Università degli Studi di Pisa

DIPARTIMENTO DI MATEMATICA
Corso di Laurea Triennale in Matematica

Tesi di laurea triennale

Il gruppo di Brauer di un campo locale

Candidato:
Roberto Pagaria

Relatore:
Angelo Vistoli

Correlatore:
Ilaria Del Corso

Anno Accademico 2013/2014

Indice

Capitolo 1

Introduzione

In questa tesi introduciamo il gruppo di Brauer di un campo, un importante invariante utilizzato in algebra e nella teoria dei numeri.

Nella prima parte trattiamo le nozioni base per definire il gruppo di Brauer, fornendo informazioni sulle algebre, sui moduli e sul prodotto tensore. In particolare definiamo le algebre finite, semplici e centrali (C.S.A.) su un campo e dotiamo l'insieme delle algebre semplici centrali di una relazione d'equivalenza. Solo in seguito definiamo il gruppo di Brauer come l'insieme delle algebre semplici centrali quozientato per la relazione d'equivalenza. Infine dotiamo l'insieme dell'operazione indotta dal prodotto tensore di algebre ottenendo così il gruppo (abeliano) di Brauer. Inoltre parliamo brevemente di campi di spezzamento di algebre e del polinomio caratteristico ridotto di un elemento di un'algebra.

Nella seconda parte iniziamo lo studio del gruppo di Brauer di un campo qualsiasi. Per fare ciò introduciamo i factor set, funzioni dal gruppo di Galois di un'estensione di campi nel campo esteso con particolari proprietà. Per ogni factor set si riesce a costruire un'algebra semplice centrale; risulta naturale introdurre una relazione d'equivalenza sui factor set tale che due factor set sono equivalenti se e solo se generano algebre equivalenti. Il punto fondamentale è mostrare che ogni elemento del gruppo di Brauer è della forma particolare generata da una classe d'equivalenza di factor set. Arriviamo a caratterizzare il gruppo in base alle estensioni di Galois del campo base e alle classi dei relativi factor set. Nel caso di gruppi di Galois ciclici possiamo scegliere rappresentanti di una classe di factor set molto semplici.

Per comprendere meglio il gruppo di Brauer si osserva, senza dimostrare, che i factor set non sono altro che i due cocicli del secondo gruppo di coomologia del gruppo di Galois e che la relazione introdotta non è altro che il quoziente per il sottogruppo dei cobordi.

In seguito definiamo i campi locali, campi dotati di una valutazione discreta, completi rispetto alla metrica indotta e con campo dei residui finito. In questo caso le algebre su campi locali sono dotate di una valutazione e

dimostriamo che le estensioni finite di campi locali sono ancora campi locali. Infine caratterizziamo le estensioni non ramificate di campi locali e i loro gruppi di Galois.

Solo nell'ultimo capitolo definiamo l'invariante di Hasse per un campo locale: un isomorfismo canonico tra il gruppo di Brauer di un campo locale e il gruppo delle radici dell'unità ($\mathbb{Q}/\mathbb{Z}$).

Una profonda conoscenza dei gruppi di Brauer oltre a fornire un invariante per i campi e classificare le algebre su un determinato campo, è necessaria anche in teoria dei numeri. Alcune applicazioni si trovano nella risoluzione del problema inverso di Galois tramite forme quadratiche; infatti è importante conoscere la due-torsione del gruppo di Brauer del campo su cui si vuole risolvere il problema inverso.

Inoltre alcune nozioni sui gruppi di Brauer hanno permesso di trovare controesempi al fatto che una varietà algebrica unirazionale sia anche birazionale (ostruzione di Brauer-Manin).

Capitolo 2

Notazioni

- Ogni volta che parliamo di un anello richiediamo che abbia un unità e solitamente lo chiameremo R. Poiché un algebra è un particolare anello a volte anche gli anelli saranno denotati con la lettera A.
- Gli ideali di un anello sono solitamente denotati con I e J, se si tratta di ideali massimali useremo anche la lettera minuscola m. Per ideali primi useremo le lettere P e Q.
- Un modulo su un anello R sarà indicato con ${}_RM$ se modulo sinistro e M_R se modulo destro.
- I corpi sono denotati con la lattera D. Se sono commutativi, cioè campi, useremo le lettere K, L, F e solitamente K sarà il campo base. Per i campi residui (campi finiti) useremo rispettivamente le minuscole k, l, f.
- Con pc intendiamo il polinomio caratteristico e con pcr il polinomio caratteristico ridotto. A pedice saranno presenti o l'elemento di cui è il polinomio caratteristico o l'estensione di algebre relativa al polinomio.
- Indichiamo la traccia e la norma di un elemento con tr e N. Quando si parla di traccia e norma ridotte useremo trd e Nrd.
- I morfismo tra due oggetti sono indicati con $\mathrm{Hom}_R(V, W)$ che è l'insieme delle funzioni R-lineari da V in W. Indichiamo con $\mathrm{End}_R(V)$ il caso particolare degli endomorfismi di V.
- Come da usuale convenzione gli automorfismi di un campo L di Galois su K (normale e separabile) che fissano gli elemnti di K si indicano con $\mathrm{Gal}_K L$.
- La dimensione di uno spazio vettoriale o di un'algebra viene indicata con $\dim_K(V)$ o con $[A : K]$. Inoltre nel caso di estensioni di campi si

indica la dimensione separabile con $[L : K]_s$ e quella inseparabile con $[L : K]_i$.

Capitolo 3

Algebre

In questa prima parte forniremo definizioni e nozioni necessarie per studiare le algebre e definire il gruppo di Brauer.

Tutte le algebre che tratteremo in questa tesi sono su campi, quindi la definizione che useremo è quella di algebre su campi.

