visto che la moltiplicazione è ben definita, è chiaro che $A \otimes_F B$ è un'algebra su F , con elemento neutro $1_A \otimes 1_B$. I sottoinsiemi $A \otimes 1_B$ e $1_A \otimes B$ sono sottoalgebre di $A \otimes_F B$ isomorfe rispettivamente ad A e B , gli elementi dell'una commutano con quelli dell'altra e i loro prodotti generano $A \otimes_F B$ su F . \square

Proposizione 1.2.15. *Siano A e B due F -algebre, in più richiediamo che B sia commutativa. Allora $A \otimes_F B$ è una B -algebra.*

Dimostrazione. Sappiamo già che $A \otimes_F B$ è una F -algebra, che contiene una sottoalgebra isomorfa a B . Per avere il risultato ci basta osservare che, dal momento che B è commutativa, per ogni $b \in B$ si ha:

$$\begin{aligned} (1 \otimes b) \left(\sum a_i \otimes b_i \right) \left(\sum a'_i \otimes b'_i \right) &= \left(\sum a_i \otimes bb_i \right) \left(\sum a'_i \otimes b'_i \right) \\ &= \left(\sum a_i \otimes b_i b \right) \left(\sum a'_i \otimes b'_i \right) \\ &= \left(\sum a_i \otimes b_i \right) (1 \otimes b) \left(\sum a'_i \otimes b'_i \right) \\ &= \left(\sum a_i \otimes b_i \right) \left(\sum a'_i \otimes bb'_i \right). \end{aligned}$$

□

Proposizione 1.2.16. *Siano A e B due F -algebre, B commutativa, e sia C una B -algebra commutativa, allora c'è un isomorfismo di C algebre*

$$(A \otimes_F B) \otimes_B C \simeq A \otimes_F C.$$

Dimostrazione. Per 1.2.13 e 1.2.11, sappiamo che esistono gli isomorfismi di gruppi

$$(A \otimes_F B) \otimes_B C \simeq A \otimes_F (B \otimes_B C) \simeq A \otimes_F C$$

tali che

$$(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c) \mapsto a \otimes bc,$$

vogliamo quindi vedere che $f : (A \otimes_F B) \otimes_B C \rightarrow A \otimes_F C$ dato da

$$f((a \otimes b) \otimes c) = a \otimes bc$$

è anche un isomorfismo di C -algebre. Sicuramente f è C -lineare, resta da

vedere come si comporta per il prodotto. Per questo basta osservare che

$$\begin{aligned}
f(((a \otimes b) \otimes c)((a' \otimes b') \otimes c')) &= f((a \otimes b)(a' \otimes b') \otimes cc') \\
&= f((aa' \otimes bb') \otimes cc') \\
&= aa' \otimes bb'cc' \\
&= aa' \otimes bcb'c' \\
&= (a \otimes bc)(a' \otimes b'c') \\
&= f((a \otimes b) \otimes c)f((a' \otimes b') \otimes c').
\end{aligned}$$

□

Teorema 1.2.17. *Siano A e B due F -algebre, B commutativa, sia C una B -algebra, non necessariamente commutativa. Supponiamo che esista un omomorfismo di F -algebre, $f : A \rightarrow C$. Allora esiste un unico omomorfismo di B -algebre (detto l'estensione sinistra B -lineare di f), $f_B : A \otimes_F B \rightarrow C$, tale che*

$$f(a \otimes b) = bf(a).$$

Dimostrazione. Consideriamo la mappa $g : A \times B \rightarrow C$ data da

$$g(a, b) = bf(a),$$

questa è F -bilanciata, quindi esiste un omomorfismo di gruppi $f_B : A \otimes_F B \rightarrow C$ tale che

$$f_B(a \otimes b) = bf(a).$$

f_B è chiaramente B -lineare, per concludere verichiamo che rispetti il prodotto:

$$\begin{aligned}
f_B((a \otimes b)(a' \otimes b')) &= f_B(aa' \otimes bb') \\
&= bb'f(aa') \\
&= bb'f(a)f(a') \\
&= bf(a)b'f(a') \\
&= f_B(a \otimes b)f_B(a' \otimes b').
\end{aligned}$$

□

Questo teorema ha una conseguenza molto importante:

Proposizione 1.2.18. *Sia A una F -algebra, e $j : M_n(F) \rightarrow M_n(A)$ l'iniezione indotta dall'iniezione canonica $\iota : F \rightarrow A$ con $\iota(k) = k1$. Allora l'estensione sinistra A -lineare*

$$j_A : M_n(F) \otimes_F A \rightarrow M_n(A)$$

è un isomorfismo di A -algebre.

Dimostrazione. Per il teorema 1.2.17 abbiamo l'omomorfismo di B -algebre $j_A : M_n(F) \otimes_F A \rightarrow M_n(A)$ con

$$j_A(M \otimes a) = aj(M),$$

ma $M_n(F)$ è un F -modulo libero con base $\{E_{ij}\}$, quindi $M_n(F) \otimes_F A$ è un A -modulo libero con base $\{E_{ij} \otimes 1\}$, la quale viene inviata tramite j_A nella base $\{E_{ij}\}$ di $M_n(A)$. Allora j_A è un isomorfismo. \square

Osservazione 1.2.19. $M_n(F) \otimes_F M_m(F) \simeq M_n(M_m(F)) \simeq M_{nm}(F)$.

1.3 Gruppo di Brauer

Definizione 1.3.1. Un'algebra A si dice *centrale semplice* su un campo F se A è un'algebra semplice che ha F come suo centro.

Proposizione 1.3.2. Se A è un'algebra centrale semplice sul campo F e B è un'algebra semplice il cui centro contiene F , allora $A \otimes_F B$ è semplice.

Dimostrazione. Sicuramente $A \otimes_F B$ è artiniana, perché è di dimensione finita su F . Sia ora $U \neq 0$ un ideale di $A \otimes_F B$, e sia $0 \neq u \in U$. Scriviamo $u = \sum a_i \otimes b_i$ dove $a_i \in A$ e $b_i \in B$ scegliendo i b_i in modo che siano linearmente indipendenti su F e chiamiamo il numero di a_i non nulli di questa espressione, la *lunghezza* di u . Scegliamo $u \in U$ di lunghezza minima. Se $r, s \in A$, allora $(r \otimes 1)u(s \otimes 1) = \sum r a_i s \otimes b_i \in U$. Ora, $A a_i A$ è un ideale bilatero di A non nullo, quindi coincide con A , perché A è semplice. Allora esistono $r_j, s_j \in A$ tali che $\sum_j r_j a_1 s_j = 1$ e $\sum_j r_j a_i s_j \neq 0$ per $a_i \neq 0$, quindi

$$\begin{aligned} U \ni u_1 &:= \sum_j (r_j \otimes 1)u(s_j \otimes 1) \\ &= \sum_i \left(\sum_j r_j a_i s_j \otimes b_i \right) \\ &= 1 \otimes b_1 + a'_2 \otimes b_2 + \cdots + a'_m \otimes b_m, \end{aligned}$$

dove m è la lunghezza di u e quindi anche di u_1 . Dato $a \in A$, si ha

$$\begin{aligned} U \ni (a \otimes 1)u_1 - u_1(a \otimes 1) &= (a \otimes b_1 + a a'_2 \otimes b_2 + \cdots + a a'_m \otimes b_m) \\ &\quad - (a \otimes b_1 + a'_2 a \otimes b_2 + \cdots + a'_m a \otimes b_m) \\ &= (a a'_2 - a'_2 a) \otimes b_2 + \cdots + (a a'_m - a'_m a \otimes b_m). \end{aligned}$$

Ma questo è un elemento di U di lunghezza minore di u , quindi dev'essere nullo. Visto che i b_i sono linearmente indipendenti su F , $1 \otimes b_i$ sono linearmente indipendenti su A , quindi

$$(a a'_2 - a'_2 a) \otimes b_2 + \cdots + (a a'_m - a'_m a \otimes b_m) = 0$$

implica $(aa'_i - a'_i a) = 0$ per ogni $i = 2, \dots, m$; cioè $aa'_i = a'_i a$ per ogni $i = 2, \dots, m$ e per ogni $a \in A$.

Quindi $a'_i \in F$ per ogni $i = 1, \dots, m$ e possiamo scrivere

$$\begin{aligned} u_1 &= 1 \otimes b_1 + a'_2 \otimes b_2 + \dots + a'_m \otimes b_m \\ &= 1 \otimes b_1 + 1 \otimes a'_2 b_2 + \dots + 1 \otimes a'_m b_m \\ &= 1 \otimes (b_1 + a'_2 b_2 + \dots + a'_m b_m). \end{aligned}$$

Dal momento che i b_i sono indipendenti su F ,

$$b = b_1 + a'_2 b_2 + \dots + a'_m b_m \neq 0,$$

da cui

$$U \supset (1 \otimes B)u_1(1 \otimes B) = 1 \otimes BbB = 1 \otimes B$$

per la semplicità di B . Da questo si ottiene che

$$U \supset (A \otimes 1)(1 \otimes B) = A \otimes_F B$$

quindi $U = A \otimes_F B$, che è quindi un'algebra semplice. \square

Teorema 1.3.3. *Se A e B sono algebre centrali semplici sul campo F , allora $A \otimes_F B$ è centrale semplice su F .*

Dimostrazione. Per la proposizione precedente, sappiamo già che $A \otimes_F B$ è semplice, vogliamo allora far vedere che il suo centro è F . Chiaramente F , inteso come $F(1 \otimes 1)$, è contenuto nel centro di $A \otimes_F B$ vogliamo vedere l'inclusione inversa. Supponiamo che $z = \sum a_i \otimes b_i$ sia nel centro di $A \otimes_F B$ e supponiamo ancora che i b_i siano linearmente indipendenti su F . Dato $a \in A$,

$$0 = (a \otimes 1)z - z(a \otimes 1) = \sum (aa_i - a_i a) \otimes b_i$$

da cui $aa_i - a_i a = 0$ e quindi $a_i \in F$ per ogni i . Scriviamo allora

$$z = \sum a_i \otimes b_i = 1 \otimes \sum a_i b_i = 1 \otimes b$$

Ora, se prendiamo $x \in B$

$$\begin{aligned} 0 &= (1 \otimes x)z - z(1 \otimes x) \\ &= (1 \otimes xb) - (1 \otimes bx) \\ &= (1 \otimes xb - bx) \end{aligned}$$

da cui $xb - bx = 0$ per ogni $x \in B$, quindi $b \in F$. Con questo abbiamo concluso perché allora

$$z = 1 \otimes b = b(1 \otimes 1) \in F(1 \otimes 1).$$

□

Lemma 1.3.4. *Sia D un'algebra di divisione su un campo algebricamente chiuso F . Allora $D = F$.*

Dimostrazione. Per ogni $d \in D$, possiamo considerare il campo $F(d) \subset D$ generato da d e F . Allora $[F(d) : F] \leq [D : F]$, quindi $F(d)/F$ è un'estensione algebrica, in quanto finita, di F . Ne segue che $F(d) = F$ da cui $d \in F$ per ogni $d \in D$, cioè $D = F$. □

Proposizione 1.3.5. *Sia A un'algebra centrale semplice su F , allora $[A : F]$ è un quadrato perfetto.*

Dimostrazione. Per il teorema di Wedderburn (1.1.13) abbiamo che $A \simeq M_m(D)$ con D algebra di divisione centrale su F . Sia \bar{F} la chiusura algebrica di F , allora $\bar{D} = D \otimes_F \bar{F}$ è semplice per 1.3.2; inoltre $[D : F] = [\bar{D} : \bar{F}]$. Ora, sempre per il teorema di Wedderburn, abbiamo che \bar{D} , essendo un'algebra semplice che contiene \bar{F} nel suo centro, è isomorfa ad una qualche algebra di matrici $M_n(L)$, con L algebra di divisione su \bar{F} . Quindi, per il lemma 1.3.4, abbiamo che $L = \bar{F}$, cioè $\bar{D} \simeq M_n(\bar{F})$. Ne ricaviamo che

$$[D : F] = [\bar{D} : \bar{F}] = [M_n(\bar{F}) : \bar{F}] = n^2.$$

In conclusione, si ha

$$[A : F] = [M_m(D) : F] = m^2[D : F] = m^2n^2 = (mn)^2.$$

□

Definizione 1.3.6. Dato un anello qualunque A , definiamo A^{op} l'*anello opposto* il cui gruppo additivo è quello di A , e il prodotto è definito così:

$$a \cdot b = ba$$

dove ba è il normale prodotto in A .

Sono evidenti le seguenti proprietà:

1. $A^{op} = A$ se e solo se A è commutativo,
2. $(A^{op})^{op} = A$,
3. A^{op} è anti-isomorfo ad A ,
4. $I \subset A$ è un ideale sinistro di A se e solo se I è un ideale destro di A^{op} ,
5. A è semplice se e solo se A^{op} lo è,
6. A è una F -algebra se e solo se A^{op} lo è.

Teorema 1.3.7. *Sia A un'algebra centrale semplice su F , e sia $n = [A : F]$, allora*

$$A \otimes_F A^{op} \simeq M_n(F).$$

Dimostrazione. L'anello $\text{End}_F(A)$ delle trasformazioni F -lineari di A come spazio vettoriale è chiaramente isomorfo a $M_n(F)$. Ora, per $a \in A$, sia $R_a : A \rightarrow A$ la moltiplicazione a destra $R_a(x) = xa$, e sia $L_a : A \rightarrow A$ la moltiplicazione a sinistra $L_a(x) = ax$.

Definiamo $A_r := \{R_a | a \in A\} \subset \text{End}_F(A)$ e $A_l := \{L_a | a \in A\} \subset \text{End}_F(A)$, se scriviamo la moltiplicazione in $\text{End}_F(A)$ come $(f \circ g)(x) = f(g(x))$ è evidente che $A_l \simeq A$ e $A_r \simeq A^{op}$. Notiamo che ogni elemento di A_l commuta con ogni elemento di A_r . Ora, per quanto appena affermato, abbiamo $A \otimes_F A^{op} \simeq A_l \otimes_F A_r$ che è centrale semplice su F perché A_l e A_r lo sono. Definiamo una mappa da $A_l \times A_r$ in $A_l A_r \subset \text{End}_F(A)$ tramite

$$(L_a, R_b) \mapsto L_a R_b.$$

Questa mappa è F -bilanciata, quindi esiste un omomorfismo di gruppi $g : A_l \otimes_F A_r \rightarrow L(A)$ con

$$g(L_a \otimes R_b) = L_a R_b$$

che è suriettivo e dalle proprietà di commutatività è anche un omomorfismo di anelli, infatti

$$\begin{aligned} g((L_a \otimes R_b)(L_{a'} \otimes R_{b'})) &= g(L_a L_{a'} \otimes R_b R_{b'}) \\ &= L_a L_{a'} R_b R_{b'} \\ &= L_a R_b L_{a'} R_{b'} \\ &= g(L_a \otimes R_b)g(L_{a'} \otimes R_{b'}). \end{aligned}$$

g deve essere iniettivo perché $A_l \otimes_F A_r$ è semplice, quindi è un isomorfismo, cioè abbiamo

$$A \otimes_F A^{op} \simeq A_l \otimes_F A_r \simeq A_l A_r \subset \text{End}_F(A).$$

Ora,

$$\begin{aligned} n^2 &= [\text{End}_F(A) : F] \\ &\geq [A_l A_r : F] \\ &= [A \otimes_F A^{op} : F] \\ &= ([A : F])^2 \\ &= n^2, \end{aligned}$$

quindi abbiamo che $[A_l A_r : F] = n^2$, che implica che $A_l A_r = \text{End}_F(A)$ e con questo abbiamo concluso, perché

$$A \otimes_F A^{op} \simeq A_l A_r = \text{End}_F(A) \simeq M_n(F).$$

□

Ora ci manca poco per poter definire il *Gruppo di Brauer* di un campo, per fare ciò introduciamo una relazione di equivalenza.

Definizione 1.3.8. Siano A e B algebre centrali semplici sul campo F , allora $A \sim B$ se esistono degli interi m e n tali che

$$A \otimes_F M_n(F) \simeq B \otimes_F M_m(F).$$

Osserviamo che questa è veramente una relazione di equivalenza, infatti è riflessiva

$$A \simeq A \otimes_F F = A \otimes_F M_1(F).$$

La simmetria è evidente dalla definizione e, per la transitività, supponiamo $A \otimes_F M_n(F) \simeq B \otimes_F M_m(F)$ e $B \otimes_F M_k(F) \simeq C \otimes_F M_l(F)$, allora

$$\begin{aligned} A \otimes_F M_{nk}(F) &\simeq A \otimes_F (M_n(F) \otimes_F M_k(F)) \\ &\simeq (A \otimes_F M_n(F)) \otimes_F M_k(F) \\ &\simeq (B \otimes_F M_m(F)) \otimes_F M_k(F) \\ &\simeq (B \otimes_F M_k(F)) \otimes_F M_m(F) \\ &\simeq (C \otimes_F M_l(F)) \otimes_F M_m(F) \\ &\simeq C \otimes_F M_{lm}(F). \end{aligned}$$

Definizione 1.3.9. Chiamiamo $\text{Br}(F)$ l'insieme delle classi di equivalenza di algebre centrali semplici sul campo F .

Teorema 1.3.10. *L'insieme $\text{Br}(F)$ con il prodotto*

$$[A][B] = [A \otimes_F B]$$

è un gruppo abeliano con elemento neutro $[F]$, e viene chiamato il Gruppo di Brauer di F .

Dimostrazione. Innanzitutto, se A e B sono algebre centrali semplici su F , anche $A \otimes_F B$ lo è, per 1.3.3.

Osserviamo poi che il prodotto è ben definito sulle classi d'equivalenza, infatti se $A \otimes_F M_n(F) \simeq A' \otimes_F M_m(F)$ e $B \otimes_F M_k(F) \simeq B' \otimes_F M_l(F)$ abbiamo che

$$\begin{aligned} (A \otimes_F B) \otimes_F M_{nk}(F) &\simeq (A \otimes_F M_n(F)) \otimes_F (B \otimes_F M_k(F)) \\ &\simeq (A' \otimes_F M_m(F)) \otimes_F (B' \otimes_F M_l(F)) \\ &\simeq (A' \otimes_F B') \otimes_F M_{ml}(F). \end{aligned}$$

Ora, $[F]$ è chiaramente l'elemento neutro per questo prodotto, visto che

$$[A][F] = [A \otimes_F F] = [A].$$

Per finire, per 1.3.7 abbiamo che A^{op} è l'inverso di A , infatti

$$[A][A^{op}] = [A \otimes_F A^{op}] = [M_n(F)] = [F].$$

□

Osservazione 1.3.11. Per il teorema di Wedderburn, abbiamo che per ogni A algebra centrale semplice su F , $A \simeq M_n(D)$ con D algebra di divisione centrale su F , cioè

$$A \simeq M_n(D) \simeq M_n(F) \otimes_F D;$$

quindi la relazione di equivalenza che abbiamo scritto in 1.3.8 è in realtà una relazione tra algebre di divisione e si ha per ogni A , $[A] = [D]$ per una qualche algebra di divisione D ed una sola. Per studiare il gruppo di Brauer di un campo F , possiamo allora limitarci a studiare le algebre di divisione centrali su F .

Un esempio molto semplice di gruppo di Brauer si osserva nel caso dei campi algebricamente chiusi: visto che l'unica algebra di divisione su F campo algebricamente chiuso è F stesso, non ci sono altre classi di equivalenza di algebre centrali semplici, quindi in tal caso $\text{Br}(F)$ è il gruppo banale.

1.4 Teorema di Noether-Skolem e Teorema del Centralizzatore

Lemma 1.4.1. *Sia R un anello Artiniano e sia $x \in R$. Se x non è uno zero divisore, allora è invertibile.*

Dimostrazione. Consideriamo catena discendente di ideali

$$R \supset Rx \supset Rx^2 \supset \cdots \supset Rx^n \supset \cdots ,$$

siccome R è Artiniano, questa si stabilizza da un certo N in poi. E' impossibile che $Rx^N = 0$ perché altrimenti avremmo $x^N = 0$, il che contraddice l'ipotesi che x non è uno zero divisore. Abbiamo allora $Rx^N = Rx^{N+1} \neq 0$, esiste allora $y \in R$ tale che

$$\begin{aligned} x^N &= yx^{N+1} \\ x^N - yx^{N+1} &= 0 \\ (1 - yx)x^N &= 0 \end{aligned}$$

ma x^N non è uno zero divisore perché non lo è x , quindi

$$(1 - yx) = 0 \quad \text{cioè} \quad yx = 1.$$

□

Teorema 1.4.2 (Noether-Skolem). *Sia R un'algebra semplice centrale su F e siano A e B sottoalgebre semplici di R che contengono F . Sia $\phi : A \rightarrow B$ un isomorfismo di algebre che fissa gli elementi di F , allora esiste $x \in R$, invertibile, tale che*

$$\phi(a) = x^{-1}ax \quad \text{per ogni } a \in A.$$

Dimostrazione. Usando le stesse convenzioni del teorema 1.3.7, consideriamo $\text{End}_F(R)$ l'insieme degli endomorfismi di R e consideriamo R_l , A_r e B_r i suoi sottoinsiemi dati rispettivamente dalla moltiplicazione a sinistra per elementi

di R e dalla moltiplicazione a destra per elementi di A e B . Ora, $R_l \otimes_F A_r$ è un'algebra semplice ed è isomorfa a $R_l A_r \subset \text{End}_F(A)$ esattamente per lo stesso ragionamento fatto in 1.3.7, analogamente $R_l \otimes_F B_r$ è un'algebra semplice isomorfa a $R_l B_r \subset \text{End}_F(B)$. La mappa da $R_l \otimes_F A_r$ in $R_l \otimes_F B_r$ definita da

$$L_r \otimes R_a \mapsto L_r \otimes R_{\phi(a)}$$

è chiaramente un isomorfismo.

Ora, diamo a R una struttura di $R_l \otimes_F A_r$ -modulo destro identificando appunto $R_l \otimes_F A_r$ con $R_l A_r$, tramite

$$x(L_u \otimes R_a) = uxa$$

e analogamente una struttura di $R_l \otimes_F B_r$ -modulo destro tramite

$$x(L_u \otimes R_b) = uxb.$$

Per 1.1.7 R è somma diretta di $R_l \otimes A_r$ -moduli semplici (o ideali minimali) V_i isomorfi tra loro, allo stesso modo è anche somma diretta di $R_l \otimes B_r$ -moduli semplici U_j . Visto che $R_l \otimes A_r \simeq R_l \otimes B_r$, anche $V_i \simeq U_j$.

Ora, sia $R = V_1 \oplus \cdots \oplus V_n = U_1 \oplus \cdots \oplus U_m$, supponiamo $n \leq m$ senza perdere di generalità, allora possiamo trovare degli isomorfismi

$$\sigma_i : V_i \rightarrow U_i \quad i = 1, \dots, n$$

tali che

$$\sigma_i(v_i L_u R_a) = \sigma_i(v_i) L_u R_{\phi(a)} \quad \text{per ogni } v_i \in V_i, u \in R, a \in A.$$

Sia allora $\sigma = \sum_{i=1}^n \sigma_i$, $\sigma : R \rightarrow R$ è iniettivo e vale

$$\sigma(v L_u R_a) = \sigma(v) L_u R_{\phi(a)} \quad \text{per ogni } v \in R, u \in R, a \in A. \quad (1.4)$$

In particolare, se prendiamo $v = 1$ e $a = 1$ abbiamo

$$\sigma(1 L_u) = \sigma(u) = \sigma(1) L_u = u \sigma(1) \quad \text{per ogni } u \in R. \quad (1.5)$$

Definiamo $x = \sigma(1)$, e prendiamo in (1.4) $u = 1, v = 1, a \in A$, si ha

$$\sigma(1R_a) = \sigma(a) = \sigma(1)R_{\phi(a)} = \sigma(1)\phi(a) = x\phi(a). \quad (1.6)$$

Ora, prendendo $u = a \in A$ in (1.5) abbiamo $\sigma(a) = ax$, che insieme a (1.6) ci dà

$$x\phi(a) = ax.$$

Per concludere, basta mostrare che x è invertibile. Non può essere uno zero divisore perchè se $v \in R$

$$0 = vx = v\sigma(1) = \sigma(v)$$

implica $v = 0$ per l'iniettività di σ , quindi è x è invertibile per 1.4.1. □

Questo è un risultato fondamentale, che risulterà utile molte volte in seguito, ora prima di arrivare all'altro teorema importante di questa parte, abbiamo bisogno di alcune nozioni sui centralizzatori.

Definizione 1.4.3. Sia D un anello e sia $S \subset D$, il *centralizzatore* di S in D è

$$C_D(S) = \{x \in D \mid xs = sx \text{ per ogni } s \in S\}.$$

Osservazione 1.4.4. E' chiaro che $C_D(S)$ è un sottoanello di D ; se poi D è un anello di divisione, $C_D(S)$ lo sarà a sua volta.

La prossima proposizione è una piccola generalizzazione del risultato che abbiamo già visto in 1.3.3 e usa le stesse idee.

Proposizione 1.4.5. *Sia F un campo e siano A, A', B, B' delle F -algebre tali che $A' \subset A$ e $B' \subset B$, allora*

$$C_{A \otimes_F B}(A' \otimes_F B') = C_A(A') \otimes_F C_B(B') \subset A \otimes_F B.$$

Dimostrazione. Innanzitutto, l'inclusione \supset è abbastanza evidente, infatti se $a \otimes b \in C_A(A') \otimes_F C_B(B')$ e $a' \otimes b' \in A' \otimes_F B' \subset A \otimes_F B$, abbiamo

$$(a \otimes b)(a' \otimes b') = (aa' \otimes bb') = (a'a \otimes b'b) = (a' \otimes b')(a \otimes b).$$

Ora, sia $x \in C_{A \otimes B}(A' \otimes_K B')$, seguendo un ragionamento molto simile a quello in 1.3.3, possiamo scrivere

$$x = \sum e_i \otimes b_i \quad e_i \in A, b_i \in B$$

con e_i linearmente indipendenti su F e ne otteniamo che per ogni $b' \in B'$,

$$0 = (1 \otimes b')x - x(1 \otimes b') = \sum e_i \otimes (b'b_i - b_i b'),$$

da cui $b'b_i = b_i b'$ per ogni i e quindi $b_i \in C_B(B')$. Analogamente, possiamo anche scrivere

$$x = \sum a_i \otimes f_i \quad a_i \in A, f_i \in B$$

con f_i linearmente indipendenti su F e allo stesso modo otteniamo che $a_i \in C_A(A')$ per ogni i . Quindi

$$x \in C_A(A') \otimes_F B \cap A \otimes_F C_B(B') = C_A(A') \otimes_F C_B(B').$$

□

Lemma 1.4.6. *Sia A una F -algebra e siano $A_l \subset \text{End}_F(A)$ e $A_r \subset \text{End}_F(A)$ i sottoanelli di $\text{End}_F(A)$ dati rispettivamente dalla moltiplicazione a sinistra e a destra per gli elementi di A . Allora*

$$C_{\text{End}(A)}(A_l) = A_r \quad e \quad C_{\text{End}(A)}(A_r) = A_l.$$

Dimostrazione. Mostriamo solo la prima affermazione, visto che la seconda si ottiene in modo totalmente analogo. Intanto $A_r \subset C_{\text{End}(A)}(A_l)$ banalmente, per l'altra inclusione supponiamo $f \in C_{\text{End}(A)}(A_l)$, allora $fL_a = L_a f$ per ogni $a \in A$, cioè

$$f(ax) = af(x) \quad \text{per ogni } a, x \in A.$$

In particolare per $x = 1$ abbiamo $f(a) = af(1)$ per ogni $a \in A$, quindi $f = R_{f(1)} \in A_r$. □

Abbiamo ora elementi sufficienti per dimostrare il cosiddetto teorema del *doppio centralizzatore*.

Teorema 1.4.7. *Sia R un'algebra centrale semplice su F e sia $A \subset R$ una F -sottoalgebra semplice. Allora*

1. $C_R(A)$ è semplice,
2. $C_R(C_R(A)) = A$.

Dimostrazione. Sia $[A : F] = n$ e consideriamo il sottoanello $A_l \subset \text{End}_F(A)$ dato dalla moltiplicazione a sinistra per gli elementi di A ; otteniamo in questo modo un'immersione di A in $M := M_n(F)$. Ora $C_M(A_l) = A_r$ per il lemma precedente, ma A_r è semplice in quanto isomorfo a A^{op} , ed abbiamo anche $C_M(C_M(A_l)) = C_M(A_r) = A_l$; quindi il teorema è verificato per $R = M = M_n(F)$.

Adesso, nel caso generale, $R \otimes_F M$ è un'algebra centrale semplice su F e abbiamo $A \subset M$ (considerando A come A_l), ma anche $A \subset R$. Quindi $A \otimes 1$ e $1 \otimes A$ sono F -sottoalgebre semplici di $R \otimes_F M$ e sono isomorfe tra loro tramite un isomorfismo che fissa F . Per il teorema di Noether-Skolem (1.4.2) sono quindi coniugate, cioè esiste $x \in R$ invertibile tale che

$$A \otimes 1 = x^{-1}(1 \otimes A)x.$$

Da ciò si deduce che anche i loro centralizzatori sono coniugati, infatti se $r \in C_{R \otimes M}(1 \otimes A)$ si ha che

$$\begin{aligned} x^{-1}rx(A \otimes 1) &= x^{-1}rxx^{-1}(1 \otimes A)x \\ &= x^{-1}r(1 \otimes A)x \\ &= x^{-1}(1 \otimes A)rx \\ &= x^{-1}(1 \otimes A)xx^{-1}rx, \end{aligned}$$

cioè $x^{-1}rx \in C_{R \otimes M}(A \otimes 1)$ e il viceversa si vede analogamente.

Ora, usando 1.4.5, abbiamo

$$C_{R \otimes M}(A \otimes 1) = C_R(A) \otimes_F M \quad \text{e}$$

$$C_{R \otimes M}(1 \otimes A) = R \otimes_F C_M(A).$$

ancora una volta, essendo questi coniugati, lo sono anche i loro centralizzatori, cioè

$$\begin{aligned} C_{R \otimes M}(C_{R \otimes M}(A \otimes 1)) &= C_{R \otimes M}(C_R(A) \otimes_F M) \\ &= C_R(C_R(A)) \otimes_F F \\ &\simeq C_R(C_R(A)) \end{aligned}$$

e

$$\begin{aligned} C_{R \otimes M}(C_{R \otimes M}(1 \otimes A)) &= C_{R \otimes M}(R \otimes_F C_M(A)) \\ &= C_R(R) \otimes_F C_M(C_M(A)) \\ &= F \otimes_F A \quad (\text{poiché il risultato è vero in } M_n(A)) \\ &\simeq A. \end{aligned}$$

Quindi $C_R(C_R(A))$ ed A sono isomorfe, e sono quindi della stessa dimensione su F ; ma, dal momento che $A \subset C_R(C_R(A))$, per ragioni di dimensione vale l'uguaglianza.

Abbiamo così ottenuto la parte (2) del teorema. Per la parte (1) osserviamo che, dal ragionamento precedente, abbiamo visto che $C_R(A) \otimes_F M$ e $R \otimes_F C_M(A)$ sono coniugate, quindi isomorfe. Sappiamo che $C_M(A) \simeq A^{op}$ da cui $R \otimes_F C_M(A)$ è semplice, quindi lo è anche $C_R(A) \otimes_F M$ per cui lo è $C_R(A)$. \square

Osservazione 1.4.8. Notiamo che $C_R(A) \otimes_F M_n(F) \simeq R \otimes_F A^{op}$ con $n = [A : F]$ implica che $[C_R(A) : F][A : F]^2 = [R : F][A : F]$ e quindi

$$[R : F] = [A : F][C_R(A) : F].$$

In particolare se A è un sottocampo di R tale che $[A : F]^2 = [R : F]$ abbiamo che $A = C_R(A)$.

Definizione 1.4.9. Sia K un sottocampo di un anello di divisione D . Diciamo che K è un *sottocampo massimale* se non è contenuto propriamente in nessun'altro sottocampo di D .

Osservazione 1.4.10. Un sottocampo massimale K di D deve per forza contenere il centro di D , altrimenti $C_D(D)K$ sarebbe un campo strettamente più grande di K .

Proposizione 1.4.11. *Sia D un anello di divisione e K un suo sottocampo, allora K è un sottocampo massimale se e solo se $K = C_D(K)$.*

Dimostrazione. Se $K = C_D(K)$ e $K \subset L$ sottocampo di D , allora si ha $L \subset C_D(K) = K$, cioè $L = K$ e quindi K è massimale.

Viceversa, se K è massimale e $a \in C_D(K)$, allora $K \subset K(a)$ che è un sottocampo di D ; quindi $K = K(a)$ per la massimalità di K . Ne segue che $C_D(K) \subset K$; ma abbiamo banalmente che $K \subset C_D(K)$ da cui l'uguaglianza. □

Osservazione 1.4.12. La prima parte della dimostrazione si può applicare anche quando K è un sottocampo di una F -algebra centrale semplice R , non necessariamente di divisione. In particolare, per l'osservazione 1.4.8 se $[K : F]^2 = [R : F]$ allora K è un sottocampo massimale.

Definizione 1.4.13. Sia A un'algebra semplice centrale sul campo F e sia K un'estensione di F , diciamo che K è un *campo di spezzamento* per A se per un qualche intero n

$$A \otimes_F K \simeq M_n(K).$$

Ad esempio, data A , una chiusura algebrica \bar{F} di F è un campo di spezzamento, come abbiamo visto nella dimostrazione di 1.3.5.

Osservazione 1.4.14. Se K è un campo di spezzamento per A , allora una qualunque estensione L/K è ancora un campo di spezzamento, infatti si ha

$$\begin{aligned} A \otimes_F L &\simeq A \otimes_F (K \otimes_K L) \\ &\simeq (A \otimes_F K) \otimes_K L \\ &\simeq M_n(K) \otimes_K L \\ &\simeq M_n(L). \end{aligned}$$

Teorema 1.4.15. *Sia D un'algebra di divisione centrale sul campo F e sia K un sottocampo massimale di D , allora K è un campo di spezzamento per D e $[D : F] = [K : F]^2$.*

Dimostrazione. Riprendiamo la dimostrazione di 1.4.7 considerando $R = D$ e $A = K$. Alla fine avevamo mostrato l'isomorfismo tra $D \otimes_F C_M(K)$ e $C_D(K) \otimes_F M$; ma K è commutativo, quindi $C_M(K) \simeq K^{op} \simeq K$, ed è un sottocampo massimale di D , quindi, per 1.4.11, $C_D(K) = K$. Ne otteniamo che

$$\begin{aligned} D \otimes_F K &\simeq D \otimes_F C_M(K) \\ &\simeq C_D(K) \otimes_F M \\ &= K \otimes_F M_n(F) \\ &\simeq M_n(K), \end{aligned}$$

dove $n = [K : F]$.

Per concludere, da quanto appena visto, si ha che

$$[D \otimes_F K : K] = n^2 = [K : F]^2$$

e poi

$$\begin{aligned} [D : F][K : F] &= [D \otimes_F K : F] \\ &= [D \otimes_K K : K][K : F] \\ &= [K : F]^2[K : F], \end{aligned}$$

da cui il risultato. □

Teorema 1.4.16. *Se A è un'algebra centrale semplice su F e K è un sottocampo di A , $K \supset F$, con $[A : F] = [K : F]^2$; allora K è un campo di spezzamento per A .*

Dimostrazione. Se $[A : F] = [K : F]^2$, per 1.4.8 abbiamo $C_A(K) = K$. Per lo stesso ragionamento del teorema appena visto, prendendo $D = A$ abbiamo

$$A \otimes_F K \simeq C_A(K) \otimes_F M_n(F) \simeq K \otimes_F M_n(F) \simeq M_n(K).$$

□

1.4.1 Il Gruppo di Brauer di \mathbb{R}

Possiamo vedere un'interessante applicazione di questi risultati nel determinare il gruppo di Brauer di \mathbb{R} . Innanzitutto osserviamo che i quaternioni \mathbb{H} sono un'algebra di divisione centrale su \mathbb{R} , che ha periodo 2 in $\text{Br}(\mathbb{R})$.

Infatti esiste un anti-automorfismo $\bar{\cdot} : \mathbb{H} \rightarrow \mathbb{H}$ dato da

$$z = a + ib + jc + kd \mapsto \bar{z} = a - ib - jc - kd$$

per cui si ha

$$\overline{z + w} = \bar{z} + \bar{w}$$

e

$$\overline{zw} = \bar{w}\bar{z}.$$

In conclusione si ha un isomorfismo $\bar{\cdot} : \mathbb{H} \rightarrow \mathbb{H}^{op}$. Da ciò deduciamo, utilizzando 1.3.7, che in $\text{Br}(\mathbb{R})$,

$$[\mathbb{H}]^2 = [\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}] = [\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{op}] = [M_4(\mathbb{R})] = [\mathbb{R}] = 1.$$

Ora, per studiare il gruppo di Brauer di \mathbb{R} , come conseguenza del teorema di Wedderburn, sappiamo che ci basta vedere quali sono le algebre di divisione centrali su \mathbb{R} . Sappiamo che una di queste è \mathbb{H} , vogliamo adesso vedere che non ce ne sono altre.

Teorema 1.4.17 (Frobenius). *Se D è un'algebra di divisione centrale di dimensione finita su \mathbb{R} e $D \not\simeq \mathbb{R}$, allora $D \simeq \mathbb{H}$.*

Dimostrazione. Consideriamo un sottocampo massimale K di D . Essendo K un'estensione finita di \mathbb{R} , abbiamo solo due possibilità: $K \simeq \mathbb{R}$ oppure $K \simeq \mathbb{C}$. Nel primo caso, per 1.4.15, abbiamo

$$[D : \mathbb{R}] = [K : \mathbb{R}]^2 = 1^2 = 1$$

e quindi $D \simeq \mathbb{R}$. Ci mettiamo quindi nel secondo caso; sempre per 1.4.15 abbiamo

$$[D : \mathbb{R}] = [K : \mathbb{R}]^2 = 2^2 = 4.$$

Ora, K è un sottocampo di D isomorfo ai numeri complessi, quindi avremo $K = \mathbb{R} + \mathbb{R}i$ con $i^2 = -1$. Il coniugio in K , dato da

$$\phi(a + bi) = (a - bi),$$

è un automorfismo di K che fissa \mathbb{R} , quindi per il teorema di Noether-Skolem (1.4.2) esiste $x \in D$ tale che

$$\phi(a + bi) = x^{-1}(a + bi)x,$$

da cui abbiamo $\phi(i) = -i = x^{-1}ix$ per cui

$$x^{-2}ix^2 = i \quad \text{cioè} \quad ix^2 = x^2i$$

e quindi $x^2 \in C_D(K) = K$ perchè K è massimale (1.4.11).

Ora, però, sappiamo che $x \notin K$ e che x^2 commuta con x ; quindi dobbiamo avere $x^2 \in \mathbb{R}$. Osserviamo che non è possibile che $x^2 > 0$, perché altrimenti avremmo $x \in \mathbb{R}$, dal momento che le radici quadrate di numeri reali positivi stanno ancora in \mathbb{R} . Si ha quindi $x^2 = -\alpha^2$ per un qualche $\alpha \in \mathbb{R}$; poniamo allora $j := \frac{x}{\alpha}$ e vediamo che

$$j^2 = \frac{x^2}{\alpha^2} = -1 \quad \text{e} \quad ji = \frac{x}{\alpha}i = -\frac{ix}{\alpha} = -ij.$$

Se definiamo $k := ij$ abbiamo

$$k^2 = ijij = -iijj = -(-1)(-1) = -1 \quad \text{e} \quad ijk = k^2 = -1.$$

I quattro elementi $1, i, j, k$ sono linearmente indipendenti su \mathbb{R} ; quindi, poiché $[D : \mathbb{R}] = 4$, generano tutto D , e con questo abbiamo concluso. \square

Corollario 1.4.18. $\text{Br}(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Dimostrazione. Una classe $[A]$ di algebre centrali semplici in $\text{Br}(\mathbb{R})$ ha sempre come rappresentante un'algebra di divisione, quindi per il teorema appena dimostrato le uniche due possibilità sono $[A] = [\mathbb{R}]$ oppure $[A] = [\mathbb{H}]$. Chiaramente $[\mathbb{R}] \neq [\mathbb{H}]$, quindi $\text{Br}(\mathbb{R})$ è un gruppo con due elementi. \square

Il caso di \mathbb{R} è un caso particolarmente semplice, ma per studiare dei gruppi di Brauer più complicati ci servono altri risultati. In particolare vogliamo collegarci alla teoria di Galois; ci serve quindi sapere se il campo di spezzamento di un'algebra centrale semplice è un'estensione di Galois del campo di base.

Teorema 1.4.19. *Se D è un'algebra di divisione algebrica sul suo centro F , con $D \neq F$, allora esiste $x \in D \setminus F$ tale che x è separabile su F .*

Dimostrazione. Se D ha caratteristica 0 non c'è niente da provare perché ogni elemento di D è separabile su F . Consideriamo dunque D di caratteristica $p \neq 0$. Se per assurdo la proposizione fosse falsa, D sarebbe puramente inseparabile su F , cioè dato $x \in D$, allora $x^{p^{n(x)}} \in F$ per un qualche $n(x) \geq 0$. Quindi esisterebbe $a \in D \setminus F$ tale che $a^p \in F$.

Definiamo $\delta : D \rightarrow D$ tramite

$$\delta(x) = xa - ax.$$

Mostriamo per induzione che

$$\delta^n(x) = \sum_{i=0}^n (-1)^i \binom{n}{i} a^i x a^{n-i}.$$

Per $n = 1$ è banalmente vero; supponiamolo vero per n , allora

$$\begin{aligned}
\delta^{n+1}(x) &= \delta(\delta^n(x)) \\
&= \left(\sum_{i=0}^n (-1)^i \binom{n}{i} a^i x a^{n-i} \right) a - a \left(\sum_{i=0}^n (-1)^i \binom{n}{i} a^i x a^{n-i} \right) \\
&= \sum_{i=0}^n (-1)^i \binom{n}{i} a^i x a^{n-i+1} - \sum_{i=0}^n (-1)^i \binom{n}{i} a^{i+1} x a^{n-i} \\
&= x a^{n+1} + \sum_{i=1}^n (-1)^i \binom{n}{i} a^i x a^{n-i} - \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} a^i x a^{n-i} + (-1)^{n+1} a^{n+1} x \\
&= x a^{n+1} + \sum_{i=1}^n (-1)^i \binom{n}{i} a^i x a^{n-i} - \sum_{j=1}^n (-1)^{j-1} \binom{n}{j-1} a^i x a^{n-j+1} + (-1)^{n+1} a^{n+1} x \\
&= x a^{n+1} + \sum_{i=1}^n (-1)^i \binom{n}{i} a^i x a^{n-i} + \sum_{i=1}^n (-1)^i \binom{n}{i-1} a^i x a^{n-i+1} + (-1)^{n+1} a^{n+1} x \\
&= x a^{n+1} + \sum_{i=1}^n (-1)^i \left(\binom{n}{i} + \binom{n}{i-1} \right) a^i x a^{n-i} + (-1)^{n+1} a^{n+1} x \\
&= \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} a^i x a^{n+1-i}.
\end{aligned}$$

Quindi, visto che siamo in caratteristica p e $p \mid \binom{p}{i}$ per $0 < i < p$,

$$\delta^p(x) = x a^p - a^p x$$

che è nullo perché $a^p \in F$.

Dal momento che $a \notin F$, $\delta \neq 0$; quindi se $\delta(y) \neq 0$, esiste $k > 1$ tale che $\delta^k(y) = 0$, ma con $\delta^{k-1}(y) \neq 0$. Poniamo $x = \delta^{k-1}(y)$; visto che $k > 1$, abbiamo che $x = \delta(w) = wa - aw$, ed anche, essendo $\delta(x) = 0$, $xa = ax$. Siamo in un anello di divisione, quindi possiamo scrivere $x = au$, con u che commuta con a perché x lo fa.

Allora $au = wa - aw$ da cui

$$a = (wa - aw)u^{-1} = (wu^{-1})a - a(wu^{-1}) = ca - ac \quad (\text{ponendo } c = wu^{-1})$$

e quindi $c = 1 + aca^{-1}$.

Sappiamo però che esiste t tale che $c^{p^t} \in F$, il che ci dà

$$\begin{aligned} c^{p^t} &= (1 + aca^{-1})^{p^t} \\ &= 1 + (aca^{-1})^{p^t} \\ &= 1 + ac^{p^t}a^{-1} \\ &= 1 + aa^{-1}c^{p^t} \\ &= 1 + c^{p^t}. \end{aligned}$$

Ciò è assurdo perchè si avrebbe $0 = 1$. □

Teorema 1.4.20. *Sia D un'algebra di divisione centrale su F , allora D ha un sottocampo massimale che è separabile su F .*

Dimostrazione. Se $D = F$ non c'è niente da dimostrare. Se $D \neq F$, per 1.4.19 sappiamo che esiste $a \in D \setminus F$, separabile su F . Quindi esistono sottocampi separabili di D che contengono strettamente F . Sia K un tale sottocampo e richiediamo che sia massimale con questa proprietà; vogliamo mostrare che K è un sottocampo massimale di D , cioè, per 1.4.11, che $C_D(K) = K$.