3.1 Definizioni preliminari

Per prima cosa diamo la definizione di algebra e di omomorfismo di algebre:

Definizione 3.1 (K-Algebra)**.** A è una K-algebra se è uno spazio vettoriale su K, è un anello con identità (non necessariamente commutativo) ed il prodotto ($\cdot : A \times A \longrightarrow A$) è K bilineare.

Definizione 3.2 (Omomorfismo di algebre)**.** $f : A \longrightarrow B$ è un omomorfismo di K-algebre se è omomorfismo di anelli che preserva l'unità ed è K lineare.

Definizione 3.3 (Centro)**.** Il centro di un anello (o di un algebra) è l'insieme degli elementi che commutano con tutti gli altri.

$$Z(A) = \{a \in A \mid ax = xa \quad \forall x \in A\}$$

Osservazione 3.4. *Il centro di un anello è un sottoanello.*

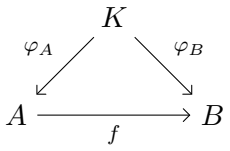
Dimostrazione. Il centro è chiuso per somma, infatti se due elementi a, b appartengono al centro $Z(A)$ allora anche la somma appartiene: $(a+b)x = ax + bx = xa + xb = x(a+b)$.

Il centro è chiuso per prodotto, perché dati due elementi a, b nel centro anche il prodotto appartiene al centro: $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$. □

Le algebre e gli omomorfismi di algebre si possono vedere anche come immersione di un campo in un anello nel seguente modo.

Osservazione 3.5. *Una definizione equivalente di K-algebra è un anello A con un omomorfismo di anelli $\varphi_A : K \longrightarrow Z(A)$.*

Osservazione 3.6. *Una definizione equivalente di omomorfismo di algebre è un omomorfismo f di anelli che conserva l'unità tale che il diagramma*



sia commutativo.

Definizione 3.7. Data un anello A definiamo l'anello opposto A^{opp} come l'anello con la stessa struttra additiva e con la moltiplicazione $\cdot_{\text{opp}} : A \times A \longrightarrow A$ definita da $a \cdot_{\text{opp}} b := b \cdot a$.

Dimostriamo che in anelli non commutativi esistono ideali massimali destri e sinistri, fatto usato spesso in seguito.

Abbiamo due diversi concetti di algebre "finite" (come spazio vettoriale finito o come estensione finita di anelli) che distingueremo con le seguenti definizioni

Definizione 3.8 (Algebra finitamente generata)**.** A è un'algebra finitamente generata se è un estensione finita di anelli.

Definizione 3.9 (Algebra finita)**.** A è un'algebra finita se è finitamente generata come K spazio vettoriale.

Definizione 3.10 (Corpo)**.** D è un corpo o algebra di divisione se è un anello diverso da zero e ogni elemento non nullo è invertibile ($D^* = D \setminus \{0\}$).

Osservazione 3.11. *In un corpo D il suo centro $Z(D)$ è un campo perché $1 \in Z(D)$ per definizione di unità ed è chiuso per addizione e moltiplicazione. Si osserva che D è una $Z(D)$-algebra.*

Questa osservazione spiega perché un corpo è una particolare algebra.

Facciamo alcuni esempi di algebre:

Esempio 1.

- $K[x]$, l'anello dei polinomi in una variabile, è un'algebra finitamente generata e commutativa, ma non finita.
- $\mathbb{H}$, i quaternioni su $\mathbb{R}$, sono una $\mathbb{R}$ algebra di divisione finita generata da $\{1, i, j, k\}$.

- Un'estensione di campi ${}^{L}\!/_{K}$ è una K algebra commutativa e di divisione.
- $\mathcal{M}_n(K)$, le matrici $n \times n$ su K, sono una K-algebra finita non commutativa (se $n > 1$) (che chiameremo algebre di matrici).
- Dato un gruppo G e un campo K sia $K^G = \left\{\sum_{g\in G} k_g x_g \mid k_g \in G\right\}$ allora K^G è una K-algebra con il prodotto definito $x_g \cdot x_h = x_{gh}$ ed esteso per linearità a tutto K^G.

Definizione 3.12. Una K-algebra (A) si dice centrale se $Z(A) = K$.

Diamo la definizione di modulo che ci servirà in seguito per definire le algebre semplici:

Definizione 3.13. Dato un anello R, definiamo M_R un R-modulo destro (rispettivamente ${}_RM$ modulo sinistro) un gruppo additivo con una moltiplicazione per scalare $\cdot : R \times M \longrightarrow M$ (rispetivamente $\cdot : M \times R \longrightarrow M$) che è distributiva a destra (o a sinistra) si rispetto all'addizione di R sia rispetto a quella di M e che sia associativa con la moltiplicazione di R.

Definizione 3.14. $f : M_R \longrightarrow N_R$ è un omomorfismo di R-moduli se è omomorfismi di gruppi additivi e commuta col prodotto per scalare.

Diamo ora la definizione di "semplice" per moduli e algebre.

Definizione 3.15. M un R-modulo è semplice se è un modulo non nullo e non ha sottomoduli non banali.

Proposizione 3.16. *Sia M un R-modulo, allora sono equivalenti:*

1. *Il modulo M è somma di sottomoduli semplici.*
2. *Il modulo M è somma diretta di sottomoduli semplici.*
3. *Per ogni sottomodulo di M esiste un altro sottomodulo tale che sono in somma diretta e che generino tutto il modulo M.*

Se un modulo soddisfa uno dei fatti equivalenti allora si dice semisemplice.