Ora, poiché K è commutativo, $K \subset C_D(K)$; inoltre K è semplice e di dimensione finita su F , quindi, per 1.4.7, $K = C_D(C_D(K))$. Quindi K è il centro di $C_D(K)$. Ma, se $C_D(K) \neq K$, per 1.4.19 avremmo un $u \in C_D(K) \setminus K$ separabile su K ; questo porterebbe ad avere $K(u)$ separabile su F e strettamente più grande di K , il che ne contraddice la massimalità. In conclusione $C_D(K) = K$ che è quindi un sottocampo massimale di D . □

Corollario 1.4.21. *Se A è un'algebra semplice centrale su F , allora A ha un campo di spezzamento separabile. Inoltre si può anche richiedere che tale campo di spezzamento sia normale su F , quindi sia un'estensione di Galois di F .*

Dimostrazione. Per il teorema di Wedderburn (1.1.13), $A \simeq D \otimes_F M_n(F)$ con D algebra di divisione centrale su F . Sia K un sottocampo massimale

separabile di D ; allora

$$\begin{aligned} A \otimes_F K &\simeq (D \otimes_F M_n(F)) \otimes_F K \\ &\simeq (D \otimes_F K) \otimes_F M_n(F) \\ &\simeq M_m(F) \otimes_F M_n(F) \\ &\simeq M_{mn}(F). \end{aligned}$$

Quindi K è un campo di spezzamento separabile per A . Per concludere prendiamo L un'estensione normale finita di F che contiene K (ad esempio la chiusura normale di K); allora L è ancora un campo di spezzamento, in quanto estensione di K , quindi ha tutte le caratteristiche richieste. \square

1.5 Norma e Traccia ridotta

Ricordiamo rapidamente la definizione e alcune proprietà delle applicazioni norma e traccia; per i dettagli si può vedere, ad esempio, [5] cap.VIII §5.

Definizione 1.5.1. Se A un'algebra sul campo F , $[A : F] = n$, ogni $\alpha \in A$ definisce $\alpha_L \in \text{End}_F(A)$ tramite

$$\alpha_L(x) = \alpha x.$$

Il *polinomio caratteristico* di α su F (che possiamo a volte indicare con $\text{pol. car.}_{A/F} \alpha$), è il polinomio caratteristico di α_L in $\text{End}_F(A)$.

Definiamo l'applicazione *norma* e *traccia*

$$N_{A/F} : A \rightarrow F \quad \text{e} \quad \text{Tr}_{A/F} : A \rightarrow F$$

tramite

$$\alpha \mapsto \det(\alpha_L) \quad \text{e} \quad \alpha \mapsto \text{traccia di } \alpha_L.$$

Per ogni $\alpha, \beta \in A$, $k \in F$ valgono le seguenti proprietà:

$$\begin{cases} \text{Tr}(\alpha\beta) = \text{Tr}(\beta\alpha), \quad \text{Tr}(\alpha + \beta) = \text{Tr}(\alpha) + \text{Tr}(\beta), \quad \text{Tr}(k\alpha) = k \text{Tr}(\alpha) \\ \text{N}(\alpha\beta) = \text{N}(\alpha) \text{N}(\beta), \quad \text{N}(k\alpha) = k^n \text{N}(\alpha) \end{cases}$$

Proposizione 1.5.2. *Alcune altre proprietà:*

- Se K è un'estensione di F , per ogni $\alpha \in A$ si ha

$$\text{pol. car.}_{A/F} \alpha = \text{pol. car.}_{A \otimes K/K}(\alpha \otimes 1).$$

- Se K è un'estensione di F e A è una K -algebra abbiamo che, per ogni $\alpha \in A$,

$$\text{Tr}_{A/F} \alpha = \text{Tr}_{A/K}(\text{Tr}_{K/F} \alpha) \quad \text{e} \quad \text{N}_{A/F} \alpha = \text{N}_{A/K}(\text{N}_{K/F} \alpha).$$

- Se K/F è un'estensione di Galois si ha che, per ogni $\alpha \in K$

$$\text{Tr}_{K/F} \alpha = \sum_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha) \quad \text{e} \quad \text{N}_{K/F} \alpha = \prod_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha).$$

Definizione 1.5.3. Se K è un'estensione di F , possiamo definire la *forma traccia* $\tau : K \times K \rightarrow F$ tramite

$$\tau(\alpha, \beta) = \text{Tr}_{K/F}(\alpha\beta) \quad \alpha, \beta \in K.$$

E' una forma bilineare simmetrica e si ha il seguente risultato.

Teorema 1.5.4. *Sia K/F un'estensione, sono equivalenti le seguenti affermazioni:*

1. K è separabile su F ;
2. la forma traccia da $K \times K$ in F è non degenera;
3. esiste un $\alpha \in K$ tale che $\text{Tr}_{K/F} \alpha = 1$;
4. l'applicazione $\text{Tr}_{K/F} : K \rightarrow F$ è suriettiva.

Ora, sia A un'algebra centrale semplice sul campo F ; per 1.4.21 esiste un'estensione K/F con K campo di spezzamento per A . Quindi esiste un isomorfismo di K -algebre

$$h : A \otimes_F K \simeq M_n(K) \quad n^2 = [A : F]. \quad (1.7)$$

Se g è un altro tale isomorfismo, allora $h \circ g^{-1}$ è un K -automorfismo di $M_n(K)$; quindi, per 1.4.2, esiste $C \in M_n(K)$, C invertibile, tale che

$$h(u) = Cg(u)C^{-1}, \quad \text{per ogni } u \in A \otimes_F K.$$

Ne segue che le matrici $h(u)$ e $g(u)$ hanno lo stesso polinomio caratteristico; cioè il polinomio caratteristico di $h(u)$ non dipende dalla scelta del K -isomorfismo h in (1.7), è quindi ben posta la seguente definizione.

Definizione 1.5.5. Sia $a \in A$, il *polinomio caratteristico ridotto* di a su F , che indicheremo con $\text{pcr}_{A/F} a$, è il polinomio caratteristico di $h(a \otimes 1) \in M_n(K)$.

Teorema 1.5.6. *Per ogni $a \in A$, $\text{pcr}_{A/F} a \in F[X]$ e non dipende dalla scelta del campo di spezzamento K usato per la definizione.*

Dimostrazione. Se L è un altro campo di spezzamento per A , possiamo trovare un campo Ω , che contiene F , nel quale esistono le F -immersioni $K \rightarrow \Omega$ e $L \rightarrow \Omega$. Per vedere che il polinomio caratteristico ridotto non dipende dalla scelta del campo di spezzamento, ci basta quindi vedere che $\text{pcr}_{A/F} a$ è lo stesso, sia che lo definiamo usando K , sia usando Ω . Abbiamo un isomorfismo di Ω -algebre

$$h \otimes 1 : (A \otimes_F K) \otimes_K \Omega \simeq M_n(K) \otimes_K \Omega,$$

dopo aver fatto le identificazioni canoniche, possiamo riscrivere questo isomorfismo come

$$h' : A \otimes_F \Omega \simeq M_n(\Omega).$$

Possiamo vedere ogni elemento $u \in A \otimes_F K$ come un elemento di $A \otimes_F \Omega$ ed in tal caso $h'(u)$ è esattamente la matrice $h(u)$ vista come elemento di $M_n(\Omega)$. Di conseguenza i polinomi caratteristici di $h(u)$ e di $h'(u)$ coincidono per $u \in A \otimes_F K$. In particolare questo vale quando $u = a \otimes 1$, quindi $\text{pcr}_{A/F} a$ non dipende dalla scelta del campo di spezzamento usato per definirlo.

Ora, per vedere che $\text{pcr}_{A/F} a \in F[X]$, possiamo supporre che l'estensione K/F che abbiamo usato per definire pcr sia un'estensione di Galois (vedi 1.4.21). Sia $\sigma \in \text{Gal}(K/F)$, allora $1 \otimes \sigma \in \text{Aut}_F(A \otimes_F K)$; definiamo poi $\sigma^* : M_n(K) \rightarrow M_n(K)$ come l'automorfismo che manda ogni elemento b_{ij} della matrice in $\sigma(b_{ij})$; chiaramente $\sigma^* \in \text{Aut}_F(M_n(K))$. Sia h l'isomorfismo che abbiamo usato in (1.7), definiamo allora

$$h' := \sigma^* \circ h \circ (1 \otimes \sigma)^{-1},$$

abbiamo $h' : A \otimes_F K \rightarrow M_n(K)$ ed è un isomorfismo tale che $\sigma^* h = h'(1 \otimes \sigma)$. Quindi, per $a \in A$

$$\sigma^* h(a \otimes 1) = h'(1 \otimes \sigma)(a \otimes 1) = h'(a \otimes 1).$$

Abbiamo allora, per la definizione di $\text{pcr}_{A/F} a$,

$$\begin{aligned} \text{pcr}_{A/F} a &= \text{pol. car. } h'(a \otimes 1) \\ &= \text{pol. car. } \sigma^* h(a \otimes 1) \\ &= \sigma(\text{pol. car. } h(a \otimes 1)) \\ &= \sigma(\text{pcr}_{A/F} a) \end{aligned}$$

questo mostra che i coefficienti di $\text{pcr}_{A/F} a$ sono invarianti per ogni $\sigma \in \text{Gal}(K/F)$, quindi $\text{pcr}_{A/F} a \in F[X]$. \square

Teorema 1.5.7. *Se $[A : F] = n^2$, allora*

$$\text{pol. car.}_{A/F} a = (\text{pcr}_{A/F} a)^n \quad \text{per ogni } a \in A.$$

Dimostrazione. Sia $K \supset F$ un campo di spezzamento di A , cioè $A \otimes_F K = M_n(K)$. Abbiamo che

$$\text{pol. car.}_{A/F} a = \text{pol. car.}_{A \otimes K/K} a \otimes 1 \quad \text{per ogni } a \in A.$$

Per 1.1.7 $A \otimes_F K \simeq I^m$, dove I è un ideale sinistro minimale di $A \otimes_F K$; in particolare, per 1.1.15 abbiamo $[I : K] = n$, quindi $m = n$ per ragioni di dimensione. Allora

$$\text{pol. car.}_{A \otimes K/K} a \otimes 1 = f(X)^n,$$

dove $f(X)$ è il polinomio caratteristico della matrice che descrive la moltiplicazione a sinistra per $(a \otimes 1)$ su una base di I su K . D'altra parte, il K -isomorfismo (1.7) può essere ottenuto inviando ogni $y \in A \otimes_F K$ sulla matrice y_L che descrive la moltiplicazione a sinistra per y su una base di I su K , e quindi

$$\text{pol. car. } h(y) = \text{pol. car. } y_L \quad \text{per ogni } y \in A \otimes_F K.$$

Se prendiamo $y = a \otimes 1$ con $a \in A$ abbiamo allora

$$\text{pcr}_{A/F} a = \text{pol. car. } h(a \otimes 1) = \text{pol. car. } (a \otimes 1)_L$$

e quindi $\text{pol. car.}_{A/F} a = f(X)^n$, come richiesto. \square

Definizione 1.5.8. Se scriviamo

$$\text{pcr}_{A/F} a = X^m - (\text{trd}_{A/F}(a))X^{m-1} + \cdots + (-1)^m \text{nrd}_{A/F}(a), \quad \text{per ogni } a \in A.$$

Chiamiamo $\text{trd}_{A/F}(a)$ e $\text{nrd}_{A/F}(a)$ rispettivamente la *traccia ridotta* e la *norma ridotta* di a su F .

Osservazione 1.5.9. Per 1.5.7 abbiamo che

$$\text{Tr}_{A/F}(a) = n \text{trd}_{A/F}(a) \quad \text{e} \quad \text{N}_{A/F}(a) = (\text{nrd}_{A/F}(a))^n.$$

Osservazione 1.5.10. Usando la notazione della dimostrazione di 1.5.7, l'applicazione $a \mapsto (a \otimes 1)_L$ è un isomorfismo di K -algebre di A in $\text{End}_K(I)$.

Dal momento che $\text{trd}(a)$ è la traccia di $(a \otimes 1)_L$ e $\text{nrd}(a)$ è il determinante di $(a \otimes 1)_L$, ne concludiamo che per ogni $a, b \in A$ e $\alpha \in F$

$$\text{trd}(ab) = \text{trd}(ba), \quad \text{trd}(a + b) = \text{trd}(a) + \text{trd}(b), \quad \text{trd}(\alpha a) = \alpha \text{trd}(a)$$

$$\text{nrd}(ab) = \text{nrd}(a) \text{nrd}(b) \quad \text{nrd}(\alpha a) = \alpha^n \text{nrd}(a).$$

1.6 Prodotti Incrociati

Sia A un'algebra centrale semplice su F , per il teorema di Wedderburn $A \simeq D \otimes_F M_k(F)$ con D algebra di divisione centrale su F . Se $[D : F] = n^2$ e K è un sottocampo massimale separabile di D , allora $[K : F] = n$. Sia L la chiusura normale di K e supponiamo che $[L : K] = m$. Poniamo $B = D \otimes_F M_m(F)$, allora B è centrale semplice su F ed inoltre $L \subset B$ perchè

$$B \supset K \otimes_F M_m(F) \simeq M_m(K) \supset L$$

con l'inclusione di L in $M_m(K)$ data dalla rappresentazione regolare su K .

Ora,

$$[B : F] = [D : F][M_m(F) : F] = n^2 m^2 = ([L : K][K : F])^2 = [L : F]^2.$$

Osservazione 1.6.1. Per quanto appena visto, per ogni A algebra centrale semplice su F , esiste un'algebra B , con $[B] = [A]$ in $\text{Br}(F)$; tale che B ha un sottocampo massimale L che è un'estensione di Galois di F , con $[B : F] = [L : F]^2$.

Possiamo quindi, per studiare il gruppo di Brauer di un campo F , limitarci a considerare algebre di questo tipo. Vedremo in quello che segue che c'è un certo modo di costruire tali algebre.

Definizione 1.6.2. Sia K un campo e sia G un gruppo. Una funzione $f : G \times G \rightarrow K^*$ si dice un *factor set* su G in K se

$$f(\sigma\tau, \nu)f(\sigma, \tau) = f(\sigma, \tau\nu)\sigma(f(\tau, \nu)) \quad \text{per ogni } \sigma, \tau, \nu \in G.$$

Osservazione 1.6.3. Se poniamo $\sigma = \tau = 1$ otteniamo che

$$f(1, \nu) = f(1, 1) \quad \text{per ogni } \nu \in G$$

e, se poniamo $\tau = \nu = 1$, abbiamo

$$f(\sigma, 1) = \sigma(f(1, 1)) \quad \text{per ogni } \sigma \in G.$$

Definizione 1.6.4. Sia K/F un'estensione di Galois, sia $G = \text{Gal}(K/F)$ e sia f un factor set su G in K . Definiamo formalmente un'algebra *prodotto incrociato* $A = (K/F, f)$ con $A = \left\{ \sum_{\sigma \in G} k_{\sigma} x_{\sigma} \mid k_{\sigma} \in K \right\}$. L'uguaglianza e l'addizione in A si fanno componente per componente e i simboli x_{σ} hanno le seguenti proprietà:

- (1) $x_{\sigma} k = \sigma(k) x_{\sigma}$ per ogni $k \in K$
- (2) $x_{\sigma} x_{\tau} = f(\sigma, \tau) x_{\sigma\tau}$ per ogni $\sigma, \tau \in G$.

Proposizione 1.6.5. $A = (K/F, f)$ come appena definita, è una F -algebra; inoltre $[A : F] = n^2$ dove $n = |G|$.

Dimostrazione. Vediamo che A è uno spazio vettoriale su F ed è un anello. Supponiamo $v, w \in A$, $v = \sum_{\sigma \in G} k_{\sigma} x_{\sigma}$ e $w = \sum_{\sigma \in G} l_{\sigma} x_{\sigma}$, $\alpha \in F$, allora

$$\begin{aligned} v + w &= \sum_{\sigma \in G} k_{\sigma} x_{\sigma} + \sum_{\sigma \in G} l_{\sigma} x_{\sigma} = \sum_{\sigma \in G} (k_{\sigma} + l_{\sigma}) x_{\sigma} \in A, \\ \alpha v &= \alpha \left(\sum_{\sigma \in G} k_{\sigma} x_{\sigma} \right) = \sum_{\sigma \in G} (\alpha k_{\sigma}) x_{\sigma} \in A, \\ vw &= \left(\sum_{\sigma \in G} k_{\sigma} x_{\sigma} \right) \left(\sum_{\tau \in G} l_{\tau} x_{\tau} \right) = \sum_{\sigma, \tau \in G} k_{\sigma} x_{\sigma} l_{\tau} x_{\tau} \\ &= \sum_{\sigma, \tau \in G} k_{\sigma} \sigma(l_{\tau}) x_{\sigma} x_{\tau} = \sum_{\sigma, \tau \in G} k_{\sigma} \sigma(l_{\tau}) f(\sigma, \tau) x_{\sigma\tau} \in A. \end{aligned}$$

L'unità per la moltiplicazione è $f(1, 1)^{-1} x_1$, infatti

$$\begin{aligned} f(1, 1)^{-1} x_1 \left(\sum_{\sigma \in G} k_{\sigma} x_{\sigma} \right) &= \sum_{\sigma \in G} f(1, 1)^{-1} x_1 k_{\sigma} x_{\sigma} \\ &= \sum_{\sigma \in G} f(1, 1)^{-1} k_{\sigma} x_1 x_{\sigma} \\ &= \sum_{\sigma \in G} k_{\sigma} f(1, 1)^{-1} f(1, \sigma) x_{1\sigma} \\ &= \sum_{\sigma \in G} k_{\sigma} f(1, 1)^{-1} f(1, 1) x_{\sigma} \\ &= \sum_{\sigma \in G} k_{\sigma} x_{\sigma}. \end{aligned}$$

Si vede facilmente che che $f(1, 1)^{-1}x_1$ è un unità anche a destra e che la moltiplicazione è distributiva. Per l'associatività, basta limitarsi a mostrare che per ogni $\sigma, \tau, \nu \in G$ si ha

$$(x_\sigma x_\tau)x_\nu = x_\sigma(x_\tau x_\nu)$$

ma abbiamo

$$\begin{aligned} (x_\sigma x_\tau)x_\nu &= f(\sigma, \tau)x_{\sigma\tau}x_\nu \\ &= f(\sigma, \tau)f(\sigma\tau, \nu)x_{\sigma\tau\nu} \end{aligned}$$

poiché f è un factor set

$$\begin{aligned} &= \sigma(f(\tau, \nu))f(\sigma, \tau\nu)x_{\sigma\tau\nu} \\ &= \sigma(f(\tau, \nu))x_\sigma x_{\tau\nu} \\ &= x_\sigma f(\tau, \nu)x_{\tau\nu} \\ &= x_\sigma(x_\tau x_\nu). \end{aligned}$$

Per quanto riguarda la dimensione, è evidente che

$$[A : F] = [A : K][K : F] = |G||G| = n^2.$$

□

Ci interessa sapere quando due algebre tali sono isomorfe, in particolare come dipendono dalla scelta del factor set.

Definizione 1.6.6. Due factor set f e g si dicono *equivalenti* se esiste una funzione $\lambda : G \rightarrow K^*$ tale che

$$g(\sigma, \tau) = \sigma(\lambda_\tau)\lambda_\sigma\lambda_{\sigma\tau}^{-1}f(\sigma, \tau) \quad \forall \sigma, \tau \in G.$$

Osservazione 1.6.7. Questa è una relazione di equivalenza. Infatti prendendo $\lambda \equiv 1$ abbiamo che f è equivalente a sè stesso; poi se $g(\sigma, \tau) = \sigma(\lambda_\tau)\lambda_\sigma\lambda_{\sigma\tau}^{-1}f(\sigma, \tau)$, allora prendendo $\mu = \frac{1}{\lambda}$ si ha

$$f(\sigma, \tau) = \sigma(\mu_\tau)\mu_\sigma\mu_{\sigma\tau}^{-1}g(\sigma, \tau);$$

infine da

$$g(\sigma, \tau) = \sigma(\lambda_\tau)\lambda_\sigma\lambda_{\sigma\tau}^{-1}f(\sigma, \tau)$$

e

$$f(\sigma, \tau) = \sigma(\mu_\tau)\mu_\sigma\mu_{\sigma\tau}^{-1}h(\sigma, \tau),$$

si ha

$$g(\sigma, \tau) = \sigma(\rho_\tau)\rho_\sigma\rho_{\sigma\tau}^{-1}h(\sigma, \tau),$$

con $\rho = \lambda\mu$.

Vogliamo ora vedere che questa relazione di equivalenza è proprio quella di cui abbiamo bisogno.

Proposizione 1.6.8. *Le algebre $(K/F, f)$ e $(K/F, g)$ sono isomorfe se e solo se f e g sono equivalenti.*

Dimostrazione. Supponiamo f e g siano equivalenti, allora

$$g(\sigma, \tau) = \lambda_{\sigma\tau}^{-1}\sigma(\lambda_\tau)\lambda_\sigma f(\sigma, \tau).$$

Siano $x_\sigma \in A = (K/F, f)$ tali che $A = \sum_{\sigma \in G} Kx_\sigma$ e che hanno le proprietà

$$x_\sigma x_\tau = f(\sigma, \tau)x_{\sigma\tau} \quad \text{e} \quad x_\sigma k = \sigma(k)x_\sigma.$$

Ora $y_\sigma = \lambda_\sigma x_\sigma \in A$ sono ancora tali che $A = \sum_{\sigma \in G} Ky_\sigma$, inoltre si ha

$$y_\sigma k = \lambda_\sigma x_\sigma k = \lambda_\sigma \sigma(k)x_\sigma = \sigma(k)\lambda_\sigma x_\sigma = \sigma(k)y_\sigma,$$

ed anche

$$\begin{aligned} y_\sigma y_\tau &= \lambda_\sigma x_\sigma \lambda_\tau x_\tau \\ &= \lambda_\sigma \sigma(\lambda_\tau) x_\sigma x_\tau \\ &= \lambda_\sigma \sigma(\lambda_\tau) f(\sigma, \tau) x_{\sigma\tau} \\ &= \lambda_\sigma \sigma(\lambda_\tau) f(\sigma, \tau) \lambda_{\sigma\tau}^{-1} y_{\sigma\tau} \\ &= g(\sigma, \tau) y_{\sigma\tau}. \end{aligned}$$

Abbiamo così visto che A si scrive anche come $(K/F, g)$, quindi $(K/F, f) \simeq (K/F, g)$.

Viceversa, se $A = (K/F, f) = \sum_{\sigma \in G} Kx_\sigma$ e $B = (K/F, g) = \sum_{\sigma \in G} Ky_\sigma$ sono isomorfe, allora possiamo trovare un isomorfismo $\psi : A \rightarrow B$ che fissa K . Quindi, dal fatto che

$$\psi(x_\sigma)k = \psi(x_\sigma k) = \psi(\sigma(k)x_\sigma) = \sigma(k)\psi(x_\sigma) \quad \text{per ogni } k \in K,$$

e che possiamo sempre scrivere

$$\psi(x_\sigma) = \sum_{\tau \in G} \lambda_\tau y_\tau,$$

ricaviamo

$$\begin{aligned} \sum_{\tau \in G} \tau(k)\lambda_\tau y_\tau &= \sum_{\tau \in G} \lambda_\tau y_\tau k \\ &= \psi(x_\sigma)k \\ &= \sigma(k)\psi(x_\sigma) \\ &= \sum_{\tau \in G} \sigma(k)\lambda_\tau y_\tau \\ 0 &= \sum_{\tau \in G} (\sigma(k) - \tau(k))\lambda_\tau y_\tau \end{aligned}$$

da cui si deduce che $\lambda_\tau = 0$ per ogni $\tau \neq \sigma$, cioè $\psi(x_\sigma) = \lambda_\sigma y_\sigma$.