Osservazione 3.17. *Se la proprietà 3 è valida per un modulo M allora è ancora valida per tutti i suoi sottomoduli e quozienti.*

Dimostrazione. Per quanto riguarda i sottomoduli N di M, per ogni sottomodulo di N (P) esiste un complementare in M che chiamiamo P' tale che $P \oplus P' = M$ quindi intersecando con N si ottiene $P \oplus (P' \cap N) = N$.

Vediamo ora che passa ai quozienti. Sia $\bar{P}$ un sottomodulo di ${}^{M}\!/_{N}$ e prendiamo in considerazione il sottomodulo P di M. Esso ha un complementare P' (cioè $P \oplus P' = M$) e la proiezione di $P' + N$ nel quoziente è un complementare di $\bar{P}$. □

Dimostrazione proposizione 3.16.

- $1 \Rightarrow 2$: Per ipotesi il modulo M è somma di sottomoduli semplici M_i ($M = \sum_{i\in I} M_i$). Sia $\mathcal{F}$ l'iniseme dei sottoinsiemi di I tali che i moduli semplici corrispondenti siano in somma diretta.

$$\mathcal{F} = \left\{ J \subseteq I \mid \sum\nolimits_{j\in J} M_j = \bigoplus\nolimits_{j\in J} M_j \right\}$$

  L'insieme $\mathcal{F}$ è parzialmente ordinato per inclusione, non vuoto perché $\emptyset \in \mathcal{F}$, inoltre è un insieme induttivo perchè se $J_k \in \mathcal{F}$ è una catena ascendente allora $J = \cup_k J_k \in \mathcal{F}$ è maggiorante. Dimostro che $J \in \mathcal{F}$, se la somma non fosse diretta allora esisterebbe una combinazione lineare di elementi nulla, $\sum_{j\in J} m_j = 0$ ma solo finiti elementi sono non nulli $m_j \neq 0$, quindi tutti gli $m_j \in J_k$ per k abbastanza grande e ciò implica che tutti gli addendi sono nulli ($m_j = 0$ per ogni $j \in J$). Applichiamo il lemma di Zorn su $\{\mathcal{F}, \subset\}$, quindi esiste $\bar{J}$ massimale. Dimostriamo che $\sum_{j\in\bar{J}} M_j = M$: per assurdo esistesse $i \in I$ tale che $M_i \not\subseteq \bigoplus_{j\in\bar{J}} M_j$ si avrebbe per la semplicità di M_i che $M_i \bigcap \bigoplus_{j\in\bar{J}} M_j = 0$. Ciò implica che $i \cup \bar{J} \in \mathcal{F}$ cosa che contraddice la massimalità di $\bar{J}$.

- $2 \Rightarrow 3$: Uso il lemma di Zorn su

$$\mathcal{F} = \left\{ J \subseteq I \;\middle|\; \left(\bigoplus\nolimits_{j\in J} M_j\right) \bigcap N = 0 \right\}$$

  L'insieme è non vuoto perché $\emptyset \in \mathcal{F}$ e induttivo perché come nel punto precedente se un elemento appartiene a una somma infinita è combinazione lineare di finiti termini. Preso $\bar{J}$ massimale se

$$P := \left(\bigoplus_{j\in\bar{J}} M_j \right) \bigoplus N \subsetneq M$$

  allora esiste $i \in I$ tale che $M_i \not\subset P$ e poichè M_i è semplice allora $M_i \cap P = 0$ e ciò contraddice la massimalità di $\bar{J}$.

- $3 \Rightarrow 1$: Per la dimostrazione serve il seguente lemma.

  Lemma 3.18. *Se M modulo destro soddisfa la condizione 3 allora ogni sottomodulo non nullo ($P \subseteq M$) contiene un modulo semplice.*

  Dimostrazione lemma. Esiste un elemento p in P non nullo, cerco un modulo semplice in $pA \subseteq P$. Sia J ideale massimale contenente l'annullatore di P ($J \supseteq \mathrm{Ann}(p) =: I$). Utilizzando il terzo teorema di omomorfismo di anelli si ha che ${}^{A}\!/_{J} \simeq {}^{A/I}\!/_{I/J} \simeq {}^{pA}\!/_{I/J}$ è sottomodulo semplice di ${}^{P}\!/_{PJ}$ poiché (usando 3) $P \simeq PJ \oplus N'$ posso sollevare ${}^{A}\!/_{J}$ a sottomodulo semplice di P da cui la tesi. □

Riprendiamo la dimostrazione di $1 \Rightarrow 3$, sia $N = \sum_{i \in I} M_i$ dove gli M_i sono tutti i sottomoduli semplici di M. Se $N \subsetneq M$ allora esiste un altro modulo non nullo $N' \neq 0$ tale che $M = N \oplus N'$ dunque, poichè la proprietà 3 passa ai sottomoduli, N' ha un sottomodulo semplice (per lemma 3.18) che però deve stare in N (per definizione di N) e ciò è assurdo.

□

L'osservazione 3.17 afferma che la proprietà 3 passa a sottomoduli e quozienti e di conseguenza anche la proprietà equivalente di essere semisemplice passa a sottomoduli e quozienti.

Definizione 3.19. Un'algebra A si dice semisemplice se è un A-modulo destro semisemplice.

Definizione 3.20. Una K-algebra A è semplice se è un A-modulo destro semisemplice con una unica classe di isomorfismo di moduli semplici.

Forniamo qualche esempio di modulo:

Esempio 2.

- Ogni anello R è un R-modulo destro e sinistro con la moltiplicazione in R.
- Un ideale destro (o sinistro) I di un anello R è un R-modulo destro (o sinistro).
- Un ideale minimale (se esiste) I è un R-modulo semplice.
- Un K-spazio vettoriale V è sia un modulo destro sia un modulo sinistro su K.
- Dato un corpo D, sia D^n il modulo dei vettori a coefficienti in D allora è un $\mathcal{M}_n(D)$-modulo destro semplice, dove l'azione di $\mathcal{M}_n(D)$ è data dalla moltiplicazione matrice - vettore. E' semplice perché dato $v \in D^n$ per ogni $w \in D^n$ esiste una matrice α tale che $\alpha v = w$, quindi ogni sottomodulo destro o è 0 oppure è D^n.

Osserviamo che se abbiamo M_R un R-modulo destro allora possiamo ottenere un R^{opp}-modulo sinistro M^{opp} utilizzando la struttura additiva di M e definendo $\cdot_{\text{opp}} : R^{\text{opp}} \times M \longrightarrow M$ definito come $a \cdot_{\text{opp}} m := m \cdot a$. Si osserva che è ancora un modulo poiché vale la proprietà distributiva e inoltre $(a \cdot_{\text{opp}} b) \cdot_{\text{opp}} m = (b \cdot a) \cdot_{\text{opp}} m = m \cdot (b \cdot a) = (m \cdot b) \cdot a = (b \cdot_{\text{opp}} m) \cdot a = a \cdot_{\text{opp}} (b \cdot_{\text{opp}} m)$ (usando la definizione 3.7).

Enunciamo ora un utile teorema sugli omomorfismi di moduli:

Teorema 3.21. *Per ogni A-modulo M vale* $\text{End}_A(M_A^n) \simeq \mathcal{M}_n(\text{End}_A M_A)$

Dimostrazione. Sia $f \in \mathrm{End}_A(M_A^n)$ e π_j, i_j la proiezione e l'inclusione della j-esima componente in M^n, definiamo $f_{j,k} = \pi_j \circ f \circ i_k$ e la matrice $F \in \mathcal{M}_n(\mathrm{End}_A M)$ con componenti $f_{j,k}$. $\varphi(f) = F$ è omomorfismo di algebre, infatti

$$(\varphi(f \cdot g))_{j,k} = \pi_j \circ f \circ g \circ i_k = \pi_j \circ f \circ \left(\sum_{h=1}^{n} i_h \circ \pi_h \right) \circ g \circ i_k$$
$$= \sum_{h=1}^{n} (\pi_j \circ f \circ i_h) \circ (\pi_h \circ g \circ i_k) = \sum_{h=1}^{n} \varphi(f)_{j,h} \circ \varphi(g)_{h,k}$$

quindi $\varphi(fg) = \varphi(f)\varphi(g)$. Inoltre definiamo $\psi(F) = \{x \mapsto Fx\}$ è un omomorfismo di algebre $\psi : \mathcal{M}_n(\mathrm{End}\, M) \longrightarrow \mathrm{End}(M^n)$ ed è l'inverso di φ quindi le due algebre sono isomorfe. Verifichiamo che ψ sia un omomorfismo di algebre: $\psi(F \cdot G)\, x = (F \cdot G)\, x = F \cdot (G\, x) = F \cdot \psi(G)\, x = \psi(F) \cdot \psi(G)\, x$. □

Teorema 3.22. *Sia A un anello allora vale che $A \simeq \mathrm{End}_A(A_A)$.*

Dimostrazione. L'endomorfismo di A come A-modulo è univocamente determinato dall'immagine di 1 per A linearità. Inoltre per ogni $a \in A$, la moltiplicazione per a a sinistra L_a è un endomorfismo di A che manda 1 in a. L'isomorfismo di A con $\mathrm{End}_A(A)$ è un isomorfismo di algebre perché vale l'uguaglianza $L_{ab} = L_a L_b$. □

3.2 Radicale di Jacobson

Poichè un algebra è anche un anello è utile esibire le relazioni tra il radicale di Jacobson di A e il fatto che sia semisemplice. Per questo forniamo innanzitutto la definizione di radicale di Jacobson.

Definizione 3.23. Sia A un anello, definiamo il radicale di Jacobson $J(A)$ come l'intersezione di tutti gli ideali massimali destri.

Mostriamo per prima cosa che il radicale di Jacobson non può essere l'intero anello. Per fare ciò basta dimostrare che esiste un ideale massimale.

Proposizione 3.24. *In ogni anello esiste un ideale massimale destro (e uno sinistro).*

Dimostrazione. Sia $\mathcal{F}$ la famiglia degli ideali destri (rispettivamente sinistri) propri di un anello A ordinati per inclusione. La famiglia è non vuota perché $\{0\}$ è un ideale destro (rispettivamente sinistro), inoltre è induttiva perché unione arbitraria di una catena di ideali è ancora un ideale. Sia m un elemento massimale della famiglia $\mathcal{F}$ allora è un ideale massimale perché per ogni $x \in A \setminus m$ l'ideale $m + xA$ è un ideale contenente strettamente m quindi non può essere proprio cioè $m + xA = A$. □

Corollario 3.25. *Il radicale di Jacobson di un anello è un ideale proprio.*

La dimostrazione del corollario è immediata conseguenza della proposizione 3.24.

Caratteriziamo in diversi modi il radicale di Jacobson di un anello:

Proposizione 3.26. *Dato un anello A e un suo elemento x sono equivalenti:*

1. *L'elemento x appartiene al radicale di Jacobson.*
2. *Per ogni a di A l'elemento $1 + xa$ è invertibile.*
3. *Per ogni A-modulo destro M semplice abbiamo che $Mx = 0$.*

Dimostrazione.