Per finire,

$$\begin{aligned} f(\sigma, \tau)\psi(x_{\sigma\tau}) &= \psi(f(\sigma, \tau)x_{\sigma\tau}) \\ &= \psi(x_\sigma x_\tau) \\ &= \psi(x_\sigma)\psi(x_\tau) \\ &= \lambda_\sigma y_\sigma \lambda_\tau y_\tau \\ &= \lambda_\sigma \sigma(\lambda_\tau) y_\sigma y_\tau \\ &= \lambda_\sigma \sigma(\lambda_\tau) g(\sigma, \tau) y_{\sigma\tau} \\ &= \lambda_\sigma \sigma(\lambda_\tau) g(\sigma, \tau) \lambda_{\sigma\tau}^{-1} \psi(x_{\sigma\tau}); \end{aligned}$$

quindi f e g sono equivalenti. □

Osservazione 1.6.9. Ogni factor set è equivalente ad uno normalizzato, cioè con

$$f(\sigma, 1) = f(1, \sigma) = 1 \in K \quad \text{per ogni } \sigma \in G.$$

Infatti sia g un factor set qualunque, sia $t = g(1, 1)^{-1}$ e sia $\lambda_\sigma = \sigma(t)$; definiamo allora un factor set equivalente tramite

$$f(\sigma, \tau) = \sigma(\lambda_\tau)\lambda_\sigma\lambda_{\sigma\tau}^{-1}g(\sigma, \tau) = \sigma(t)g(\sigma, \tau)$$

e questo verifica

$$f(1, \sigma) = f(1, 1) = tg(1, 1) = 1 \quad \text{e}$$

$$f(\sigma, 1) = \sigma(t)g(\sigma, 1) = \sigma(g(1, 1)^{-1})\sigma(g(1, 1)) = 1.$$

Quindi nello studio dei prodotti incrociati possiamo sempre assumere, senza perdere di generalità, che tutti i factor set siano normalizzati e che x_1 sia l'elemento neutro della moltiplicazione.

Teorema 1.6.10. *$(K/F, f)$ è un'algebra centrale semplice su F che ha K come sottocampo massimale. Inoltre, data A una qualunque algebra centrale semplice su F , esistono K ed f tali che, in $\text{Br}(F)$, $[A] = [(K/F, f)]$.*

Dimostrazione. Per l'osservazione appena fatta, assumiamo f normalizzato e identifichiamo F con Fx_1 , allora F è sicuramente nel centro di $B = (K/F, f)$ dal momento che per ogni $a \in F$,

$$x_\sigma a = \sigma(a)x_\sigma = ax_\sigma.$$

Inoltre $K = C_B(K)$; infatti sia $C_B(K) \ni b = \sum_{\sigma \in G} k_\sigma x_\sigma$, allora

$$\begin{aligned} \sum_{\sigma \in G} k k_\sigma x_\sigma &= k b \\ &= b k \\ &= \sum_{\sigma \in G} k_\sigma x_\sigma k \\ &= \sum_{\sigma \in G} k_\sigma \sigma(k) x_\sigma \\ 0 &= \sum_{\sigma \in G} (\sigma(k) - k) k_\sigma x_\sigma \end{aligned}$$

da cui $k_\sigma = 0$ per ogni $\sigma \neq 1$ e quindi $b = k_1 x_1 \in K$, cioè $C_B(K) \subset K$. L'inclusione $K \subset C_B(K)$ è ovvia, abbiamo quindi l'uguaglianza; questo ci dice, per 1.4.11, che K è un sottocampo massimale. Sia ora y nel centro di B ; chiaramente y deve commutare con K , quindi $y \in C_B(K) = K$. D'altra parte gli elementi di K che commutano con tutti gli x_σ sono esattamente gli elementi fissati da G , cioè F , quindi abbiamo che $y \in F$. L'altra inclusione l'avevamo già vista, quindi F è proprio il centro di B .

Per vedere che B è semplice, osserviamo innanzitutto che ogni x_σ è invertibile; consideriamo allora un ideale $U \neq 0$ di B . Sia $U \ni u \neq 0$, $u = \sum_{\sigma \in G} k_\sigma x_\sigma$ di lunghezza minima in U . Moltiplicando a destra per un qualche x_σ^{-1} possiamo supporre $k_1 \neq 0$. Per ogni $k \in K$, $uk - ku \in U$, ma

$$uk - ku = \sum_{\sigma \in G} (\sigma(k) - k) k_\sigma x_\sigma \in U.$$

Dal momento che, per $\sigma = 1$, $\sigma(k) - k = 0$, si ha che $uk - ku$ è un elemento di U di lunghezza minore di u . Quindi

$$0 = uk - ku = \sum_{\sigma \in G} (\sigma(k) - k) k_\sigma x_\sigma \quad \text{per ogni } k \in K,$$

cioè $k_\sigma = 0$ per $\sigma \neq 1$. Dunque $u = x_1 k_1 \in U$, con $k_1 \neq 0$, quindi u è invertibile e $U = B$.

Vediamo ora di dimostrare l'ultima affermazione. Per 1.6.1, sappiamo che per ogni A algebra centrale semplice su F possiamo sempre trovare una B , con $[A] = [B]$ in $\text{Br}(F)$, tale che B ha un sottocampo massimale K ; con K/F estensione di Galois, e con $[B : F] = [K : F]^2$. Ora vediamo che una tale algebra B può essere scritta come prodotto incrociato.

Per ogni $\sigma \in G = \text{Gal}(K/F)$, per il teorema di Noether-Skolem (1.4.2), esiste $x_\sigma \in B$ tale che

$$\sigma(k) = x_\sigma k x_\sigma^{-1} \quad \text{cioè} \quad x_\sigma k = \sigma(k) x_\sigma \quad \text{per ogni } k \in K.$$

Inoltre osserviamo che se $h = \sigma(k)$, si ha

$$\sigma(k) = x_\sigma k x_\sigma^{-1} \quad \text{cioè} \quad x_\sigma^{-1} h = \sigma^{-1}(h) x_\sigma^{-1}.$$

Ora vogliamo vedere che $\{x_\sigma\}_{\sigma \in G}$ sono linearmente indipendenti su K , lo facciamo per induzione. Innanzitutto, se $|G| \geq 2$, abbiamo che per ogni $\sigma, \tau \in G$, $\sigma \neq \tau$, x_σ e x_τ sono linearmente indipendenti.

Infatti, se così non fosse, avremmo $x_\sigma = k_\tau x_\tau$, con $K \ni k_\tau \neq 0$ cioè

$$\begin{aligned} \sigma(k)x_\sigma &= x_\sigma k \\ &= k_\tau x_\tau k \\ &= k_\tau \tau(k)x_\tau \\ &= \tau(k)k_\tau x_\tau \\ &= \tau(k)x_\sigma \quad \text{per ogni } k \in K, \end{aligned}$$

da cui la contraddizione perchè $\sigma \neq \tau$. Ora, supponiamo per ipotesi induttiva che ogni volta che abbiamo n elementi $\{x_{\sigma_i}\}_{1 \leq i \leq n}$ con $\sigma_i \neq \sigma_j$ per $i \neq j$ questi siano linearmente indipendenti e che invece esistano $n+1$ elementi linearmente dipendenti $\{x_{\sigma_i}\}_{1 \leq i \leq n+1}$ con $\sigma_i \neq \sigma_j$ per $i \neq j$. Senza perdere di generalità, scriviamo allora

$$x_{\sigma, n+1} = \sum_{i=1}^n k_i x_{\sigma_i} \quad \text{cioè} \quad 1 = \sum_{i=1}^n k_i x_{\sigma_i} (x_{\sigma, n+1})^{-1}$$

quindi per ogni $k \in K$ si ha

$$\begin{aligned} k \left(\sum_{i=1}^n k_i x_{\sigma_i} (x_{\sigma, n+1})^{-1} \right) &= \left(\sum_{i=1}^n k_i x_{\sigma_i} (x_{\sigma, n+1})^{-1} \right) k \\ &= \sum_{i=1}^n k_i (\sigma_i(\sigma_{n+1}^{-1}(k)) - k) x_{\sigma_i} (x_{\sigma, n+1})^{-1} \\ &= \sum_{i=1}^n k_i (\sigma_i(\sigma_{n+1}^{-1}(k)) - k) x_{\sigma_i} \quad \text{per ogni } k \in K \end{aligned}$$

ma $\sigma_i \sigma_{n+1}^{-1}$ è sempre diverso dall'identità; questa uguaglianza ci dice quindi che $\{x_{\sigma_i}\}_{1 \leq i \leq n}$ sono linearmente dipendenti, il che contraddice l'ipotesi induttiva.

Abbiamo dimostrato che $\{x_\sigma\}_{\sigma \in G}$ sono linearmente indipendenti su K , e questo implica che la dimensione su F del K -spazio generato dagli $\{x_\sigma\}_{\sigma \in G}$ è proprio $|G|^2$, quindi è tutta B . Abbiamo allora $B = \left\{ \sum_{\sigma \in G} k_\sigma x_\sigma \mid k_\sigma \in K \right\}$.

Siano ora $\sigma, \tau \in G$, $k \in K$; allora

$$\begin{aligned} x_\sigma x_\tau x_{\sigma\tau}^{-1} k &= x_\sigma x_\tau (\sigma\tau)^{-1}(k) x_{\sigma\tau}^{-1} \\ &= x_\sigma x_\tau \tau^{-1}(\sigma^{-1}(k)) x_{\sigma\tau}^{-1} \\ &= \sigma(\tau(\tau^{-1}(\sigma^{-1}(k)))) x_\sigma x_\tau x_{\sigma\tau}^{-1} \\ &= k x_\sigma x_\tau x_{\sigma\tau}^{-1} \end{aligned}$$

Questo dice che $f(\sigma, \tau) := x_\sigma x_\tau x_{\sigma\tau}^{-1} \in C_B(K) = K$, cioè che

$$x_\sigma x_\tau = f(\sigma, \tau) x_{\sigma\tau} \quad \text{con} \quad f(\sigma, \tau) \in K^*.$$

Per concludere la dimostrazione del teorema, basta dimostrare che f è un factor set, ma poichè B è un'algebra associativa, si ha

$$x_\sigma(x_\tau x_\nu) = (x_\sigma x_\tau) x_\nu;$$

da cui

$$\begin{aligned} x_\sigma f(\tau, \nu) x_{\tau\nu} &= f(\sigma, \tau) x_{\sigma\tau} x_\nu \\ \sigma(f(\tau, \nu)) x_\sigma x_{\tau\nu} &= f(\sigma, \tau) f(\sigma\tau, \nu) x_{\sigma\tau\nu} \\ \sigma(f(\tau, \nu)) f(\sigma, \tau\nu) x_{\sigma\tau\nu} &= f(\sigma, \tau) f(\sigma\tau, \nu) x_{\sigma\tau\nu} \\ \sigma(f(\tau, \nu)) f(\sigma, \tau\nu) &= f(\sigma, \tau) f(\sigma\tau, \nu). \end{aligned}$$

Per cui f è proprio un factor set. □

Adesso vogliamo arrivare ad un risultato che lega più strettamente i factor set e le classi di equivalenza dei prodotti incrociati, innanzitutto osserviamo che i factor set formano un gruppo.

Proposizione 1.6.11. *Sia K un campo e sia G un gruppo. Se $f, g : G \times G \rightarrow K^*$ sono due factor set, definiamo in modo naturale il prodotto*

$$(fg)(\sigma, \tau) = f(\sigma, \tau)g(\sigma, \tau).$$

L'insieme dei factor set, con il prodotto così definito, è un gruppo abeliano che indichiamo con $Z^2(G, K^)$.*

Dimostrazione. Innanzitutto vediamo che fg è ancora un factor set;

$$\begin{aligned} (fg)(\sigma\tau, \nu)(fg)(\sigma, \tau) &= f(\sigma\tau, \nu)g(\sigma\tau, \nu)f(\sigma, \tau)g(\sigma, \tau) \\ &= f(\sigma, \tau\nu)f(\sigma, \tau)g(\sigma\tau, \nu)g(\sigma, \tau) \\ &= f(\sigma, \tau\nu)\sigma(f(\tau, \nu))g(\sigma, \tau\nu)\sigma(g(\tau, \nu)) \\ &= (fg)(\sigma, \tau\nu)\sigma((fg)(\tau, \nu)). \end{aligned}$$

E' evidente che il prodotto è commutativo; l'elemento neutro di questo gruppo è semplicemente il factor set 1 definito da

$$1(\sigma, \tau) \equiv 1 \quad \text{per ogni } \sigma, \tau \in G,$$

che è un factor set perché

$$1(\sigma\tau, \nu)1(\sigma, \tau) = 1 \cdot 1 = 1 \cdot \sigma(1) = 1(\sigma, \tau\nu)\sigma(1(\tau, \nu)).$$

Per concludere verifichiamo che, dato un factor set f , si ha che il suo inverso

$$f^{-1}(\sigma, \tau) := (f(\sigma, \tau))^{-1},$$

è ancora un factor set. In effetti

$$\begin{aligned} f^{-1}(\sigma\tau, \nu)f^{-1}(\sigma, \tau) &= (f(\sigma\tau, \nu)f(\sigma, \tau))^{-1} \\ &= (f(\sigma, \tau\nu)\sigma(f(\tau, \nu)))^{-1} \\ &= f^{-1}(\sigma, \tau\nu)\sigma(f^{-1}(\tau, \nu)). \end{aligned}$$

□

Osservazione 1.6.12. All'interno di $Z^2(G, K^*)$, i factor set equivalenti ad 1, che sono detti *principali*, ne formano un sottogruppo, che indichiamo con $B^2(G, K^*)$.

In effetti 1 è equivalente a sé stesso, poi se f e g sono equivalenti ad 1 si ha

$$f(\sigma, \tau) = \sigma(\lambda_\tau)\lambda_\sigma\lambda_{\sigma\tau}^{-1} \quad \text{e} \quad g(\sigma, \tau) = \sigma(\mu_\tau)\mu_\sigma\mu_{\sigma\tau}^{-1},$$

da cui

$$(fg)(\sigma, \tau) = \sigma(\lambda_\tau\mu_\tau)\lambda_\sigma\mu_\sigma(\lambda_{\sigma\tau}\mu_{\sigma\tau})^{-1} = \sigma(\rho_\tau)\rho_\sigma\rho_{\sigma\tau}^{-1},$$

dove $\rho = \lambda\mu$; quindi fg è ancora equivalente ad 1.

Infine, se f è come sopra,

$$f^{-1}(\sigma, \tau) = (\sigma(\lambda_\tau)\lambda_\sigma)^{-1}\lambda_{\sigma\tau} = \sigma(\mu_\tau)\mu_\sigma\mu_{\sigma\tau}^{-1},$$

con $\mu = \lambda^{-1}$.

Ora, è evidente che due factor set f e g sono equivalenti se e solo se $fg^{-1} \in B^2(G, K^*)$.

Definizione 1.6.13. Definiamo il *secondo gruppo di coomologia* di G a coefficienti in K^*

$$H^2(G, K^*) = Z^2(G, K^*)/B^2(G, K^*).$$

Per adesso limitiamoci ad osservare che, per 1.6.8 gli elementi di $H^2(G, K^*)$ sono in corrispondenza biunivoca con le classi di isomorfismo di $(K/F, f)$.

Proposizione 1.6.14. *Sia K/F un'estensione di Galois, $[K : F] = n$. Allora*

$$(K/F, 1) \simeq M_n(F).$$

Dimostrazione. Chiamiamo $A := (K/F, 1)$, allora $[A : F] = n^2$, inoltre A ha K come sottocampo ed esistono $\{x_\sigma\}_{\sigma \in G} \subset A$ tali che

$$x_\sigma k = \sigma(k)x_\sigma \quad \text{e} \quad x_\sigma x_\tau = x_{\sigma\tau}.$$

Facciamo agire a sinistra A su K in questo modo: se $A \ni x = \sum_{\sigma \in G} k_\sigma x_\sigma$ e $k \in K$, definiamo

$$T_x k = \sum_{\sigma \in G} k_\sigma \sigma(k).$$

Abbiamo che $T_x \in \text{End}_F(K)$; infatti se $k, h \in K$, $\alpha, \beta \in F$ si ha

$$\begin{aligned} T_x(\alpha k + \beta h) &= \sum_{\sigma \in G} k_\sigma \sigma(\alpha k + \beta h) \\ &= \sum_{\sigma \in G} k_\sigma (\alpha \sigma(k) + \beta \sigma(h)) \\ &= \alpha \sum_{\sigma \in G} k_\sigma \sigma(k) + \beta \sum_{\sigma \in G} k_\sigma \sigma(h) \\ &= \alpha(T_x k) + \beta(T_x h). \end{aligned}$$

La mappa $T : A \rightarrow \text{End}_F(K)$ definita da $x \mapsto T_x$ è un omomorfismo di anelli; infatti siano $x = \sum_{\sigma \in G} k_\sigma x_\sigma$ e $y = \sum_{\sigma \in G} x_\sigma h_\sigma$; abbiamo

$$x + y = \sum_{\sigma \in G} (k_\sigma + h_\sigma) x_\sigma$$

da cui

$$\begin{aligned} T_{x+y}k &= \sum_{\sigma \in G} (k_\sigma + h_\sigma) \sigma(k) \\ &= \sum_{\sigma \in G} k_\sigma \sigma(k) + \sum_{\sigma \in G} h_\sigma \sigma(k) \\ &= T_x k + T_y k \\ &= (T_x + T_y)k. \end{aligned}$$

Abbiamo poi $T_1 = x_1$; quindi $T_1 k = k$. Infine

$$\begin{aligned} xy &= \left(\sum_{\sigma \in G} k_\sigma x_\sigma \right) \left(\sum_{\tau \in G} h_\tau x_\tau \right) \\ &= \sum_{\sigma, \tau \in G} k_\sigma x_\sigma h_\tau x_\tau \\ &= \sum_{\sigma, \tau \in G} k_\sigma \sigma(h_\tau) x_\sigma x_\tau \\ &= \sum_{\sigma, \tau \in G} k_\sigma \sigma(h_\tau) x_{\sigma\tau}, \end{aligned}$$

per cui

$$\begin{aligned} T_{xy}k &= \sum_{\sigma, \tau \in G} k_\sigma \sigma(h_\tau) \sigma(\tau(k)) \\ &= \sum_{\sigma \in G} k_\sigma \sigma \left(\sum_{\tau \in G} h_\tau \tau(k) \right) \\ &= T_x T_y k. \end{aligned}$$

Dal momento che A è semplice, questo morfismo è iniettivo; inoltre, siccome A è di dimensione n^2 su F , così come $\text{End}_F(K)$, dev'essere anche suriettivo. Quindi T è un isomorfismo. Per concludere

$$(K/F, 1) \simeq \text{End}_F(K) \simeq M_n(F).$$

□

Lemma 1.6.15. *Sia A algebra centrale semplice su F , e sia $A \ni e \neq 0$ un idempotente, allora in $\text{Br}(F)$ si ha $[A] = [eAe]$.*

Dimostrazione. Per il teorema di Wedderburn (1.1.13), abbiamo $A = M_n(D)$ e $[A] = [D]$. Attraverso un cambio di basi, cioè un automorfismo interno di A , possiamo assumere che

$$e = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

dove I_r è la matrice identità $r \times r$. Quindi

$$eAe = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} M_n(D) \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} M_r(D) & 0 \\ 0 & 0 \end{pmatrix},$$

da cui $eAe \simeq M_r(D)$ e così $[eAe] = [D] = [A]$. □

Ecco finalmente il risultato fondamentale che lega il prodotto dei factor set con il prodotto nel gruppo di Brauer.

Teorema 1.6.16. *Sia K estensione di Galois di F , $G = \text{Gal}(K/F)$ e siano $f, g : G \times G \rightarrow K^*$ due factor set. Allora*

$$[(K/F, f)][(K/F, g)] = [(K/F, fg)]$$

Dimostrazione. Sia $(K/F, f) = A = \sum_{\sigma \in G} Kx_\sigma$ e sia $(K/F, g) = B = \sum_{\tau \in G} Ky_\tau$; dove x_σ e y_τ sono come al solito gli elementi che inducono gli automorfismi $\sigma, \tau \in G$ tramite il coniugio e si moltiplicano secondo i factor set f e g .

Sia $C = A \otimes_F B$; allora C è un algebra centrale semplice su F . Vogliamo trovare un idempotente $e \in K \otimes_F K \subset C$, tale che $eCe \simeq (K/F, fg)$. Questo proverà il risultato, dato che, per il lemma appena visto, $[C] = [eCe]$.

Per cominciare, osserviamo che la moltiplicazione in $K \otimes_F K$ è commutativa. Dal momento che K è separabile su F , esiste $a \in K$ tale che $K = F(a)$

e, se $p(x)$ è il polinomio minimo di a su F , $\deg p(x) = n = [K : F]$. Ora definiamo

$$e = \frac{\prod_{\nu \in G \setminus \{1\}} (a \otimes 1 - 1 \otimes \nu(a))}{\prod_{\nu \in G \setminus \{1\}} (a - \nu(a)) \otimes 1}.$$

Notiamo che il denominatore è diverso da 0 perchè $a \neq \nu(a)$ per ogni $\nu \neq 1$ e il numeratore è anch'esso diverso da 0 perchè gli elementi $\{a^r \otimes 1\}_{0 \leq r \leq n-1}$ sono linearmente indipendenti su $1 \otimes K$. Quindi $K \otimes_F K \ni e \neq 0$.