- $1 \Rightarrow 2$: Se, per assurdo, $1+xa$ non è invertibile a destra allora esiste M ideale massimale destro che contiene $1+xa$, ma $x \in J(A) \subseteq M$ quindi otteniamo l'assurdo che $1 \in M$. Abbiamo dimostrato che ogni elemento della forma $1 + xa$ è invertibile a destra, ora vogliamo dimostrare che $1 + xa$ è invertibile a sinistra. Prendiamo $u \in A$ inverso destro di $1 + xa$ (cioè $(1 + xa)u = 1$), dimostriamo che u è invertibile a destra e di conseguenza l'inverso a destra e a sinistra di u coincidono (che è proprio $1+xa$) e concludiamo che $u(1+xa) = 1$. Per dimostrare che u è invertibile a destra usiamo la definizione di u ottenendo l'uguaglianza $u = 1 - xau$; in particolare u è ancora della forma $1 + xa'$ e per quanto appena detto è invertibile a destra. Ciò dimostra che $1 + xa$ è invertibile.

- $2 \Rightarrow 1$: Se, per assurdo, esistesse un ideale massimale M non contenente x allora $M + xA$ sarebbe ideale destro che contiene strettamente un massimale, quindi coinciderebbe con l'intero anello. Dunque $m + xa = 1$ e per ipotesi $m = 1 - xa = 1 + x(-a)$ è invertibile da cui l'assurdo perché M è proprio.

- $1 \Rightarrow 3$: Dato x nel radicale di Jacobson, per ogni elemento $m \in M$ definisco l'omomorfismo $\varphi_m : A \longrightarrow M$ come $\varphi_m(a) = ma$ e otteniamo l'isomorfismo tra $A/\ker\varphi$ e M. Essendo M semplice il nucleo di φ_m è ideale massimale e quindi $x \in \ker\varphi_m$ da cui la tesi $Mx = 0$.

- $3 \Rightarrow 1$: Dimostro la contronominale, cioè se x non è nel radicale di Jacobson allora esiste un modulo semplice M tale che $Mx \neq 0$. Per definizione 3.23 esiste un ideale massimale destro I tale che x non appartiene a I quindi A/I è semplice e $\left(A/I\right) x \neq 0$.

□

L'ultima caratterizzazione implica che $J(A)$ è anche un ideale sinistro e quindi bilatero. Infatti $x \in J(A) \implies (Ma)x = 0 \iff M(ax) = 0 \iff ax \in J(A)$ osservando che se M è semplice allora lo è anche Ma.

La proposizione 3.26 vale anche se si definisce $J'(A)$ l'intersezione di tutti gli ideali sinistri massimali con identica dimostrazione.

Lemma 3.27. *L'elemento x appartiene al radicale di Jacobson se e solo se per ogni $a, b \in A$ l'elemento $1 + axb$ è invertibile se e solo se appartiene a $J'(A)$.*

Dimostrazione. Dimostriamo la prima equivalenza. Se l'elemento ax è nel radicale di Jacobson perciò applichiamo la proposizione 3.26 e otteniamo che l'elemento $1 + (ax)b$ è invertibile. Viceversa se per ogni a e b l'elemento $1 + axb$ è invertibile allora sostituiamo ad a il valore 1 e applichiamo la proposizione 3.26 quindi x è nel radicale di Jacobson.

Per la seconda equivalenza applichiamo lo stesso ragionamento su $J'(A)$. Se x appartiene a $J'(A)$, l'elemento xb è nell'ideale bilatero $J'(A)$ quindi $1 + a(xb)$ è invertibile. Viceversa imponendo $b = 1$ si ottiene che $1 + ax$ è invertibile per ogni $a \in A$ e quindi x appartiene a $J'(A)$. □

Il lemma afferma che il radicale di Jacobson coincide con l'intersezione di tutti gli ideali massimali sinistri. Riassumiamo le proprietà del radicale di Jacobson già dimostrate.

Osservazione 3.28.

1. *Il radicale di Jacobson coincide con l'intersezione di tutti gli ideali massimali sinistri.*
2. *L'elemento x appartiene al radicale di Jacobson se e solo se per ogni $a, b \in A$ l'elemento $1 + axb$ è invertibile.*
3. *L'elemento x appartiene al radicale di Jacobson se e solo se per ogni A-modulo destro (o sinistro) M semplice si ha che $Mx = 0$ (o rispettivamente $xM = 0$).*

Trattiamo ora il caso particolare in cui A è un algebra finita su un campo.

Teorema 3.29. *Se A è algebra finita su K allora è semisemplice se e solo se $J(A) = 0$.*

Dimostrazione. Supponiamo che A sia semisemplice ($A \simeq \bigoplus_{i \in I} V_i$) e dimostriamo $J(A) = 0$. Essendo A di dimensione finita la somma è solo su finiti indici $A \simeq \bigoplus_{i \leq n} V_i$ dove gli V_i sono moduli semplici. Per ogni modulo semplice V_i vale che $V_i J(A) = 0$ per la proprietà 3 e quindi $AJ(A) = \bigoplus_{i \leq n} V_i J(A) = 0$ e otteniamo la tesi $J(A) = 0$.

Viceversa se $J(A) = 0$ esistono finiti ideali massimali con intersezione vuota poiché sono sottospazi vettoriali di dimensione finita di A. Definiamo

l'applicazione $\varphi : A \longrightarrow \prod_{i\leq n} {}^{A}\!/_{M_i}$ ed è iniettiva perchè $\ker\varphi = \bigcap_{i\leq n} M_i = J(A) = 0$, dunque A è sottomodulo di un modulo semisemplice quindi è semisemplice. □

Teorema 3.30. *Se A è un algebra finita allora è semplice se e solo se è diversa da zero e non ha ideali bilateri non banali.*

Dimostrazione. Se A non ha ideali bilateri non banali allora $J(A) = 0$ perché bilatero e diverso dall'intero anello, quindi per il teorema 3.29 A è semisemplice. Utilizzando la semisemplicità di A possiamo scrivere l'anello come somma diretta di moduli semplici $A = \bigoplus_{i\leq m} V_i = \bigoplus_{i\leq n} A_i$ dove gli V_i sono moduli semplici e A_i sono somme dirette di tutti i moduli semplici isomorfi tra loro ($A_i = \bigoplus_{j\in J} V_{i_j}$). Mostriamo che ogni A_i è ideale bilatero, quindi esiste un indice i tale che $A_i = A$ e di conseguenza A è algebra semplice. Per ogni $a \in A$ definiamo l'omomorfismo di moduli destri $L_a : A \longrightarrow A$ definito da $L_a(x) = ax$, esso si restringe a $L_i : A_i \longrightarrow A_i$ perché $L(V_i)$ o è isomorfo a V_i o è nullo. Questo dimostra che A_i è anche un ideale sinistro e quindi bilatero.

Dimostriamo l'altra implicazione per assurdo, supponiamo che esista I ideale bilatero non nullo e vogliamo dimostrare che I è l'intero anello. Poichè A è semisemplice allora esiste un ideale destro complementare a I tale che $A = I \oplus J$ e i due ideali saranno della forma $I = V^{\oplus r}$ e $J = V^{\oplus s}$ perché esiste unica classe di omomorfismo di moduli semplici. Osserviamo che r è positivo perché l'ideale I è non nullo. Guardiamo ora gli automorfismi di A come A modulo. Sappiamo dal teorema 3.22 che $\mathrm{End}_A(A_A) \simeq A$, di conseguenza ogni endomorfismo di A manda I in se stesso. Ciò è possibile solo se non ci sono altri V fuori da I cioè $s = 0$ quindi $J = 0$ da cui la tesi $I = A$. □

Un altro fatto interessante sulle algebre finite è il seguente:

Proposizione 3.31. *Se A è finita allora esiste un naturale n tale che $J(A)^n = 0$*

Dimostrazione. La catena di ideali $J(A) \supseteq J(A)^2 \supseteq \cdots \supseteq J(A)^n \supseteq \cdots$ è stazionaria perché A è artiniano. Esiste n tale che $J(A)^n = J(A)^{n+1}$ sia $M = J(A)^n$ A-modulo finitamente generato perché sottospazio vettoriale di spazio vettoriale di dimensione finita, applichiamo il lemma di Nakayama su $M = MJ(A)$ quindi $M = 0$. □

3.3 Teorema di struttura

In questa sezione dimostriamo un teorema di struttura delle algebre finite, noto come teorema di Wedderburn. Iniziamo con alcuni fatti preliminari:

Lemma 3.32 (di Schur)**.** *Se M è un R-modulo semplice allora* $\mathrm{End}_R(M)$ *è un'algebra di divisione.*

Dimostrazione. Per ogni $f \in \mathrm{End}_R(M)$, il nucleo di f è sottomodulo di M, poichè M è semplice o $f = 0$ oppure f è iniettiva. Inoltre anche l'immagine di f è un sottomodulo di M quindi, essendo l'immagine non nulla, la funzione f è suriettiva. Esiste l'inverso di f ed è ancora un omomorfismo di R-moduli. □

Nell'esempio 2 abbiamo esibito un modulo semplice sulle matrici, ora mostriamo che tutti i moduli semplici sono di quella forma.

Lemma 3.33. *Sia M un $\mathcal{M}_n(D)$-modulo semplice allora $M \simeq D^n$ come $\mathcal{M}_n(D)$ moduli.*

Dimostrazione. Un modulo semplice M è diverso dal modulo nullo e quindi ha un elemento m non nullo. Sia $f : \mathcal{M}_n(D) \longrightarrow M$ un omomorfismo di $\mathcal{M}_n(D)$-moduli definito da $f(\alpha) = \alpha m$, poiché $\mathcal{M}_n(D) \simeq (D^n)^{\oplus n}$ come $\mathcal{M}_n(D)$-moduli la funzione $f : (D^n)^{\oplus n} \longrightarrow M$ si può spezzare sulle componenti $f_i : D^n \longrightarrow M$. Inoltre $f \neq 0$ perché $m \neq 0$ quindi una delle f_i è non nulla. Sia i l'indice di una componente non nulla allora f_i è omomorfismo tra moduli semplici non nullo, quindi per il lemma 3.32 è un isomorfismo, da cui la tesi. □

Proposizione 3.34. *Un'algebra di matrici su D corpo è semplice (come algebra).*

Dimostrazione. L'algebra $\mathcal{M}_n(D)$ è somma diretta di n moduli semplici (D^n) come dimostrato nell'esempio 2 quindi è un modulo semisemplice. Inoltre i moduli semplici sono tutti isomorfi quindi (per definizione 3.20) $\mathcal{M}_n(D)$ è un'algebra semplice. □

Enunciamo ora un lemma utile per la dimostrazione del teorema di struttura.

Lemma 3.35. *Sia D un corpo e V un modulo sinistro su D finitamente generato, chiamando $A = \mathrm{End}_D^{opp}(V)$ allora $D \simeq \mathrm{End}_A(V_A)$*

Dimostrazione. Dimostriamo che V_A è semplice come A-modulo perchè la moltiplicazione per elementi di A è l'applicazione di D-omomorfismi che agiscono in modo transitivo su ${}_DV$. Chiamiamo $E = \mathrm{End}_A(V_A)$ che è un corpo per il lemma di Schur (3.32) e $D \subseteq E$. Inoltre vale $A \subseteq \mathrm{End}_E^{opp}(V) \subseteq \mathrm{End}_D^{opp}(V) = A$ dove la seconda inclusione è data dal fatto che gli endomorfismi scambiano le inclusioni fra E e D. $\mathrm{End}_D(V) = \mathrm{End}_E(V)$ implica che $\dim_D V = \dim_E V \cdot \dim_D E = \dim_E V$ da cui si ottiene che $E = D$. □

Finalmente possiamo dimostrare il teorema di struttura della algebre semisemplici noto anche come teorema di Wedderburn che useremo in seguito per dare la definizione di gruppo di Brauer.