Ora osserviamo che

$$p(X) = (X - a) \prod_{\nu \in G \setminus \{1\}} (X - \nu(a)),$$

quindi si ha, identificando a con $1 \otimes a$,

$$\begin{aligned} (a \otimes 1)e - e(1 \otimes a) &= \frac{(a \otimes 1 - 1 \otimes a) \prod_{\nu \in G \setminus \{1\}} (a \otimes 1 - 1 \otimes \nu(a))}{\prod_{\nu \in G \setminus \{1\}} (a - \nu(a)) \otimes 1} \\ &= \frac{p(a \otimes 1)}{\prod_{\nu \in G \setminus \{1\}} (a - \nu(a)) \otimes 1} \\ &= 0. \end{aligned}$$

Per cui $(1 \otimes a)e = (a \otimes 1)e \in K \otimes_F K$; vediamo per induzione che

$$(1 \otimes a^r)e = (a^r \otimes 1)e \quad \text{per ogni } r \geq 1.$$

Supponiamo sia vero per $(1 \otimes a^i)$, con $1 \leq i \leq r-1$; allora

$$\begin{aligned} (1 \otimes a^r)e &= (1 \otimes a^{r-1})(1 \otimes a)e \\ &= (1 \otimes a^{r-1})(a \otimes 1)e \\ &= (1 \otimes a^{r-1})e(a \otimes 1) \\ &= (a^{r-1} \otimes 1)e(a \otimes 1) \\ &= (a^r \otimes 1)e. \end{aligned}$$

Quindi, visto che possiamo scrivere $K \ni x = \sum_{r=0}^{n-1} x_r a^r$, abbiamo, per ogni

$x \in K$,

$$\begin{aligned} (x \otimes 1)e &= \sum_{r=0}^{n-1} x_r(a^r \otimes 1)e \\ &= \sum_{r=0}^{n-1} x_r(1 \otimes a^r)e \\ &= (1 \otimes x)e \end{aligned}$$

e, per la commutatività del prodotto, anche

$$e(x \otimes 1) = (x \otimes 1)e = (1 \otimes x)e = e(1 \otimes x). \quad (1.8)$$

Da cui si ottiene

$$\begin{aligned} e^2 &= e \frac{\prod_{\nu \in G \setminus \{1\}} (a \otimes 1 - 1 \otimes \nu(a))}{\prod_{\nu \in G \setminus \{1\}} (a - \nu(a)) \otimes 1} \\ &= e \frac{\prod_{\nu \in G \setminus \{1\}} (a \otimes 1 - \nu(a) \otimes 1)}{\prod_{\nu \in G \setminus \{1\}} (a - \nu(a)) \otimes 1} \\ &= e \frac{\prod_{\nu \in G \setminus \{1\}} (a - \nu(a)) \otimes 1}{\prod_{\nu \in G \setminus \{1\}} (a - \nu(a)) \otimes 1} \\ &= e \end{aligned}$$

che è quindi idempotente.

Ci resta da mostrare che $eCe \simeq (K/F, fg)$, abbiamo

$$\begin{aligned} eCe &= e \left(\sum_{\sigma \in G} Kx_\sigma \right) \otimes_F \left(\sum_{\tau \in G} Ky_\tau \right) e \\ &= \sum_{\sigma, \tau \in G} e(K \otimes K)(x_\sigma \otimes y_\tau)e \\ &= \sum_{\sigma, \tau \in G} e^2(K \otimes 1)(1 \otimes K)(x_\sigma \otimes y_\tau)e \\ &= \sum_{\sigma, \tau \in G} e(K \otimes 1)e(1 \otimes K)(x_\sigma \otimes y_\tau)e \\ &= \sum_{\sigma, \tau \in G} e(K \otimes 1)ee(1 \otimes K)ee(x_\sigma \otimes y_\tau)e. \end{aligned}$$

Ma, $e(1 \otimes K)e = e(K \otimes 1)e$ per (1.8), inoltre $e(K \otimes 1)e = K'$ è un campo isomorfo a K . Ci rimane da calcolare cos'è $e(x_\sigma \otimes y_\tau)e$,

$$\begin{aligned} e(x_\sigma \otimes y_\tau)e &= \frac{\prod_{\nu \in G \setminus \{1\}} (a \otimes 1 - 1 \otimes \nu(a))}{\prod_{\nu \in G \setminus \{1\}} (a - \nu(a)) \otimes 1} (x_\sigma \otimes y_\tau)e \\ &= (x_\sigma \otimes y_\tau) \frac{\prod_{\nu \in G \setminus \{1\}} (\sigma(a) \otimes 1 - 1 \otimes \tau(\nu(a)))}{\prod_{\nu \in G \setminus \{1\}} (\sigma(a) - \sigma(\nu(a))) \otimes 1} e \\ &= (x_\sigma \otimes y_\tau) \frac{\prod_{\nu \in G \setminus \{1\}} (\sigma(a) \otimes 1 - \tau(\nu(a)) \otimes 1)}{\prod_{\nu \in G \setminus \{1\}} (\sigma(a) - \sigma(\nu(a))) \otimes 1} e \\ &= (x_\sigma \otimes y_\tau) \frac{\prod_{\nu \in G \setminus \{1\}} (\sigma(a) - \tau(\nu(a))) \otimes 1}{\prod_{\nu \in G \setminus \{1\}} (\sigma(a) - \sigma(\nu(a))) \otimes 1} e \end{aligned}$$

Se $\sigma \neq \tau$, allora $\sigma(a) - \tau(\nu(a))$ quando $\nu = \tau^{-1}\sigma$, quindi in tal caso si ha $e(x_\sigma \otimes y_\tau)e = 0$. Invece, quando $\sigma = \tau$, otteniamo

$$e(x_\sigma \otimes y_\sigma)e = (x_\sigma \otimes y_\sigma)e;$$

con un ragionamento analogo si vede che $e(x_\sigma \otimes y_\sigma)e = e(x_\sigma \otimes y_\sigma)$.

Siamo quindi arrivati a mostrare che

$$eCe = \sum_{\sigma \in G} K' w_\sigma,$$

dove $K' = e(K \otimes 1)e \simeq K$ e

$$w_\sigma = e(x_\sigma \otimes y_\sigma)e = e(x_\sigma \otimes y_\sigma) = (x_\sigma \otimes y_\sigma)e.$$

Per concludere vediamo che i w_σ si comportano 'bene'.

Sia $e(k \otimes 1)e \in e(K \otimes 1)e$, $\sigma \in G$ allora

$$\begin{aligned} w_\sigma e(k \otimes 1)e &= e(x_\sigma \otimes y_\sigma) e^2(k \otimes 1)e \\ &= e(x_\sigma \otimes y_\sigma) e(k \otimes 1)e \\ &= e(x_\sigma \otimes y_\sigma)(k \otimes 1)e \\ &= e(x_\sigma k \otimes y_\sigma)e \\ &= e(\sigma(k) x_\sigma \otimes y_\sigma)e \\ &= e(\sigma(k) \otimes 1)(x_\sigma \otimes y_\sigma)e \\ &= e(\sigma(k) \otimes 1) e(x_\sigma \otimes y_\sigma)e \\ &= e(\sigma(k) \otimes 1) e w_\sigma. \end{aligned}$$

E poi

$$\begin{aligned}
w_\sigma w_\tau &= e(x_\sigma \otimes y_\sigma) e e(x_\tau \otimes y_\tau) e \\
&= e(x_\sigma \otimes y_\sigma)(x_\tau \otimes y_\tau) e \\
&= e(x_\sigma x_\tau \otimes y_\sigma y_\tau) e \\
&= e(f(\sigma, \tau) x_{\sigma\tau} \otimes g(\sigma, \tau) y_{\sigma\tau}) e \\
&= e((1 \otimes g(\sigma, \tau))(f(\sigma, \tau) \otimes 1) x_{\sigma\tau} \otimes y_{\sigma\tau}) e \\
&= e(f(\sigma, \tau) g(\sigma, \tau) \otimes 1) e w_{\sigma\tau}.
\end{aligned}$$

Quindi i w_σ inducono gli automorfismi σ tramite il coniugio e si moltiplicano secondo il factor set fg .

In conclusione $eCe \simeq (K'/F, fg)$, il che prova il teorema. \square

Questo teorema ci mostra che $\{(K/F, f) \mid f \in Z^2(G, K^*)\}$ è un sottogruppo di $\text{Br}(F)$, che indichiamo con $\text{Br}(K/F)$, quindi il teorema 1.6.16 ci dice che

$$\text{Br}(K/F) \simeq H^2(\text{Gal}(K/F), K^*).$$

Abbiamo anche notato che ogni classe di $\text{Br}(F)$ si può scrivere come $(K/F, f)$ per un certo K ed un certo f , abbiamo quindi che

$$\text{Br}(F) = \bigcup_{K/F \text{ di Galois}} \text{Br}(K/F).$$

Ora, mettendo insieme queste due osservazioni con il risultato seguente, otterremo un'importante caratteristica del gruppo di Brauer di un campo.

Lemma 1.6.17. *Sia G , un gruppo di ordine $|G|$; allora*

$$H^2(G, K^*)^{|G|} = \{1\}.$$

Dimostrazione. Sia $f \in Z^2(G, K^*)$, cioè un factor set, allora per ogni $\sigma_i \in G$, $1 \leq i \leq 3$ abbiamo

$$f(\sigma_1 \sigma_2, \sigma_3) f(\sigma_1, \sigma_2) = f(\sigma_1, \sigma_2 \sigma_3) \sigma_1(f(\sigma_2, \sigma_3)),$$

cioè

$$f(\sigma_1, \sigma_2) = f(\sigma_1\sigma_2, \sigma_3)^{-1}f(\sigma_1, \sigma_2\sigma_3)\sigma_1(f(\sigma_2, \sigma_3)).$$

Facciamo il prodotto su tutto G , facendo variare $\sigma_3 \in G$ e otteniamo

$$\begin{aligned} f(\sigma_1, \sigma_2)^{|G|} &= \prod_{\sigma_3 \in G} f(\sigma_1, \sigma_2) \\ &= \prod_{\sigma_3 \in G} (f(\sigma_1\sigma_2, \sigma_3)^{-1}f(\sigma_1, \sigma_2\sigma_3)\sigma_1(f(\sigma_2, \sigma_3))). \end{aligned} \quad (1.9)$$

Ora, definiamo

$$\lambda_{\sigma_2} := \prod_{\sigma_3 \in G} f(\sigma_2, \sigma_3),$$

e osserviamo che se σ_3 varia su tutto G , altrettanto fa $\sigma' := \sigma_2\sigma_3$, quindi

$$\prod_{\sigma_3 \in G} f(\sigma_1, \sigma_2\sigma_3) = \prod_{\sigma' \in G} f(\sigma_1, \sigma') = \lambda_{\sigma_1}.$$

Allora (1.9) diventa

$$f(\sigma_1, \sigma_2)^{|G|} = \lambda_{\sigma_1\sigma_2}^{-1}\lambda_{\sigma_1}\sigma_1(\lambda_{\sigma_2}).$$

Quindi $f(\sigma_1, \sigma_2)^{|G|} \in B^2(G, K^*)$.

Abbiamo mostrato che $Z^2(G, K^*)^{|G|} \subset B^2(G, K^*)$, cioè

$$H^2(G, K^*)^{|G|} = \{1\}.$$

□

Teorema 1.6.18. *Sia F un campo, allora $\text{Br}(F)$ è un gruppo di torsione; cioè ogni elemento di $\text{Br}(F)$ ha ordine finito.*

Dimostrazione. Come abbiamo notato prima, se $[A] \in \text{Br}(F)$, allora esiste un K tale che $[A] \in \text{Br}(K/F) = H^2(\text{Gal}(K/F), K^*)$, quindi

$$[A]^{|\text{Gal}(K/F)|} = 1.$$

□

Definizione 1.6.19. Se D è un'algebra di divisione centrale su F , allora $[D : F] = n^2$; definiamo $\text{ind}_F(D) := n$ l'indice di D su F . Se A è un'algebra centrale semplice su F , allora $A \simeq M_n(F) \otimes_F D$ con D algebra di divisione centrale su F ; definiamo quindi $\text{ind}_F(A) := \text{ind}_F(D)$. Definiamo infine $\text{exp}_F(A)$ l'ordine di $[A]$ in $\text{Br}(F)$.

Teorema 1.6.20. Se A è un'algebra centrale semplice su F , allora

$$\text{exp}_F(A) \mid \text{ind}_F(A).$$

Dimostrazione. In $\text{Br}(F)$, $[A] = [D]$ con D algebra di divisione centrale su F . Se K_0 è un sottocampo massimale separabile di D , allora

$$[D : K_0]^2 = n^2 = \text{ind}_F(A)^2 = [D : F].$$

Sia K la chiusura normale di K_0 e supponiamo che $[K : K_0] = q$. Come abbiamo già visto, $D_q := D \otimes_F M_q(F)$ contiene K e $D_q = (K/F, f)$ per un qualche factor set f . Ora, per 1.1.7 e 1.1.15 $D_q = \bigoplus_{j=0}^{q-1} I_j$ dove I_j sono ideali sinistri minimali, quindi hanno dimensione q come spazi vettoriali sinistri su D ; I_j sono anche spazi vettoriali su K . Dal momento che

$$[I_j : K]q = [D_q : K] = [K : F] = qn$$

abbiamo che $[I_j : K] = n = \text{ind}_F(A)$.

Siano $x_\sigma \in D_q = (K/F, f)$ tali che $x_\sigma k = \sigma(k)x_\sigma$ per ogni $k \in K$ e $x_\sigma x_\tau = f(\sigma, \tau)x_{\sigma\tau}$. Dal momento che I_1 è un ideale sinistro, $x_\tau I_1 \subset I_1$, quindi x_τ induce un endomorfismo T_τ di I_1 . Se $\{u_1, \dots, u_n\}$ è una base di I_1 su K , allora

$$T_\tau u_i = \sum_j t_{ij\tau} u_j \quad \text{con } t_{ij\tau} \in K,$$

dove $T_\tau = (t_{ij\tau}) \in M_n(K)$. Ora

$$T_\sigma T_\tau u_i = T_\sigma \left(\sum_j t_{ij\tau} u_j \right) = \sum_j \sigma(t_{ij\tau}) T_\sigma u_j.$$

Dal momento che $T_\sigma T_\tau = f(\sigma, \tau) T_{\sigma\tau}$ abbiamo che $f(\sigma, \tau) T_{\sigma\tau} = \sigma(T_\tau) T_\sigma$. Sia $\lambda_\sigma := \det T_\sigma$; allora $f(\sigma, \tau)^n \lambda_{\sigma, \tau} = \sigma(\lambda_\tau) \lambda_\sigma$, quindi $f(\sigma, \tau)^n$ è un factor set principale. In conclusione

$$[A]^{\text{ind}_F(A)} = [(K/F, f)]^n = [(K/F, f^n)] = [F] \quad \text{in } \text{Br}(F)$$

quindi l'ordine di $[A]$ in $\text{Br}(F)$ divide $\text{ind}_F(A)$. \square

Enunciamo ora un risultato che ci servirà in seguito, ma senza dimostrarlo. Una dimostrazione si può trovare in [6], cap.7 §29.

Teorema 1.6.21. *Siano $F \subset K \subset L$ campi, con K/F e L/F estensioni di Galois; siano $G = \text{Gal}(L/F)$, $H = \text{Gal}(L/K)$ e $\bar{G} = G/H = \text{Gal}(L/K)$. Sia $f : \bar{G} \times \bar{G} \rightarrow K^*$ un factor set, definiamo un factor set $g : G \times G \rightarrow K^* \subset L^*$ tramite*

$$g(\sigma, \tau) = f(\bar{\sigma}, \bar{\tau}) \quad \sigma, \tau \in G$$

dove $\bar{\sigma}$ e $\bar{\tau}$ sono le immagini di σ e tau in \bar{G} . Allora si ha

$$[(K/F, f)] = [(L/F, g)] \quad \text{in } \text{Br}(F).$$

1.7 Algebre Cicliche

Definizione 1.7.1. Sia K un'estensione di Galois del campo F ; diciamo che K/F è *ciclica* se $\text{Gal}(K/F)$ è un gruppo ciclico.

Definizione 1.7.2. Sia K/F un'estensione ciclica, con $\text{Gal}(K/F) = \langle \sigma \rangle$ di ordine n ; sia $a \in F^*$. Definiamo formalmente un'algebra ciclica $A = (K/F, \sigma, a)$ con $A = \left\{ \sum_{i=0}^{n-1} k_i u^i \mid k_i \in K \right\}$ analogamente a come abbiamo definito i prodotti incrociati. Il simbolo u ha le seguenti proprietà:

1. $uk = \sigma(k)u$ per ogni $k \in K$
2. $u^n = a$.

In questa definizione identifichiamo u^0 con l'elemento unità di A .

Possiamo facilmente vedere che A è un prodotto incrociato: se prendiamo $x_{\sigma^i} = u^i$ abbiamo $A \simeq (K/F, f)$ dove il factor set f è dato da

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{se } i + j < n \\ a & \text{se } i + j \geq n, \quad 0 \leq i, j \leq n-1 \end{cases}.$$

E' vero anche il viceversa.

Proposizione 1.7.3. Sia K/F un'estensione ciclica con $\text{Gal}(K/F) = \langle \sigma \rangle$, di ordine n . Sia $A = (K/F, f)$ un prodotto incrociato dove f è un factor set normalizzato. Allora

$$(K/F, f) \simeq (K/F, \sigma, a) \quad \text{dove} \quad a = \prod_{i=0}^{n-1} f(\sigma^i, \sigma) \in F^*.$$

Dimostrazione. Scriviamo $A = \sum_{i=0}^{n-1} Kx_{\sigma^i}$ con

$$x_{\sigma^i}k = \sigma^i(k)x_{\sigma^i} \quad \text{e} \quad x_{\sigma^i}x_{\sigma^j} = f(\sigma^i, \sigma^j)x_{\sigma^{i+j}} \quad \text{per } 0 \leq i, j \leq n-1.$$

Abbiamo allora

$$x_{\sigma}^2 = x_{\sigma}x_{\sigma} = f(\sigma, \sigma)x_{\sigma^2}, \quad x_{\sigma}^3 = (f(\sigma, \sigma)x_{\sigma^2})x_{\sigma} = f(\sigma, \sigma)f(\sigma^2, \sigma)x_{\sigma^3},$$

fino a

$$x_\sigma^n = ax_{\sigma^n} = a.$$

Abbiamo allora $A = \sum_{i=0}^{n-1} Kx_\sigma^i$ con

$$x_\sigma k = \sigma(k)x_\sigma \quad \text{e} \quad x_\sigma^n = a,$$

ma dal momento che x_σ^n sta nel centro di A , abbiamo appunto $a \in F^*$. \square

Teorema 1.7.4. *Sia K/F un'estensione ciclica, con $\text{Gal}(K/F) = \langle \sigma \rangle$ di ordine n ; siano $a, b \in F^*$. Allora*

1. $(K/F, \sigma, a) \simeq (K/F, \sigma^s, a^s)$ per ogni $s \in \mathbb{Z}$ tale che $(s, n) = 1$.
2. $(K/F, \sigma, 1) \simeq M_n(F)$.
3. $(K/F, \sigma, a) \simeq (K/F, \sigma, b)$ se e solo se $b = (N_{K/F} c)a$ con $c \in K^*$.
4. $[(K/F, \sigma, a)][(K/F, \sigma, b)] = [(K/F, \sigma, ab)]$ in $\text{Br}(F)$.

Dimostrazione. Per dimostrare (1), scriviamo $A = (K/F, \sigma, a) = \sum_{i=0}^{n-1} Ku^i$ con $uk = \sigma(k)u$, per ogni $k \in K$, e $u^n = a$. Se $(s, n) = 1$ allora $\text{Gal}(K/F) = \langle \sigma^s \rangle$ e possiamo scrivere

$$A = \sum_{i=0}^{n-1} Kw^i, \quad \text{con} \quad w = u^s.$$

Per concludere, osserviamo che

$$wk = u^s k = \sigma^s(u)u^s = \sigma^s(u)w \quad \text{e} \quad w^n = u^{sn} = a^s.$$

L'affermazione (2) è un caso particolare di 1.6.14; vediamo allora (3). Innanzitutto, se $c \in K^*$, abbiamo

$$A = \sum_{i=0}^{n-1} Ku^i = \sum_{i=0}^{n-1} K(cu)^i$$

e $(cu)k = c\sigma(k)u = \sigma(k)cu$, $(cu)^n = cucu \cdots cu = (c)c\sigma(c) \cdots u^n \sigma^{n-1} = N_{K/F} ca$. Quindi $A \simeq (K/F, \sigma, (N_{K/F} c)a)$. Viceversa, sia ora

$$B = (K/F, \sigma, b) = \sum_{i=0}^{n-1} K v^i$$

con $vk = \sigma(k)v$ e $v^n = b$ e supponiamo $A \simeq B$. Sia $\psi : B \rightarrow A$ un F -isomorfismo, allora, per lo stesso ragionamento nella dimostrazione di 1.6.8 (a cui possiamo ricondurci vedendo A e B come prodotti incrociati), dobbiamo avere $\psi(v) = cu$ con $c \in K^*$. Quindi

$$\begin{aligned} b &= \psi(b) \\ &= \psi(v^n) \\ &= \psi(v)^n \\ &= (cu)^n \\ &= N_{K/F} ca. \end{aligned}$$

Infine, per dimostrare (4), basta usare 1.6.16 osservando che se vediamo $A = (K/F, \sigma, a)$ e $B = (K/F, \sigma, b)$ come prodotti incrociati abbiamo $A = (K/F, f)$ e $B = (K/F, g)$ con

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{se } i+j < n \\ a & \text{se } i+j \geq n \end{cases}, \quad g(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{se } i+j < n \\ b & \text{se } i+j \geq n \end{cases},$$

e quindi

$$fg(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{se } i+j < n \\ ab & \text{se } i+j \geq n, \quad 0 \leq i, j \leq n-1 \end{cases},$$

da cui $(K/F, fg) = (K/F, \sigma, ab)$. \square

Teorema 1.7.5. *Siano $F \subset K \subset L$ campi, con K/F e L/F estensioni di Galois, dove $G = \text{Gal}(L/F) = \langle \sigma \rangle$ è ciclico di ordine t . Siano $H = \text{Gal}(L/K)$, $\bar{G} = G/H = \text{Gal}(L/K) = \langle \bar{\sigma} \rangle$, dove $\bar{\sigma}$ è l'immagine di σ in \bar{G} . Allora, per ogni $a \in F^*$,*

$$[(K/F, \bar{\sigma}, a)] = [(L/F, \sigma, a^{[L:K]})] \quad \text{in } \text{Br}(F).$$

Dimostrazione. Sia $A = (K/F, \bar{\sigma}, a) = (K/F, f)$ dove

$$f(\bar{\sigma}^i, \bar{\sigma}^j) = \begin{cases} 1 & \text{se } i + j < n \\ a & \text{se } i + j \geq n, \quad 0 \leq i, j \leq n - 1 \end{cases},$$

dove $n = [K : F]$. In $\text{Br}(F)$ abbiamo $[A] = [(L/F, g)]$ con g definito in 1.6.21, ma per 1.7.3, si ha

$$(L/F, g) \simeq (L/F, \sigma, b) \quad \text{con } b = \prod_{j=0}^{t-1} g(\sigma^j, \sigma).$$

Ora, se $s := [L : K]$, si ha $t = [L : F] = [L : K][K : F] = sn$; inoltre per $0 \leq j \leq t - 1$ abbiamo

$$g(\sigma^j, \sigma) = f(\bar{\sigma}^j, \bar{\sigma}) = \begin{cases} a & \text{se } j = n - 1, 2n - 1, \dots, sn - 1; \\ 1 & \text{altrimenti.} \end{cases}$$

In conclusione $b = a^s$. □

Capitolo 2

Campi Locali

2.1 Anelli di valutazione discreta e domini di Dedekind

Definizione 2.1.1. Un anello A è detto *anello di valutazione discreta* se è un dominio a ideali principali che possiede uno ed un solo ideale primo $P \neq 0$. Il campo quoziente A/P si chiama *campo dei residui* di A .