Teorema 3.36 (di Wedderburn)**.** *Un'algebra semisemplice si decompone come prodotto di algebre di matrici su corpi:*

$$A \simeq \prod_{i=1}^{r} \mathcal{M}_{n_i}(D_i)$$

e la decomposizione è unica a meno di isomorfismo dei D_i e dell'ordine dei prodotti.

Dimostrazione. Dimostriamo prima l'esistenza.

Siano $V_1, \dots, V_r$ moduli destri semplici rappresentanti delle classi di isomorfismo di moduli semplici e definiamo $D_i = \mathrm{End}_A(V_i)$ e gli endomorfismi formano un corpo per il lemma di Schur (3.32). Un algebra semisemplice è somma diretta dei suoi moduli semplici $A \simeq \bigoplus_{i=1}^{r} V_i^{n_i}$ e usando i teoremi 3.21 e 3.22 otteniamo:

$$A \simeq \mathrm{End}_A(A_A) \simeq \mathrm{End}_A\left(\bigoplus_{i=1}^{r} V_i^{n_i}\right) \simeq \prod_{i=1}^{r} \mathrm{End}_A(V_i^{n_i}) \simeq$$
$$\simeq \prod_{i=1}^{r} \mathcal{M}_{n_i}\left(\mathrm{End}_A(V_i)\right) \simeq \prod_{i=1}^{r} \mathcal{M}_{n_i}(D_i)$$

dove il terzo isomorfismo si ottiene dal fatto che gli endomorfismi di moduli semplici mandano il modulo in uno isomorfo o in zero.

Dimostriamo l'unicità, supponiamo che esistano due scritture come prodotto di algebre di matrici:

$$\prod_{i=1}^{r} \mathcal{M}_{n_i}(D_i) \simeq \prod_{i=1}^{s} \mathcal{M}_{m_i}(E_i)$$

osserviamo che $r = s$ perché sono il numero di classi di isomorfismo di A-moduli semplici. Sia per ogni indice i i moduli V_i e $E_i^{m_i}$ sono isomorfi perchè $E_i^{m_i}$ è modulo semplice su $\mathcal{M}_{m_i}(E_i)$ allora per il lemma 3.35 vale $E_i = \mathrm{End}_{\mathcal{M}_{m_i}(E_i)}(E_i^{m_i}) = \mathrm{End}_A(V_i) = D_i$, quindi i corpi sono isomorfi due a due. Infine $n_i = \dim_{D_i}(V_i) = \dim_{E_i}(V_i) = m_i$ e ciò conclude la dimostrazione dell'unicità. □

La seguente definizione generalizza quella già data per le algebre di divisione (3.12).

Definizione 3.37. Un'algebra A su K è algebra semplice centrale (C.S.A.) se è un algebra semplice (che per il teorema di Wedderburn è isomorfa ad un'algebra di matrici su un corpo) e il suo centro è K (cioè $Z(A) = K$).

Capitolo 4

Gruppo di Brauer

Prima di parlare del gruppo di Brauer ricordiamo la proprietà universale del prodotto tensore di due moduli.

4.1 Prodotto tensore

Definiamo il prodotto tensore di due moduli su un anello non commutativo e in seguito vediamo il caso del prodotto tensore di due K-algebre.

Definizione 4.1. Una mappa $f : M_R \times_R N \longrightarrow P$ si dice bilanciata se $\forall\, r \in R, m \in M$ e $n \in N$ vale $f(mr, n) = f(m, rn)$.

Definizione 4.2. Dato un R-modulo destro M e un R-modulo sinistro N esiste un unico gruppo abeliano $M \otimes_R N$ e una unica mappa bilanciata $\pi : M_R \times_R N \longrightarrow M \otimes N$ tale che per ogni gruppo abeliano P e per ogni mappa bilanciata $f : M_R \times_R N \longrightarrow P$ esiste unico omomorfismo di gruppi $\tilde{f}$ abeliani tale che il seguente diagramma commuti.

$$\begin{array}{ccc} M_R \times_R N & \xrightarrow{f} & P \\ {\scriptstyle\pi}\downarrow & \nearrow_{\tilde{f}} & \\ M \otimes N & & \end{array}$$

Per la buona definizione bisogna fare molte verifiche standard che non vengono riportate qui. Inoltre daremo per note le seguenti proprietà del prodotto tensore.

Proposizione 4.3.

1. *Il prodotto tensore è distributivo con la somma diretta ($\oplus$).*
2. *Se M è anche un S-modulo sinistro allora $M \otimes_R N$ è un S-modulo sinistro e vale la proprietà universale con moduli sinistri.*

3. *Se N è anche un S-modulo destro allora $M \otimes_R N$ è un S-modulo destro e vale la proprietà universale con moduli destri.*

4. *Sia N un R-modulo sinistro allora $R \otimes_R N \simeq N$ come R-moduli sinistri.*

5. *Il prodotto tensore è associativo, cioè se L è un R-modulo destro, M un (R, S)-bimodulo e N un S-modulo sinistro allora $(L \otimes_R M) \otimes_S N \simeq L \otimes_R (M \otimes_S N)$.*

Dimostrazione. La dimostrazione di questi fatti si trova nel libro di Lang [4, pp 601-612]. □

Possiamo anche definire il prodotto tensore di due omomorfismi in modo tale da poter vedere il prodotto tensore come funtore.