Gli elementi invertibili di A sono gli elementi di $A \setminus P$. In un PID gli ideali primi non nulli sono della forma πA con π elemento irriducibile, quindi la definizione precedente equivale a dire che A possiede un solo elemento irriducibile a meno di moltiplicazione per un invertibile. Gli ideali non nulli di A sono della forma $P^n = \pi^n A$, dove π è un irriducibile; se $0 \neq x \in A$, possiamo scrivere

$$x = \pi^n u \quad \text{con } n \in \mathbb{N}, u \in A^* \quad (2.1)$$

questo n è detto la *valutazione* di x e si indica con $v(x)$; non dipende dalla scelta di π . Come convenzione si pone $v(0) = +\infty$.

Sia F il campo dei quozienti di A ; se $x = \frac{a}{b} \in F^*$, si può ancora scrivere

$$x = \pi^n u \quad \text{però con } n \in \mathbb{Z}, u \in F^* \quad (2.2)$$

e porre $v(x) = n$. Si vede chiaramente che A è determinato da v , infatti $A = \{x \in F \mid v(x) \geq 0\}$ e $P = \{x \in F \mid v(x) > 0\}$.

Definizione 2.1.2. Sia F un campo; un applicazione $v : F^* \rightarrow \mathbb{Z}$ è detta una *valutazione discreta* se v è un omomorfismo suriettivo e vale

$$v(x + y) \geq \min(v(x), v(y)) \quad \text{per ogni } x, y \in F^*. \quad (2.3)$$

Osservazione 2.1.3. Se F è il campo dei quozienti di un anello di valutazione discreta, allora v , come l'abbiamo definita in (2.2), è una valutazione discreta.

Vale anche il viceversa.

Proposizione 2.1.4. *Sia F un campo e sia $v : F^* \rightarrow \mathbb{Z}$ una valutazione discreta. Allora $A := \{x \in F \mid v(x) \geq 0\}$ è un anello di valutazione discreta, e v è la valutazione definita in (2.1). A volte ci riferiremo ad A come l'anello di v .*

Dimostrazione. Innanzitutto A è un gruppo additivo per la proprietà (2.3). Abbiamo poi che $1 \in A$, perché $v(1) = 0$; inoltre A è chiuso rispetto alla moltiplicazione perché se $v(x), v(y) \geq 0$, allora

$$v(xy) = v(x) + v(y) \geq 0.$$

Visto che $v(x^{-1}) = -v(x)$, gli elementi invertibili di A sono tutti e soli gli $x \in A$ con $v(x) = 0$. Ora scegliamo un $\pi \in A$ tale che $v(\pi) = 1$; per ogni $x \in A$, se $v(x) = n$ abbiamo

$$v(x\pi^{-n}) = v(x) - v(\pi^n) = n - nv(\pi) = 0$$

da cui $x = \pi^n u$ con u invertibile. Quindi abbiamo visto che ogni ideale non nullo di A è della forma $\pi^n A$, con $n \geq 0$, e questo fa sì che A sia un anello di valutazione discreta. \square

Definizione 2.1.5. Un anello A è detto *locale* se possiede un solo ideale massimale.

Proposizione 2.1.6. *Sia A un dominio d'integrità. Allora A è un anello di valutazione discreta se e solo se A è un anello locale noetheriano, tale che il suo ideale massimale sia generato da un elemento non nilpotente.*

Dimostrazione. E' chiaro che un anello di valutazione discreta verifica le suddette proprietà. Viceversa, supponiamo che A verifichi queste proprietà e sia π un generatore dell'ideale massimale M .

Vogliamo ora dimostrare che $\bigcap_{n \geq 0} M^n = 0$; sia $y \in \bigcap_{n \geq 0} M^n$, allora per ogni $n \geq 0$ possiamo scrivere $y = \pi^n x_n$, quindi per ogni n si ha

$$\pi^n x_n = y = \pi^{n+1} x_{n+1}$$

da cui

$$x_n = \pi x_{n+1}$$

Ora, la successione di ideali Ax_n è crescente; quindi, poiché A è noetheriano, per un N abbastanza grande abbiamo $Ax_N = Ax_{N+1}$, per cui $x_{N+1} = tx_N$. Ma sappiamo già che $x_N = \pi x_{N+1}$, dunque si ottiene

$$\begin{aligned} x_{N+1} &= t\pi x_{N+1} \\ (1 - t\pi)x_{N+1} &= 0 \end{aligned}$$

Ma $1 - t\pi \notin M$, quindi è invertibile; allora $x_{N+1} = 0$, da cui $y = \pi^{N+1}x_{N+1} = 0$.

Abbiamo allora dimostrato che $\bigcap_{n \geq 0} M^n = 0$. Per ipotesi nessuno dei M^n è nullo; se $A \ni z \neq 0$ allora si può scrivere $z = \pi^n u$ con $u \notin M$ cioè u invertibile, in conclusione A è un anello di valutazione discreta. \square

Definizione 2.1.7. Siano A e B due anelli, $A \subset B$; allora $b \in B$ è detto *intero* su A se esiste un polinomio monico $f(X) \in A[X]$, tale che $f(b) = 0$.

La *chiusura integrale* di A in B è l'insieme degli elementi di B interi su A . Si dice che A è *integralmente chiuso* in B se A coincide con la sua chiusura integrale in B .

Diciamo infine che A è *integralmente chiuso*, se è un dominio di integrità ed è integralmente chiuso nel suo campo dei quozienti.

Lemma 2.1.8. Sia A un anello di valutazione discreta con valutazione v , sia P il suo ideale primo, F il suo campo dei quozienti e siano $x_i \in F$, $i = 1, \dots, n$. Supponiamo $v(x_i) > v(x_1)$ per $i \geq 2$, allora

$$v(x_1 + x_2 + \dots + x_n) = v(x_1).$$

Dimostrazione. Eventualmente dividendo per x_1 , possiamo supporre $x_1 = 1$, da cui $v(x_i) \geq 1$ per $i \geq 2$; cioè $x_i \in P$. Visto che $x_1 \notin P$, anche $x_1 + \dots + x_n \notin P$; quindi $v(x_1 + \dots + x_n) \leq 0$, ma, per le proprietà della valutazione,

$$v(x_1 + \dots + x_n) \geq \min\{v(x_1), \dots, v(x_n)\} = v(x_1) = 0$$

che conclude la dimostrazione. \square

Proposizione 2.1.9. *Sia A un dominio di integrità noetheriano. Allora A è un anello di valutazione discreta se e solo se verifica le due condizioni seguenti:*

(i) A è integralmente chiuso,

(ii) A possiede un ideale primo non nullo ed uno solo.

Dimostrazione. Chiaramente un anello di valutazione discreta verifica (ii); mostriamo che verifica (i). Sia F il campo dei quozienti di A , supponiamo per assurdo che esista $x \in F \setminus A$, x intero su A , allora $v(x) = -m$ con $m > 0$ e x verifica

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0.$$

Ma $v(x^n) = -nm$, mentre

$$v(a_i x^i) \geq -(n-1)m > -nm \quad 0 \leq i \leq n-1,$$

quindi per il lemma precedente

$$v(x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0) = v(x^n) = -nm$$

per cui

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \neq 0$$

che contraddice l'ipotesi.

Ora vogliamo vedere l'altra implicazione; la condizione (ii) mostra che A è un anello locale di cui l'ideale massimale M è diverso da 0.

Sia $M' = \{x \in F \mid xM \subset A\}$; allora M' è un sotto- A -modulo di F che contiene A , inoltre se $M \ni y \neq 0$, si ha chiaramente $M' \subset y^{-1}A$. Visto che A è noetheriano, questo implica che M' è un A -modulo finitamente generato. Per la definizione di M' , abbiamo $MM' \subset A$; d'altra parte, poiché $A \subset M'$, abbiamo $M \subset M'$. MM' è però un ideale, quindi o $MM' = M$ oppure $MM' = A$.

Vogliamo ora mostrare che $MM' = M$ è impossibile; supponiamo per assurdo ciò che sia vero, proveremo innanzitutto che (i) implica $M' = A$

e poi che (ii) implica $M' \neq A$ giungendo così ad una contraddizione. Sia $x \in M'$; abbiamo allora $xM \subset M$ e poi, iterando, $x^n M \subset M$ per ogni n ; cioè $x^n \in M'$. Sia C_n il sotto- A -modulo di K generato da $\{1, x, \dots, x^n\}$; abbiamo $C_n \subset C_{n+1} \subset M'$ per ogni n , ma poiché A è noetheriano avremo $C_{N-1} = C_N$ per un N abbastanza grande, cioè $x_N \in C_{N-1}$. Possiamo allora scrivere

$$x_N = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \quad a_i \in A.$$

Dunque x è intero su A ; per la condizione (i) questo significa che $x \in A$, quindi $M' = A$.

Ora mostriamo che la condizione (ii) implica $M' \neq A$ per cui l'ipotesi $MM' = M$ è falsa. Sia $0 \neq x \in M$ e definiamo $A_x := \{\frac{y}{x^n} \in F \mid y \in A, n \geq 0\}$; per la condizione (ii), dev'essere $A_x = F$. Infatti, se così non fosse, A_x non sarebbe un campo, quindi conterrebbe un ideale massimale non nullo P ; ma $x \notin P$ perché x è invertibile in A_x , quindi $P \cap A \neq M$. D'altra parte, se $0 \neq \frac{y}{x^n} \in P$, si ha $y \in P \cap A$, per cui $P \cap A \neq 0$; infine, poiché P è primo, anche $P \cap A$ lo è, il che contraddice (ii). Abbiamo allora $A_x = F$.

Sia $A \ni z \neq 0$, $\frac{1}{z} \in F = A_x$, quindi

$$\begin{aligned} \frac{1}{z} &= \frac{y}{x^n} \\ x^n &= yz \in zA. \end{aligned}$$

Ogni elemento di M ha quindi una potenza che appartiene a zA ; siano x_1, \dots, x_k generatori di M e sia n abbastanza grande perché $x_i^n \in zA$ per $1 \leq i \leq k$. Scegliendo $N > k(n-1)$, tutti i monomi nelle variabili x_i contengono almeno un fattore x_i^n , quindi stanno in zA ; ma, visto che l'ideale M^N è proprio generato da tali monomi, si ha $M^N \subset zA$. Se ora supponiamo $z \in M$, abbiamo $M^N \subset zA \subset M$, ne concludiamo che esiste un $N \geq 1$ minimale tale che $M^N \subset zA$; scegliamo dunque $y \in M^{N-1}$ ($M^0 = A$ nel caso), $y \notin zA$. Si ha allora che $My \subset zA$, da cui $\frac{y}{z} \in M' \setminus A$, quindi $M' \neq A$.

Tutto questo ragionamento ci ha portato a dire che $MM' \neq M$, quindi ci rimane come sola possibilità $MM' = A$. Mostriamo che ciò implica che M è principale e quindi che A è un anello di valutazione discreta. $MM' = A$

significa che esistono $x_i \in M$, $y_i \in M'$ tali che $\sum_i x_i y_i = 1$; abbiamo $x_i y_i \in A$ per ogni i , ce ne sarà almeno uno, diciamo $x_0 y_0 \notin M$; quindi $x_0 y_0 = u$ è invertibile. Dunque $x_0 u^{-1} \in M$ e $x_0 u^{-1} y_0 = 1$. Sia ora un qualunque $z \in M$, abbiamo allora $z = x_0 u^{-1} y_0 z$ con $y_0 z \in A$ poiché $y_0 \in M'$, quindi $z \in x_0 u^{-1} A$; in conclusione $M = x_0 u^{-1} A$ è principale. \square

Definizione 2.1.10. Un *ideale frazionario* di un anello A , è un sotto- A -modulo finitamente generato del campo dei quozienti di A .

L'insieme M' , che abbiamo usato in quest'ultima dimostrazione, è un esempio di ideale frazionario di A .

Osservazione 2.1.11. La costruzione di M' che abbiamo fatto non dipende dalle ipotesi su M e su A ; in effetti, per ogni ideale $I \neq 0$ di un dominio di integrità A che ha F come campo dei quozienti, possiamo definire $I' = \{x \in K \mid xI \subset A\}$. Se A è noetheriano, I è un ideale frazionario. Se $II' = A$ diciamo che I è *invertibile*; l'ultima parte della dimostrazione che abbiamo fatto mostra che, in un anello locale, ogni ideale invertibile è principale.

2.1.1 Domini di Dedekind

Sia A un dominio di integrità, e F il suo campo dei quozienti; sia poi $S \subset A$ tale che $1 \in S$ e tale che se $x, y \in S$ allora $xy \in S$ (S è un cosiddetto *sottoinsieme moltiplicativo* di A). Supponiamo inoltre che $0 \notin S$, allora definiamo l'anello $S^{-1}A := \{\frac{x}{s} \in K \mid x \in A, s \in S\}$. L'applicazione $P \rightarrow P \cap A$ è una biiezione dall'insieme degli ideali primi di $S^{-1}A$ sull'insieme degli ideali primi di A disgiunti da S .

Un esempio tipico è scegliere $S = A \setminus P$ dove P è un ideale primo di A , in questo caso indichiamo $S^{-1}A$ con A_P . Questo è un anello locale il cui ideale massimale è PA_P e il cui campo dei residui è il campo dei quozienti di A/P ; gli ideali primi di A_P corrispondono agli ideali primi di A contenuti in P . Si dice che A_P è la *localizzazione* di A in P .

Proposizione 2.1.12. Sia A un dominio di integrità noetheriano, allora sono equivalenti le due seguenti proprietà:

(i) Per ogni ideale primo $P \neq 0$ di A , A_P è un anello di valutazione discreta;

(ii) A è integralmente chiuso e ogni ideale primo $P \neq 0$ di A è massimale.

Dimostrazione. Mostriamo che (i) implica (ii). Se $P \subset P'$ sono due ideali primi di A ; allora $A_{P'}$ contiene l'ideale primo $PA_{P'}$ quindi, per 2.1.9 (ii), si ha $P = 0$ oppure $P = P'$; è quindi vero che ogni ideale primo è massimale. D'altra parte, se a è intero su A , è intero anche su A_P per ogni P primo; quindi, per 2.1.9 (i), si ha $a \in A_P$ per ogni P . Ora, se scriviamo $a = \frac{b}{c}$ con $b, c \in A$ e $c \neq 0$ e se definiamo $I := \{x \in A \mid xc \in bA\}$; l'ideale I non è contenuto in nessun ideale primo P , da cui $I = A$ ed $a \in A$.

Vediamo ora l'implicazione inversa; chiaramente gli A_P verificano la condizione di 2.1.9 (ii), ci basta dunque mostrare che sono integralmente chiusi. Sia $x \in F$, intero su A_P ; allora

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{a_0}{s_0} = 0 \quad \text{con } a_i \in A, s_i \in A \setminus P$$

ponendo $s = s_{n-1}s_{n-2} \cdots s_0$ e moltiplicando, si ha

$$sx^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0 \quad \text{con } b_i \in A, s \in A \setminus P$$

moltiplicando poi per s^{n-1} abbiamo

$$(sx)^n + b_{n-1}(sx)^{n-1} + \cdots + s^{n-1}b_0 = 0$$

che dice che sx è intero su A , quindi $sx \in A$, cioè $x \in A_P$. \square

Osservazione 2.1.13. In realtà abbiamo dimostrato che se A è un sottoanello di un campo F e S è un sottoinsieme moltiplicativo di A con $0 \notin S$, $x \in F$ è intero su $S^{-1}A$ se e solo se è della forma $\frac{a'}{s}$ con a' intero su A e $s \in S$.

Definizione 2.1.14. Un dominio di integrità noetheriano che possiede le due proprietà equivalenti di 2.1.12 si dice un *dominio di Dedekind*.

Vediamo ora rapidamente alcune proprietà dei Domini di Dedekind, le dimostrazioni si possono trovare in [7], cap. I §3.

Proposizione 2.1.15. *Sia A dominio di Dedekind e sia $A \ni x \neq 0$, allora esistono solo un numero finito di ideali primi di A che contengono x .*

Osservazione 2.1.16. Se indichiamo con v_P la valutazione su K definita da A_P , per ogni $x \in K^*$ i numeri $v_P(x)$ sono tutti nulli a parte un numero finito.

Proposizione 2.1.17. *Ogni ideale frazionario I di un dominio di Dedekind A si scrive in modo unico come*

$$I = \prod_P P^{v_P(I)}$$

dove i P sono ideali primi di A e $v_P(I)$ sono degli interi tutti nulli tranne un numero finito di essi.

Osservazione 2.1.18. Come conseguenza di questa proposizione, si hanno le formule seguenti:

- $v_P(IJ) = v_P(I) + v_P(J)$,
- $v_P(IJ^{-1}) = v_P(I) - v_P(J)$,
- $v_P(I + J) = \min\{v_P(I), v_P(J)\}$,
- $v_P(xA) = v_P(x)$.

Lemma 2.1.19 (di Approssimazione). *Sia $k \in \mathbb{N}$, e siano P_i , $1 \leq i \leq k$ ideali primi del dominio di Dedekind A , distinti a due a due. Sia K il campo dei quozienti di A e siano $x_i \in K$, $n_i \in \mathbb{Z}$ per $1 \leq i \leq k$. Allora esiste $x \in K$ tale che:*

$$\begin{cases} v_{P_i}(x - x_i) \geq n_i & \text{per } 1 \leq i \leq k, \\ v_Q(x) \geq 0 & \text{per } Q \neq P_1, \dots, P_k. \end{cases}$$

Corollario 2.1.20. *Un dominio di Dedekind che ha solo un numero finito di ideali primi è un dominio a ideali principali.*

Proposizione 2.1.21. *Sia A un dominio di Dedekind; sia I un ideale di A e sia J un ideale frazionario di A . Allora esiste un isomorfismo di A -moduli*

$$A/I \simeq J/IJ.$$

2.2 Estensioni del campo dei quozienti

In tutto ciò che segue, supponiamo che A sia un anello noetheriano e integralmente chiuso, con campo dei quozienti F . Supponiamo inoltre che K sia un'estensione finita di F e indichiamo con B la chiusura integrale di A in K ; allora per l'osservazione 2.1.13 si ha $FB = K$ e, in particolare, K è il campo dei quozienti di B .

Osservazione 2.2.1. Se B è un A -modulo finitamente generato, allora B è un anello noetheriano integralmente chiuso.

Proposizione 2.2.2. Se K/F è un'estensione separabile, allora B è un A -modulo finitamente generato.

Dimostrazione. Sappiamo che $\text{Tr}_{K/F}(xy)$ è una forma F -bilineare simmetrica, non degenerata su K . Se $x \in B$, i coniugati di x rispetto a F (in un'estensione adeguata di K) sono ancora interi su A , infatti

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

implica

$$\begin{aligned} \sigma(x)^n + \sigma(a_{n-1})\sigma(x)^{n-1} + \cdots + \sigma(a_0) &= 0 \\ \sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + \cdots + a_0 &= 0. \end{aligned}$$

quindi sarà intero anche $\text{Tr}_{K/F}(x)$, visto che è la loro somma. Dunque, dal momento che $\text{Tr}_{K/F}(x) \in F$, abbiamo $\text{Tr}(x) \in A$.

Sia allora $\{e_i\}$ una base di K su F , con $e_i \in B$ e sia $V = \bigoplus_i e_i A$. Per ogni M sotto- A -modulo di K , sia $M^* = \{x \in K \mid \text{Tr}(xy) \in A \text{ per ogni } y \in M\}$, si ha chiaramente

$$V \subset B \subset B^* \subset V^*.$$

Dal momento che V^* è il modulo libero generato dalla base duale di e_i rispetto alla forma bilineare $\text{Tr}(xy)$, se ne conclude che B è finitamente generato, e $[B : A] = [K : F]$. \square

Lemma 2.2.3. *Siano ora $P \subset Q$ due ideali primi di B tali che $P \cap A = Q \cap A$, allora $P = Q$.*

Dimostrazione. A meno di quotizzare per P , possiamo supporre $P = 0$. Se $Q \neq P$, esiste un elemento $Q \ni x \neq 0$. Sia allora

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \quad a_i \in A$$

l'equazione minimale di x su A . Abbiamo $a_0 \neq 0$ e $a_0 \in xB$, quindi $a_0 \in Q \cap A = P \cap A = 0$ il che è assurdo. \square

Proposizione 2.2.4. *Se B è un A -modulo finitamente generato e A è un dominio di Dedekind; allora B è un domino di Dedekind.*

Dimostrazione. Per 2.2.1, B è noetheriano e integralmente chiuso. Per 2.1.12 ci resta da dimostrare che i suoi ideali primi sono massimali; siano $P_1 \subset P_2$ due ideali primi di B , allora $P_1 \cap A \subset P_2 \cap A$ sono due ideali primi di A . Dal momento che A è noetheriano, abbiamo quindi due possibilità: o $P_1 \cap A = 0$, oppure $P_1 \cap A = P_2 \cap A$. Per il lemma appena visto, abbiamo quindi $P_1 = 0$ oppure $P_1 = P_2$. \square

D'ora in avanti supponiamo che B sia un A -modulo finitamente generato, e che B sia quindi un dominio di Dedekind.

Definizione 2.2.5. Sia $Q \neq 0$ un ideale primo di B e sia $P = Q \cap A$. Diciamo allora che Q divide P e lo noteremo con $Q|P$.

Questo equivale a dire che $PB \subset Q$.

Definizione 2.2.6. Se $Q|P$, definiamo e_Q l'esponente di Q nella decomposizione in ideali primi di PB , cioè

$$e_Q = v_Q(PB) \quad \text{e} \quad PB = \prod_{Q|P} Q^{e_Q}.$$

L'intero e_Q si chiama l'indice di ramificazione di Q nell'estensione K/F .

D'altra parte, se Q divide P , il campo B/Q è un'estensione del campo A/P ; dal momento che B è finitamente generato su A , B/Q è un'estensione finita di A/P .

Definizione 2.2.7. Definiamo $f_Q := [B/Q : A/P]$, f_Q viene chiamato il *grado residuo* di Q nell'estensione K/F .

Definizione 2.2.8. Quando c'è un solo ideale primo Q che divide P , e $f_Q = 1$, si dice che K/F è *totalmente ramificata* in P .

Quando $e_Q = 1$ e B/Q è un'estensione separabile di A/P , si dice che K/F è *non ramificata* in Q . Se K/F è non ramificata per ogni Q ideale primo che divide P , si dice che K/F è non ramificata in P .

Proposizione 2.2.9. Sia $P \neq 0$ un ideale primo di A . L'anello B/PB è una A/P -algebra di dimensione $n = [K : F]$, isomorfa al prodotto $\prod_{Q|P} B/Q^{e_Q}$. Si ha la formula

$$n = \sum_{Q|P} e_Q f_Q.$$

Dimostrazione. Sia $S = A \setminus P$, e sia $A' = A_P = S^{-1}A$; sia inoltre $B' = S^{-1}B$. L'anello A' è un anello di valutazione discreta e B' è la sua chiusura integrale in K , per 2.1.13. Si ha $A'/PA' = A/P$ e si vede facilmente che $B'/PB' = B/PB$. Dal momento che A' è principale e B è un A -modulo finitamente generato, B' è un A' -modulo libero di rango $n = [K : F]$ e B'/PB' è libero di rango n su A'/PA' . Si vede dunque che B/PB è una A/P -algebra di dimensione n .

Visto che $PB = \cap Q^{e_Q}$, l'applicazione canonica

$$B/PB \rightarrow \prod_{Q|P} B/Q^{e_Q}$$

è iniettiva e, per il lemma di approssimazione (2.1.19), è anche suriettiva; quindi è un isomorfismo. Confrontando le dimensioni, si vede che

$$n = \sum_{Q|P} n_Q \quad \text{dove definiamo} \quad n_Q := [B/Q^{e_Q} : A/P].$$

Per concludere la dimostrazione, consideriamo la catena discendente di A/P -moduli

$$B/Q^{e_Q} \supset Q/Q^{e_Q} \supset \dots \supset Q^{e_Q-1}/Q^{e_Q} \supset 0;$$

si ha che, per ogni $i = 0, \dots, e_Q - 1$;

$$(Q^i/Q^{e_Q})/(Q^{i+1}/Q^{e_Q}) \simeq Q^i/Q^{i+1} \simeq B/Q \quad (\text{per 2.1.21}),$$

quindi

$$n_Q = \sum_{i=0}^{e_Q-1} [(Q^i/Q^{e_Q})/(Q^{i+1}/Q^{e_Q}) : A/P] = e_Q[B/Q : A/P] = e_Q f_Q.$$

□

2.2.1 Estensioni nel caso locale

In quello che segue, sia A un anello di valutazione discreta, con ideale primo P e sia $\bar{F} := A/P$ il suo campo dei residui. Sia poi $\mathbb{N} \ni n \geq 1$ e sia $f \in A[X]$ un polinomio monico di grado n . Indichiamo con (f) l'ideale principale generato da f e definiamo $B_f := A[X]/(f)$. Abbiamo che B_f è una A -algebra che ha come base $\{1, X, \dots, X^{n-1}\}$. Poniamo $\bar{B}_f = B_f/PB_f = A[X]/(P, f)$. Se indichiamo con \bar{f} l'immagine di f in $\bar{F}[X]$ tramite la riduzione modulo P si ha dunque

$$\bar{B}_f = \bar{F}[X]/(\bar{f}).$$

Supponiamo inoltre che \bar{f} sia irriducibile.

Proposizione 2.2.10. *B_f è un anello di valutazione discreta d'ideale massimale PB_f e con campo dei residui $\bar{F}[X]/(\bar{f})$.*

Dimostrazione. Se \bar{f} è irriducibile, $B_f/PB_f = \bar{B}_f = \bar{F}[X]/(\bar{f})$ è un campo, quindi PB_f è un ideale massimale di B_f . Vogliamo vedere che ogni ideale massimale M di B_f è uguale a PB_f ; per fare ciò basta mostrare che $PB_f \subset M$. Se così non fosse, avremmo $M + PB_f = B_f$ e, visto che B_f è un A -modulo finitamente generato, per il lemma di Nakayama (vedi [5], cap. IX

§1) avremmo $M = B_f$ che è assurdo. Quindi B_f è un anello locale, di ideale massimale PB_f e con campo dei residui $\overline{F}[X]/(\overline{f})$; inoltre se π genera P , l'immagine di π in B_f genera PB_f e non è un elemento nilpotente, quindi per 2.1.6 è un anello di valutazione discreta. \square

Corollario 2.2.11. *Sia F è il campo dei quozienti di A . Allora il polinomio f è irriducibile in $F[X]$; inoltre se K è il campo $F[X]/(f)$, l'anello B_f è la chiusura integrale di A in K .*

Dimostrazione. Abbiamo che $F[X]/(f) = B_f \otimes_A F$; dal momento che B_f è un dominio di integrità, lo è anche $B_f \otimes_A F$, quindi f è irriducibile e $F[X]/(f)$ è un campo. Poiché B_f è integralmente chiuso e ammette K come campo dei quozienti, è esattamente la chiusura integrale di A in K . \square

Corollario 2.2.12. *Se \overline{f} è separabile, l'estensione K/F è non ramificata.*

Dimostrazione. Il fatto che PB_f sia l'ideale massimale di B_f ci dice che l'indice di ramificazione è 1. Se \overline{f} è separabile si ha che l'estensione

$$(\overline{F}[X]/(\overline{f}))/\overline{F}$$

è separabile. \square

Proposizione 2.2.13. *Sia A un anello di valutazione discreta con campo dei quozienti F e sia K/F un'estensione di grado n . Sia B la chiusura integrale di A in K . Supponiamo che B sia un anello di valutazione discreta e che il campo dei residui \overline{K} di B sia un'estensione semplice di grado n del campo dei residui \overline{F} di A , cioè $\overline{K} = \overline{F}(\overline{x})$, con $\overline{x} \in \overline{K}$. Sia $x \in B$ tale che la sua immagine in \overline{K} sia \overline{x} , e sia f il polinomio caratteristico di x su F . Allora l'omomorfismo da $A[X]$ in B tale che $X \mapsto x$ definisce per passaggio al quoziente un isomorfismo tra B_f e B .*

Dimostrazione. I coefficienti di f sono interi su A e stanno in F , quindi $f \in A[X]$, poiché A è integralmente chiuso. Inoltre $f(x) = 0$, quindi l'applicazione $A[X] \rightarrow B$, definita da $X \mapsto x$, si può fattorizzare in

$$A[X] \rightarrow B_f \rightarrow B.$$

D'altra parte, $\bar{f}(\bar{x}) = 0$ e, dal momento che \bar{x} è di grado n su \bar{F} , ne concludiamo che \bar{f} è il polinomio minimo di \bar{x} su \bar{F} ; è quindi irriducibile. Possiamo allora applicare 2.2.11 ed ottenere che B_f è la chiusura integrale di A in K , cioè $B_f = B$. \square

2.3 Completamento

Definizione 2.3.1. Sia F un campo e sia $|\cdot| : F \rightarrow \mathbb{R}$ una funzione tale che

- $|x| = 0$ se e solo se $x = 0$
- $|xy| = |x||y|$ per ogni $x, y \in F$
- $|x + y| \leq \max\{|x|, |y|\}$

$|\cdot|$ è detto un *valore assoluto ultrametrico* su F .

Osservazione 2.3.2. Sia F un campo con una valutazione discreta v , di anello A . Sia $a \in \mathbb{R}$, $0 < a < 1$; allora

$$|x| := \begin{cases} a^{v(x)} & \text{se } x \neq 0 \\ 0 & \text{se } x = 0 \end{cases}$$

è un valore assoluto ultrametrico su F .

Possiamo in questo caso definire

$$d(x, y) := |x - y|.$$

Si verifica facilmente che d è una metrica su F , e la topologia indotta su F non dipende dalla scelta di $a \in \mathbb{R}$. Consideriamo allora il completamento metrico \hat{F} di F tramite d . Si verifica che \hat{F} è ancora un campo e che si può prolungare $|\cdot|$ a \hat{F} in modo che, per ogni $x \in \hat{F}$,

$$|x| = a^{\hat{v}(x)}$$

dove \hat{v} è una valutazione discreta su \hat{F} il cui anello \hat{A} è il completamento di A . Se π è un generatore dell'ideale massimale di A , si vede che

$$A/\pi^n A \simeq \hat{A}/\pi^n \hat{A} \quad \text{per ogni } n \in \mathbb{Z},$$

in particolare i campi dei residui di A ed \hat{A} coincidono.

Definizione 2.3.3. Un campo F con una valutazione discreta di anello A , completo rispetto alla topologia indotta dalla valutazione, e tale che il campo residuo $\bar{F} = A/P$ sia un campo finito, è detto un *campo locale*.

Un risultato importante negli anelli di valutazione discreta completi è il Lemma di Hensel, di cui diamo una versione.

Proposizione 2.3.4 (Lemma di Hensel). *Sia A un anello di valutazione discreta, completo per la topologia indotta dalla valutazione, sia P l'ideale massimale di A , con generatore π , e sia $\bar{F} = A/P$ il campo residuo di A . Sia $f \in A[X]$ tale che la sua riduzione modulo π , $\bar{f} \in \bar{F}[X]$ abbia una radice semplice λ in \bar{F} , esiste allora una ed una sola $x \in A$, radice di f , tale che $\bar{x} = \lambda$.*

Dimostrazione. Per vedere l'unicità, supponiamo che x sia una soluzione, abbiamo allora $f(X) = (X - x)g(X)$ con $\bar{g}(\lambda) \neq 0$. Se x' è un'altra soluzione, abbiamo

$$0 = f(x') = (x' - x)g(x')$$

ma la riduzione modulo π di $g(x')$ è $\bar{g}(\lambda)$, quindi $g(x')$ è invertibile, cioè $x = x'$.

Vogliamo ora dimostrare l'esistenza; prendiamo $x_1 \in A$ tale che $\bar{x}_1 = \lambda$, abbiamo

$$f(x_1) \equiv 0 \pmod{\pi}.$$

Ora, per induzione, supponiamo di aver trovato $x_n \in A$ tale che $\bar{x}_n = \lambda$ e con $f(x_n) \equiv 0 \pmod{\pi^n}$ e mostriamo che si può trovare $x_{n+1} \in A$, $x_{n+1} \equiv x_n \pmod{\pi^n}$ e $f(x_{n+1}) \equiv 0 \pmod{\pi^{n+1}}$. Per fare ciò, scriviamo $x_{n+1} = x_n + h$ con $h \in \pi^n A$. Applichiamo la formula di Taylor

$$f(x_{n+1}) = f(x_n) + hf'(x_n) + h^2y \quad \text{con } y \in A.$$

Abbiamo $v(h^2y) \geq 2v(h)$, quindi $h^2y \in \pi^{n+1}A$. Il tutto sta allora nel trovare $h \in \pi^n A$ tale che

$$f(x_n) + hf'(x_n) \equiv 0 \pmod{\pi^{n+1}}.$$

Ma, dal momento che λ è una radice semplice di \bar{f} , si ha $\bar{f}'(\lambda) \neq 0$, quindi $f'(x_n)$ è invertibile in A . Allora scegliendo $h = -f(x_n)(f'(x_n))^{-1}$ abbiamo appunto $h \in \pi^n A$ che ha le proprietà richieste.

Abbiamo allora una successione x_n che è di Cauchy, perchè

$$|x_{n+p} - x_n| \leq \max\{|x_{n+p} - x_{n+p-1}|, \dots, |x_{n+1} - x_n|\} \leq a^{v(\pi^n)} \xrightarrow{n \rightarrow \infty} 0,$$

ed è quindi convergente in quanto A è completo. Se prendiamo come x il limite della successione, abbiamo, per continuità, visto che $f(x_n) \equiv 0 \pmod{\pi^n}$,

$$|f(x)| = \lim_{n \rightarrow \infty} |f(x_n)| \leq \lim_{n \rightarrow \infty} a^n = 0.$$

□

2.3.1 Estensioni di campi completi

Teorema 2.3.5. *Sia F un campo con una valutazione discreta v , di anello A , e completo per la metrica indotta da v . Sia K/F un'estensione finita di F , e sia B la chiusura integrale di A in K . Allora B è un anello di valutazione discreta, è un A -modulo libero di rango $n = [K : F]$ e K è completo per la metrica indotta dalla valutazione in B .*

Dimostrazione. Cominciamo con il caso in cui K/F è separabile; allora, per 2.2.2, B è un A -modulo libero di rango n , quindi è un dominio di Dedekind. Siano Q_i gli ideali primi di B e siano w_i le valutazioni corrispondenti; ogni w_i definisce, come in 2.3.2, un valore assoluto ultrametrico su K che è anche una norma in K visto come F -spazio vettoriale. Dal momento che F è completo, un risultato conosciuto sugli spazi vettoriali normati (vedi [1], cap.I §2) ci dice che la topologia τ_i definita dalla norma w_i è in realtà la topologia prodotto di K visto come F^n , e non dipende quindi da i . Ma w_i è determinata dalla topologia τ_i perchè l'anello di w_i è esattamente l'insieme $\{x \in K | x^{-n} \not\equiv 0 \pmod{\pi^n} \text{ per } n \rightarrow \infty\}$, in cui il limite di x^{-n} è inteso nella topologia τ_i . Se ne deduce che di w_i ce n'è in realtà una sola, e quindi B è un anello di valutazione discreta. Dal momento che F è completo, anche $K = F^n$ è completo.

Avendo visto il caso separabile, per dimostrare il teorema ci basta trattare il caso in cui K/F è radicale e non separabile; infatti, ragionando per estensioni successive, possiamo sempre ricondurci ad uno di questi due casi. Sia dunque K/F radicale non separabile; esiste allora un q tale che $x^q \in F$ per ogni $x \in K$. Se poniamo $v'(x) := v(x^q)$, l'applicazione $v' : K^* \rightarrow \mathbb{Z}$ è un omomorfismo; sia m il generatore positivo del sottogruppo $v'(K^*) \subset \mathbb{Z}$, allora la funzione $v_K := \frac{1}{m}v'$ è una valutazione discreta su K . Il suo anello di valutazione è B e lo stesso ragionamento del caso precedente dimostra che la topologia definita da v_K coincide con quella di F^n e che quindi K è completo.

Resta da vedere che B è un A -modulo finitamente generato. Sia π un generatore dell'ideale massimale di A e sia $\overline{B} = B/\pi B$, siano poi $b_i \in B$ tali che le loro immagini $\overline{b}_i \in \overline{B}$ siano linearmente indipendenti su $\overline{F} = A/\pi A$. I b_i sono linearmente indipendenti su A , infatti, se ci fosse una relazione non banale $\sum a_i b_i = 0$, potremmo supporre che almeno uno degli a_i non sia divisibile per π e, riducendo modulo πB , otterremmo una relazione tra i \overline{b}_i . In particolare, il numero dei b_i è minore o uguale a n . Supponiamo ora che i \overline{b}_i formino una base di \overline{B} e sia M il sotto- A -modulo di B generato dai b_i . Ogni $b \in B$ si scrive quindi

$$b = b_0 + \pi b_1 \quad \text{con} \quad b_0 \in M \text{ e } b_1 \in B,$$

applicando questo a b_1 ed iterando, ne concludiamo che b si scrive della forma

$$b = b_0 + \pi b_1 + \pi^2 b_2 + \cdots, \quad b_i \in M;$$

allora, poiché A è completo, questo mostra che $b \in M$. □

Corollario 2.3.6. *Se e ed f indicano rispettivamente l'indice di ramificazione e il grado residuo di K/F , abbiamo $ef = n$.*

Dimostrazione. Avendo mostrato che B è un A -modulo finitamente generato, il risultato segue subito da 2.2.9. □

Corollario 2.3.7. *Esiste una ed una sola valutazione v_K di K che prolunga v e due elementi di K coniugati su F hanno la stessa valutazione.*

Dimostrazione. La prima affermazione risulta dalla dimostrazione del teorema. Per quanto riguarda la seconda affermazione, a meno di ingrandire K , possiamo supporre che K/F sia un'estensione normale. Sia allora $\sigma \in \text{Gal}(K/F)$; $v_K \circ \sigma$ è una valutazione che prolunga v , quindi coincide con v_K . \square

Corollario 2.3.8. *Si ha che $v_K(x) = \frac{1}{f}v(\text{N}_{K/F}(x))$ per ogni $x \in K$.*

Dimostrazione. Come nel corollario precedente, possiamo ricondurci al caso in cui K/F è normale, abbiamo allora

$$v(\text{N}_{K/F}(x)) = v_K \left(\prod_{i=1}^f \sigma_i(x) \right) = \sum_{i=1}^f v_K(\sigma_i(x)) = f v_K(x).$$

\square

In termini di valori assoluti, quest'ultimo corollario ci dice che la topologia di K può essere definita dalla norma

$$|x|_K = |\text{N}_{K/F}(x)|_F \quad x \in K.$$

Teorema 2.3.9. *Sia A un anello di valutazione discreta completo, sia F il suo campo dei quozienti e sia \bar{F} il campo dei residui. Sia F'/F un'estensione finita non ramificata, corrispondente all'estensione residua \bar{F}'/\bar{F} , e sia F''/F un'estensione finita qualunque, di estensione residua \bar{F}''/\bar{F} . L'insieme degli F -isomorfismi di F' in F'' corrisponde biunivocamente (per riduzione) all'insieme degli \bar{F} -isomorfismi di \bar{F}' in \bar{F}'' .*

Dimostrazione. Se indichiamo con A' e A'' le chiusure integrali di A rispettivamente in F' ed F'' , abbiamo chiaramente che

$$\text{Hom}_K(K', K'') = \text{Hom}_A(A', A''),$$

si tratta quindi di mostrare che l'omomorfismo canonico

$$\theta : \text{Hom}_A(A', A'') \rightarrow \text{Hom}_{\bar{F}}(\bar{F}', \bar{F}'')$$

è biiettivo.

Per 2.2.13, esiste $x \in A'$ tale che, se $n := [F' : F]$, gli elementi $\{1, x, \dots, x^{n-1}\}$ formano una base di A' su A : Inoltre se f è il polinomio caratteristico di x ; la riduzione \bar{f} di f è il polinomio caratteristico dell'immagine \bar{x} di x in \bar{F}' . Ne segue che gli elementi di $\text{Hom}_A(A', A'')$ (e rispettivamente di $\text{Hom}_{\bar{F}}(\bar{F}', \bar{F}'')$) corrispondono biunivocamente agli elementi $a'' \in A''$ (e $\xi'' \in \bar{F}''$) tali che $f(a'') = 0$ (rispettivamente $\bar{f}(\xi'') = 0$).

L'applicazione θ corrisponde dunque alla riduzione $a'' \rightarrow \xi'' = \bar{a}''$. Tutto si riconduce allora a mostrare che una radice di \bar{f} in \bar{F}'' si solleva in modo unico in una radice di f in A'' . Questo è vero per il Lemma di Hensel (2.3.4), dal momento che tutte le radici di \bar{f} sono semplici, visto che \bar{f} è irriducibile e separabile su \bar{F} . \square

Corollario 2.3.10. *Sia \bar{F}'/\bar{F} un'estensione separabile finita. Esiste allora un'unica (a meno di isomorfismo unico) estensione finita non ramificata F'/F tale che la corrispondente estensione residua sia \bar{F}'/\bar{F} . Inoltre F'/F è un'estensione di Galois se e solo se lo è \bar{F}'/\bar{F} e si ha $\text{Gal}(F'/F) \simeq \text{Gal}(\bar{F}'/\bar{F})$.*

Dimostrazione. Dal momento che \bar{F}'/\bar{F} è finita e separabile, è semplice. Sia ξ un generatore dell'estensione e sia φ il suo polinomio minimo su \bar{F} , abbiamo $\deg \varphi = n = [\bar{F}' : \bar{F}]$. Sia $f \in A[X]$ un polinomio unitario tale che la sua riduzione modulo P , $\bar{F}[X] \ni \bar{f} = \varphi$. Per 2.2.10, l'anello $A' = A[X]/(f)$ è un anello di valutazione discreta, non ramificato su A , e di estensione residua \bar{F}'/\bar{F} . Il suo campo dei quozienti è il campo F' cercato, il che dimostra l'esistenza. L'unicità è garantita dal teorema appena visto, così come l'ultima affermazione. \square

Corollario 2.3.11. *Sia F''/F un'estensione finita con estensione residua \bar{F}''/\bar{F} . Le sottoestensioni F'/F di F''/F che sono non ramificate su F corrispondono biunivocamente alle sottoestensioni \bar{F}'/\bar{F} di \bar{F}''/\bar{F} che sono separabili. Di conseguenza esiste un'estensione non ramificata massimale K/F , $K \subset F''$, il cui campo dei residui \bar{K} è la più grande estensione separabile di \bar{F} contenuta in \bar{F}'' .*

Dimostrazione. Questo è chiaro dal teorema. \square

Teorema 2.3.12. *Supponiamo che F sia un campo locale, e che il campo dei residui \overline{F} abbia cardinalità q . Allora per ogni $f \in \mathbb{N}$ esiste un'unica estensione non ramificata K di F tale che $f = [K : F] = f(K/F)$. Questa estensione è precisamente $K = F(\omega)$, dove ω è una radice primitiva $(q^f - 1)$ -esima dell'unità in F . Inoltre se indichiamo con A l'anello di valutazione di F e con B quello di K , abbiamo $B = A[\omega]$ e $\overline{K} = \overline{F}(\overline{\omega})$.*

Dimostrazione. Esiste un'unica estensione separabile di \overline{F} , di grado f , ed è $\overline{F}(\xi)$ dove ξ è una radice primitiva $(q^f - 1)$ -esima dell'unità in \overline{F} , quindi per 2.3.10 esiste un'unica estensione non ramificata K/F tale che $[K : F] = [\overline{F}(\xi) : \overline{F}] = f$. Ci basta allora mostrare che $F(\omega)$ è un'estensione non ramificata di F tale che $[F(\omega) : F] = f$. Ora, ω è una radice del polinomio

$$g(X) = X^{q^f - 1} - 1 \in A[X],$$

dal momento che $\overline{g}(X) \in \overline{F}(X)$ è separabile, $F(\omega)$ è non ramificata su F per 2.2.12. Inoltre

$$g(X) = \prod_{i=1}^{q^f - 1} (X - \omega^i), \quad \overline{g}(X) = \prod_{i=1}^{q^f - 1} (X - \overline{\omega}^i).$$

Quindi $\overline{\omega}$ è una radice primitiva $(q^f - 1)$ -esima dell'unità su \overline{F} , e allora

$$[F(\omega) : F] = [\overline{F}(\overline{\omega}) : \overline{F}] = f.$$

\square

Corollario 2.3.13. *Sia F un campo locale, tale che il campo residuo \overline{F} abbia cardinalità q . Sia K l'unica estensione non ramificata di F con $[K : F] = f$; allora K/F e $\overline{K}/\overline{F}$ sono estensioni di Galois e $\text{Gal}(K/F)$ è ciclico di ordine f , generato da $\omega \rightarrow \omega^q$.*

Dimostrazione. Sappiamo che $\overline{K}/\overline{F}$ è un'estensione di Galois, quindi per 2.3.10, l'estensione K/F è di Galois e $\text{Gal}(K/F) \simeq \text{Gal}(\overline{K}/\overline{F})$. Il gruppo

$\text{Gal}(\overline{K}/\overline{F})$ è ciclico di ordine f , generato da $\overline{\omega} \rightarrow \overline{\omega}^q$, quindi il polinomio minimo di $\overline{\omega}$ su \overline{F} è

$$\overline{h}(X) = \prod_{i=0}^{f-1} (X - \overline{\omega}^{q^i})$$

allora il polinomio minimo di ω su F è

$$h(X) = \prod_{i=0}^{f-1} (X - \omega^{q^i})$$

per cui $\omega \rightarrow \omega^q$ è un generatore di $\text{Gal}(K/F)$, e viene chiamato l'*automorfismo di Frobenius* di K/F . \square

Teorema 2.3.14. *Sia F un campo locale e sia K/F l'unica estensione finita non ramificata, con $[K : F] = f$; sia v la valutazione su F , di anello A , e sia v_K l'unico prolungamento di v in K , con anello B . Dato $\alpha \in F$, esiste $x \in K$ tale che*

$$N_{K/F} x = \alpha \quad x \in K$$

se e solo se $f|v(\alpha)$.

Dimostrazione. Innanzitutto vediamo che la condizione è necessaria; sia $x \in K$ tale che $N_{K/F} x = \alpha$, allora usando 2.3.8

$$v(\alpha) = v(N_{K/F} x) = f v_K(x) \equiv 0 \pmod{f}.$$

Per vedere che è sufficiente, il caso $\alpha = 0$ è banale, quindi possiamo supporre $\alpha \neq 0$. Osserviamo che se $v(\alpha) = fq$ con $q \in \mathbb{Z}$ allora esiste $x \in K$ con $v_K(x) = q$, quindi

$$\begin{aligned} v(\alpha) &= f v_K(x) \\ &= v(N_{K/F} x) \end{aligned}$$

da cui

$$\begin{aligned} v(N_{K/F} x) - v(\alpha) &= 0 \\ v((N_{K/F} x)\alpha^{-1}) &= 0 \\ (N_{K/F} x)\alpha^{-1} &= \alpha_1 \in A^* \\ (N_{K/F} x)\alpha_1^{-1} &= \alpha \end{aligned}$$

per avere una soluzione ci basta quindi che esista y con $N_{K/F}y = \alpha_1^{-1}$. Abbiamo quindi ridotto il problema iniziale a trovare una soluzione di

$$N_{K/F}x = \alpha \quad \text{quando} \quad \alpha \in A^*.$$

Ora, dal momento che $\text{Gal}(K/F) \simeq \text{Gal}(\overline{K}/\overline{F})$, si ha che

$$\overline{N_{K/F}x} = N_{\overline{K}/\overline{F}}\overline{x} \quad \text{e} \quad \overline{\text{Tr}_{K/F}x} = \text{Tr}_{\overline{K}/\overline{F}}\overline{x} \quad \text{per ogni } x \in B.$$

Sappiamo che $\text{Tr}_{\overline{K}/\overline{F}}$ è suriettiva perché $\overline{K}/\overline{F}$ è un'estensione separabile; vogliamo mostrare anche $N_{\overline{K}/\overline{F}}$ è suriettiva. Il gruppo moltiplicativo \overline{K}^* è ciclico di ordine $q^f - 1$ con generatore $\overline{\omega}$ (stiamo usando le stesse notazioni di 2.3.12), quindi ogni elemento di \overline{K}^* è della forma $\overline{\omega}^t$ con $0 \leq t \leq q^f - 1$; inoltre $\text{Gal}(\overline{K}/\overline{F}) = \langle \overline{\sigma} \rangle$ dove $\overline{\sigma}$ è definita da $\overline{\omega} \rightarrow \overline{\omega}^q$. Allora abbiamo

$$\begin{aligned} N_{\overline{K}/\overline{F}}\overline{\omega}^t &= \prod_{i=0}^{f-1} (\overline{\omega}^t)^{q^i} \\ &= \overline{\omega}^{t(1+q+\dots+q^{f-1})} \\ &= \overline{\omega}^{t \frac{q^f-1}{q-1}}. \end{aligned}$$

Quindi $N_{\overline{K}/\overline{F}} = 1$ se e solo se $(q-1)|t$, che significa che ci sono esattamente $\frac{q^f-1}{q-1}$ elementi di \overline{K} con norma 1. In conclusione, la cardinalità dell'immagine di $N_{\overline{K}/\overline{F}}$ è $q-1$, cioè è suriettiva.

Ora, sia $\pi \in A$ tale che $v(\pi) = 1$, e sia $\alpha \in A^*$. Siccome $N_{\overline{K}/\overline{F}}$ è suriettiva, possiamo scegliere $b_0 \in B$ tale che

$$\alpha \equiv N_{K/F}b_0 \pmod{\pi A}.$$

Ora per $i \geq 1$, supponiamo di aver trovato un elemento

$$a_i = b_0 + \pi b_1 + \dots + \pi^{i-1}b_{i-1} \in B$$

tale che

$$\alpha \equiv N_{K/F}a_i \pmod{\pi^i A}.$$

Sicuramente $a_i \in B^*$ poiché $N_{K/F} a_i \in A^*$; l'approssimazione successiva sarà del tipo

$$a_{i+1} = a_i + \pi^i b$$

con $b \in B$ da determinare in modo che

$$\alpha \equiv N_{K/F} a_{i+1} \pmod{\pi^{i+1} A}. \quad (2.4)$$

Poiché $i \geq 1$, abbiamo

$$\begin{aligned} N_{K/F} a_{i+1} &= \prod_{s=0}^{f-1} (\sigma^s(a_i + \pi^i b)) \\ &= \prod_{s=0}^{f-1} (\sigma^s(a_i) + \pi^i \sigma^s(b)) \\ &\equiv N_{K/F} a_i + \pi^i \sum_{s=0}^{f-1} c_s \pmod{\pi^{i+1} A}, \end{aligned}$$

dove per ogni s si ha

$$c_s = a_i \sigma(a_i) \cdots \sigma^{s-1}(a_i) \sigma^{s+1}(a_i) \cdots \sigma^{f-1}(a_i) \sigma^s(b).$$

Se poniamo $y := \sigma(a_i) \sigma^2(a_i) \cdots \sigma^{f-1}(a_i)$, allora $c_s = \sigma^s(y) \sigma^s(b) = \sigma^s(yb)$, da cui

$$\sum_{s=0}^{f-1} c_s = \text{Tr}_{K/F}(yb).$$

La condizione (2.4) diventa allora

$$\alpha \equiv N_{K/F} a_i + \pi^i \text{Tr}_{K/F}(yb) \pmod{\pi^{i+1} A}.$$

Ma y è invertibile in B e $\text{Tr}_{\overline{K}/\overline{F}}$ è suriettiva, quindi possiamo sempre trovare $b \in B$ che soddisfa questa condizione. Abbiamo così ottenuto l'approssimazione successiva a_{i+1} .

Se poniamo $x = \lim_{i \rightarrow \infty} a_i$ allora $x \in B$ e $\alpha = N_{K/F} x$. □

2.4 Gruppo di Brauer di un campo locale

Ora siamo arrivati all'ultima parte di questa trattazione: vogliamo determinare il gruppo di Brauer di un campo locale. Per fare questo cominciamo a vedere come sono fatte le algebre di divisione su un tale campo.

In tutto ciò che segue, sia D un'algebra di divisione centrale sul campo locale F , con $[D : F] = m^2$. Così come abbiamo fatto nel caso delle estensioni di F , vogliamo definire una valutazione discreta su D che prolunghi la valutazione v di F . Sia $x \in D$, definiamo

$$v'(x) = \begin{cases} v(\text{nrd}_{D/F}(x)) & \text{se } x \neq 0 \\ 0 & \text{se } x = 0 \end{cases}.$$

L'applicazione $v' : D^* \rightarrow \mathbb{Z}$ è un omomorfismo per 1.5.10 e si ha $v'(x) = mv(x)$ se $x \in F^*$ (perché in tal caso $\text{nrd}_{D/F}(x) = x^m$). Sia d il generatore positivo del sottogruppo $v'(D^*) \subset \mathbb{Z}$ e poniamo

$$w = \frac{1}{d}v'.$$

L'applicazione $w : D^* \rightarrow \mathbb{Z}$ è un omomorfismo suriettivo.

Proposizione 2.4.1. *Abbiamo allora che*

1. $w(x) = \frac{m}{d}v(x)$ se $x \in F^*$;
2. $w(x+y) \geq \min\{w(x), w(y)\}$ e $w(xy) = w(x) + w(y)$ per ogni $x, y \in D$;
3. se $a \in \mathbb{R}$, $0 < a < 1$, e poniamo $\|x\|_D = a^{w(x)}$, otteniamo una norma su D e la topologia definita da questa norma è la topologia prodotto di D identificato a F^{m^2} ;
4. se $y \in D$, y è intero su $A = \{x \in F \mid v(x) \geq 0\}$ se e solo se $w(x) \geq 0$; $B = \{y \in D \mid w(y) \geq 0\}$ è un sottoanello di D .

Dimostrazione. L'affermazione (1) è ovvia. Vogliamo mostrare (2); la seconda disuguaglianza è ovvia perché w è un omomorfismo. Sia K un sottocampo massimale di D e sia $x \in K$. Abbiamo $N_{D/F}(x) = (N_{K/F}(x))^m$,

quindi $\text{nr}_D(x) = N_{K/F}(x)$ per (1.5.9). Questo, usando 2.3.8, ci dice che la restrizione di w a K è un multiplo della valutazione discreta v_K che prolunga v su K ; ora, presi $x, y \in D$ possiamo considerare il sottocampo massimale K tale che $F(x^{-1}y) \subset K$. Abbiamo allora

$$\begin{aligned} v_K(1 + x^{-1}y) &\geq \min\{v_K(1), v_K(x^{-1}y)\} \\ w(1 + x^{-1}y) &\geq \min\{w(1), w(x^{-1}y)\} \\ w(x) + w(1 + x^{-1}y) &\geq \min\{w(x) + w(1), w(x) + w(x^{-1}y)\} \\ w(x + y) &\geq \min\{w(x), w(y)\}. \end{aligned}$$

Da (2) deduciamo che $\|\cdot\|_D$ è una norma, quindi D è uno spazio vettoriale normato su K e, poiché K è completo, deduciamo (3) (vedi [1], cap.I §2). Per finire, perché $x \in D$ sia intero su A , è necessario e sufficiente che $v_K(x) \geq 0$ dove K è un sottocampo massimale di D con $F(x) \subset K$ (vedi la dimostrazione di 2.3.5), il che equivale a $w(x) \geq 0$; l'affermazione (2) ci garantisce che $\{x \in D | w(x) \geq 0\}$ è proprio un anello. \square

Lemma 2.4.2. *Sia $[D : F] = m^2$ con $m \geq 2$, allora esiste un K sottocampo di D , con $F \subset K$, K non ramificato su F e $K \neq F$.*

Dimostrazione. Supponiamo per assurdo che un tale campo non esista; allora per ogni estensione K/F , con $K \subset D$, i campi residui \bar{K} ed \bar{F} coincidono. Se così non fosse, visto che ogni estensione di \bar{F} è separabile, esisterebbe per 2.3.11 una sottoestensione di K , non ramificata su F e distinta da F .

Sia $\pi \in D$ tale che $w(\pi) = 1$ e sia $b \in B$. Abbiamo allora $\overline{F(b)} = \bar{F}$, quindi esiste $a \in A$ con $\bar{b} = \bar{a}$; cioè $w(b - a) \geq 1$, che equivale a

$$b = a + \pi b_1 \quad \text{con } b_1 \in B.$$

Applicando lo stesso ragionamento a b_1 ed iterando abbiamo che, per ogni $N \in \mathbb{N}$, possiamo scrivere

$$b = a + \pi a_1 + \cdots + \pi^{N-1} a_{N-1} + \pi^N b_N, \quad \text{con } a_i \in A, b_N \in B.$$

Questo mostra che b è un punto di accumulazione di $F(\pi)$; però $F(\pi)$, in quanto sottospazio vettoriale di D , è chiuso; quindi $b \in F(\pi)$. Abbiamo

allora dimostrato che $B \subset F(\pi)$, però per ogni $x \in D$ si ha $\pi^m x \in B$ per m abbastanza grande e questo vorrebbe dire che $D = F(\pi)$. Questo è assurdo perché D non è commutativo. \square

Proposizione 2.4.3. *Esiste un sottocampo massimale di D che è non ramificato su F .*

Dimostrazione. Ragioniamo per ricorrenza su m ; il caso $m = 1$ è banale perché $D = F$. Supponiamo allora $m \geq 2$ e supponiamo che il risultato sia vero fino a $m - 1$. Per 2.4.2 esiste F'/F estensione non ramificata, con $F' \subset D$ e $F' \neq F$. Sia $D' = C_D(F')$, allora, per 1.4.7, l'algebra di divisione D' ha come centro F' ; inoltre $[D' : F'] < [D : F] = m^2$. Per ipotesi ricorsiva esiste allora K , sottocampo massimale di D' , con $F' \subset K$, K non ramificato su F' e $F' \neq K$. Il campo K è non ramificato su F , inoltre abbiamo

$$\begin{aligned} [K : F]^2 &= [K : F']^2 [F' : F]^2 \\ &= [D' : F'] [F' : F]^2 \\ &= [D' : F] [F' : F] \\ (\text{per 1.4.8}) &= [D : F]. \end{aligned}$$

E quindi K è un sottocampo massimale di D , sempre per 1.4.8. \square

Quest'ultimo risultato ci dice che ogni algebra di divisione D sul campo locale F , con $[D : F] = m^2$, si può scrivere come prodotto incrociato $D = (K/F, f)$ per un qualche factor set f , dove K/F è un'estensione non ramificata e $[K : F] = m$. Ma, per 2.3.12, per ogni m esiste una sola tale estensione, che indicheremo con K_m ; inoltre $\text{Gal}(K_m/F)$ è ciclico, quindi per 1.7.3 possiamo scrivere

$$D = (K_m/F, \sigma, a),$$

dove σ genera $\text{Gal}(K_m/F)$ e $a \in F^*$.

Chiaramente non tutte le algebre cicliche della forma $(K_m/F, \sigma, a)$ sono algebre di divisione (ad esempio è un'algebra di matrici se $a = 1$, per 1.7.4 (2)); sappiamo solo che sono algebre centrali semplici di dimensione m^2 su F e che ammettono K_m come sottocampo massimale.

Vediamo innanzitutto quante algebre del tipo $(K_m/F, \sigma, a)$ esistono, a meno di isomorfismo. Se fissiamo σ e prendiamo $a, b \in F^*$ abbiamo, per 1.7.4 (3) che

$$(K_m/F, \sigma, a) \simeq (K_m/F, \sigma, b)$$

se e solo se esiste $c \in K^*$ tale che $b = (N_{K/F} c)a$, cioè se e solo se l'equazione

$$N_{K/F} c = ba^{-1}$$

ha soluzione. Per 2.3.14 questo è vero se e solo se

$$\begin{aligned} v(ba^{-1}) &\equiv 0 \pmod{m} \\ v(b) - v(a) &\equiv 0 \pmod{m} \\ v(b) &\equiv v(a) \pmod{m}. \end{aligned}$$

Fissato σ esistono quindi m classi di isomorfismo di algebre corrispondenti alle diverse classi di congruenza modulo m ; se fissiamo $\pi \in A$ tale che $v(\pi) = 1$ possiamo ad esempio prendere $(K_m/F, \sigma, \pi^i)$ con $0 \leq i \leq m - 1$ come rappresentanti.

Supponiamo ora invece di fissare π^i , e sia $\sigma_{K_m/F}$ l'automorfismo di Frobenius di K_m/F , come visto in 2.3.13. Allora $\sigma_{K_m/F}$ è un generatore di $\text{Gal}(K_m/F)$ e tutti gli altri generatori sono del tipo $(\sigma_{K_m/F})^r$ con $(r, m) = 1$, abbiamo allora che tutte le possibilità sono

$$(K_m/F, (\sigma_{K_m/F})^r, \pi^i). \quad \text{con } (r, m) = 1.$$

Però, poiché $(r, m) = 1$, esiste $s \in \mathbb{Z}$, tale che $rs \equiv 1 \pmod{m}$; allora abbiamo $(s, m) = 1$ e, per 1.7.4 (1),

$$(K_m/F, (\sigma_{K_m/F})^r, \pi^i) \simeq (K_m/F, (\sigma_{K_m/F})^r s, \pi^{is}) \simeq (K_m/F, \sigma_{K_m/F}, \pi^{is}).$$

In conclusione, esistono solo m algebre cicliche del tipo $(K_m/F, \sigma, a)$ a meno di isomorfismo e possiamo prendere come insieme di rappresentanti

$$\{(K_m/F, \sigma_{K_m/F}, \pi^s) \mid 0 \leq s \leq m - 1\}.$$

Definizione 2.4.4. Sia A un'algebra del tipo $(K_m/F, \sigma_{K_m/F}, \pi^s)$. Abbiamo visto che la sua classe di isomorfismo dipende solo da $s \bmod m$, cioè dalla frazione $\frac{s}{m}$ vista come elemento del gruppo additivo \mathbb{Q}/\mathbb{Z} . È quindi ben definito l'*invariante di Hasse* di A

$$\text{inv } A = \frac{s}{m} \in \mathbb{Q}/\mathbb{Z}.$$

Teorema 2.4.5. Se $(s, m) = 1$, l'algebra ciclica $(K_m/F, \sigma_{K_m/F}, \pi^s)$ è un'algebra di divisione.

Dimostrazione. L'algebra $A = (K_m/F, \sigma_{K_m/F}, \pi^s)$ è centrale semplice su F e in $\text{Br}(F)$ si ha

$$[A]^t = [(K_m/F, \sigma_{K_m/F}, \pi^{st})].$$

Quindi $\exp_F(A)$ è il più piccolo $t \geq 1$ tale che

$$[(K_m/F, \sigma_{K_m/F}, \pi^{st})] = [F] = [(K_m/F, \sigma_{K_m/F}, 1)].$$

Come abbiamo appena osservato, ciò si verifica se e solo se $st \equiv 0 \pmod{m}$, cioè, poiché $(s, m) = 1$, se e solo se $t \equiv 0 \pmod{m}$. Abbiamo quindi $\exp_F(A) = m$. Per il teorema di Wedderburn, si ha $A \simeq M_r(F) \otimes_F D$ con D algebra di divisione su F . Sia $\text{ind}_F(D) = d$, confrontando le dimensioni abbiamo allora $m^2 = r^2 d^2$, quindi $m = rd$. Ma, per 1.6.20, abbiamo $m|d$, quindi si ha $m = d$ e $r = 1$, il che significa che $A = D$. \square

Teorema 2.4.6. Sia $\frac{s}{m} = \frac{s'}{m'}$ con $(s', m') = 1$, allora

$$[(K_m/F, \sigma_{K_m/F}, \pi^s)] = [(K_{m'}/F, \sigma_{K_{m'}/F}, \pi^{s'})] \quad \text{in } \text{Br}(F).$$

Dimostrazione. Sia K' il sottocampo di K_m fissato dal sottogruppo $\langle (\sigma_{K_m/F})^{m'} \rangle$, allora K'/F è non ramificata e $[K' : F] = m'$, quindi $K' = K_{m'}$. L'omomorfismo suriettivo $\text{Gal}(K_m/F) \rightarrow \text{Gal}(K_{m'}/F)$ porta $\sigma_{K_m/F}$ in $\sigma_{K_{m'}/F}$. Ponendo $d = [K_m : K_{m'}] = \frac{m}{m'}$, abbiamo $s'd = s' \frac{m}{m'} = s$ e segue da 1.7.5 che, in $\text{Br}(F)$,

$$[(K_{m'}/F, \sigma_{K_{m'}/F}, \pi^{s'})] = [(K_m/F, \sigma_{K_m/F}, \pi^{s'd})].$$

\square

Corollario 2.4.7. *L'algebra $A = (K_m/F, \sigma_{K_m/F}, \pi^s)$ è un'algebra di divisione se e solo se $(m, s) = 1$.*

Dimostrazione. La condizione è sufficiente per 2.4.5. D'altra parte se $(s, m) > 1$, sia $D = (K_{m'}/F, \sigma_{K_{m'}/F}, \pi^{s'})$ con $\frac{s}{m} = \frac{s'}{m'}$ e $(s', m') = 1$. Allora in $\text{Br}(F)$, $[A] = [D]$; ma D è un'algebra di divisione, per 2.4.5, quindi è l'unica algebra di divisione nella sua classe di equivalenza in $\text{Br}(F)$, quindi A non è un'algebra di divisione. \square

Abbiamo quindi stabilito che le algebre di divisione centrali su F sono tutte e sole quelle della forma

$$(K_m/F, \sigma_{K_m/F}, \pi^s) \quad \text{con } m, s \in \mathbb{Z} \quad (m, s) = 1.$$

Osservazione 2.4.8. Sia A un'algebra centrale semplice su F . Allora in $\text{Br}(F)$, $[A] = [D]$ con D algebra di divisione centrale su F . Possiamo allora definire l'invariante di Hasse

$$\text{inv } A = \text{inv } D.$$

Per 2.4.6, questa definizione coincide con quella che abbiamo dato in 2.4.4. Abbiamo quindi che l'invariante di Hasse dipende solamente dalla classe $[A] \in \text{Br}(F)$ ed è ben definita un'applicazione inv da $\text{Br}(F)$ in \mathbb{Q}/\mathbb{Z} .

Teorema 2.4.9. *Sia F un campo locale, allora l'applicazione*

$$\text{inv} : \text{Br}(F) \rightarrow \mathbb{Q}/\mathbb{Z}$$

è un isomorfismo di gruppi.

Dimostrazione. L'applicazione inv è suriettiva, perché ogni elemento di \mathbb{Q}/\mathbb{Z} può essere scritto nella forma $\frac{s}{m}$ con $m \geq 1$, $(s, m) = 1$ e quindi è immagine dell'algebra di divisione $(K_m/F, \sigma_{K_m/F}, \pi^s)$.

Sia ora $[A] \in \text{Br}(F)$, allora un rappresentante di $[A]$ è della forma $A = (K_m/F, \sigma_{K_m/F}, \pi^s)$, con $(s, m) = 1$. Allora

$$\text{inv}[A] = \frac{s}{m} = 0$$

se e solo se $s \equiv 0 \pmod{m}$, cioè se e solo se $[A] = [F]$, quindi inv è iniettiva.

Per concludere, vediamo che è un omomorfismo. Se $[A], [B] \in \text{Br}(F)$, per 2.4.6 possiamo trovare $m, s, t \in \mathbb{Z}$ tali che

$$A = (K_m/F, \sigma_{K_m/F}, \pi^s) \quad \text{e} \quad B = (K_m/F, \sigma_{K_m/F}, \pi^t),$$

Abbiamo allora, per 1.7.4,

$$[A][B] = [(K_m/F, \sigma_{K_m/F}, \pi^{s+t})]$$

cioè

$$\text{inv}([A][B]) = \frac{s+t}{m} = \frac{s}{m} + \frac{t}{m} = \text{inv}[A] + \text{inv}[B]$$

quindi inv è proprio un isomorfismo. □

Bibliografia

- [1] N.Bourbaki: *Espaces Vectorielles Topologiques*, Hermann, Paris 1966
- [2] C.W.Curtis, I.Reiner: *Representation theory of finite groups and associative algebras*, Interscience, London, New York 1962
- [3] P.K.Draxl: *Skew fields*, Cambridge University Press, Cambridge, New York, Melbourne, 1983
- [4] I.N.Herstein: *Noncommutative rings*, Mathematical association of America, 1968
- [5] S.Lang: *Algebra*, Addison-Wesley, Reading, London, Sidney, 1971
- [6] I.Reiner: *Maximal orders*, Academic Press, London, New York 1975
- [7] J.P.Serre: *Corps Locaux*, Hermann, Paris 1962