Definizione 4.4. Dato $f : M \longrightarrow M'$ un omomorfismo di moduli destri e $g : N \longrightarrow N'$ un omomorfismo di moduli sinistri definiamo $f \otimes g : M \otimes_R N \longrightarrow M' \otimes_R N'$ l'unico omomorfismo di gruppi abeliani tali che $(f \otimes g)(m \otimes n) = f(m) \otimes f(n)$ per ogni $m \in M$ e $n \in N$ o equivalentemente che il diagramma commuti.

$$\begin{array}{ccc} M \times N & \xrightarrow{(f,g)} & M' \times N' \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ M \otimes_R N & \xrightarrow[f \otimes g]{} & M' \otimes_R N' \end{array}$$

Analogamente si può definire il prodotto tensore di due algebre.

Definizione 4.5. Date due K-algebre A e B allora $A \otimes B$ è K-algebra col prodotto definito da $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ ed esteso per linearità a $A \otimes B$. Equivalentemente si può vedere il prodotto come prodotto tensore delle funzioni prodotto di A e di B osservando che il diagramma commuta.

$$\begin{array}{ccc} A \otimes A \otimes B \otimes B & \xrightarrow{\cdot_A \otimes \cdot_B} & A \otimes B \\ \downarrow & \nearrow{\scriptstyle \cdot_{A \otimes B}} & \\ A \otimes B \otimes A \otimes B & & \end{array}$$

Nel caso in cui B sia un campo otteniamo la nota operazione di estensione di scalari:

Osservazione 4.6. *Se L è un estensione di campi su K allora $A \otimes_K L$ è una L-algebra col prodotto definito dall'immersione canonica $L \hookrightarrow 1 \otimes L \subseteq A \otimes_K L$.*

Osservazione 4.7. *Se f, g sono due mappe non nulle tra K-algebre allora $f \otimes g$ è una mappa tra K-algebre non nulla.*

Enunceremo due teoremi sul prodotto tensore che serviranno in seguito per dimostrare le proprietà dei campi di spezzamento di algebre, ma trovano anche utili applicazioni in teoria delle rappresentazioni su campi non algebricamente chiusi.

Vediamo ora l'estensione sinistra L-lineare di algebre e moduli.

Teorema 4.8. *Sia L un estensione di K, A una K-algebra e B una L-algebra allora*

$$\mathrm{Hom}_K(A, B) \otimes_K L \hookrightarrow \mathrm{Hom}_L(A \otimes_K L, B)$$

Dimostrazione. Definiamo l'omomorfismo iniettivo φ che manda f in $f \otimes 1 : A \otimes L \longrightarrow B \otimes L \simeq B$ si estende a $\tilde{\varphi}$ omomorfismo L-lineare. $\tilde{\varphi}$ è iniettivo perché φ è iniettivo (osservazione 4.7). □

Inoltre vale un risultato analogo con i moduli.

Teorema 4.9. *Dati due K-moduli V e W e un'estensione di campi L/K allora la mappa $\varphi : \mathrm{Hom}_K(V, W) \otimes_K L \hookrightarrow \mathrm{Hom}_L(V \otimes_K L, W \otimes_K L)$ è iniettiva.*

Inoltre se L/K è finita o $\dim_K V$ è finita allora è anche suriettiva, quindi isomorfismo di moduli.

Dimostrazione. La mappa è definita da $\varphi(f \otimes l) = f \otimes R_l$, dove R_l è la moltiplicazione per l, è iniettiva per osservazione 4.7. Nel primo caso in cui l'estensione di campi è finita di grado $n = [L : K]$ sia $\{l_i\}$ base di L/K definisco per ogni omomorfismo L-lineare $g(v \otimes 1) = \sum_{i=1}^{n} w_i \otimes l_i$ le funzioni $f_i(v) = w_i$ K-lineari vale:

$$\varphi\left(\sum_{i=1}^{n} f_i \otimes l_i\right) = g$$

Nel secondo caso in cui $\dim_K V = n$ si ottiene:

$$\mathrm{Hom}_K(V, W) \otimes_K L \simeq (W^n) \otimes_K L \simeq (W \otimes_K L)^n \simeq \mathrm{Hom}_L(V \otimes_K L, W \otimes_K L)$$

□

I seguenti fatti ci serviranno per dimostrare la buona definizione del gruppo di Brauer.

Proposizione 4.10. *Se A e B sono due K-algebra allora $\mathcal{M}_n(A) \otimes_K B \simeq \mathcal{M}_n(A \otimes_K B)$.*

Dimostrazione. La mappa $\varphi : \mathcal{M}_n(A) \otimes_K B \longrightarrow \mathcal{M}_n(A \otimes_K B)$ definita da $\varphi((a_{i,j}) \otimes b) = (a_{i,j} \otimes b)$ ed estesa per linearità a tutto il prodotto tensore è biunivoca e rispetta le operazioni. □

Corollario 4.11. *Vale che*

$$\mathcal{M}_n(K) \otimes_K \mathcal{M}_m(K) \simeq \mathcal{M}_n(\mathcal{M}_m(K)) \simeq \mathcal{M}_{nm}(K)$$

Dimostrazione. Applichiamo la proposizione 4.10 con $A = K$ e $B = \mathcal{M}_m(K)$ e otteniamo il primo isomorfismo $\mathcal{M}_n(K) \otimes_K \mathcal{M}_m(K) \simeq \mathcal{M}_n(\mathcal{M}_m(K))$, il secondo isomorfismo si ottiene mandando gli elementi $A^{i,j}$ della matrice nei minori della matrice $nm \times nm$ di dimensione $m \times m$ e verificando che si comporta bene con le operazioni. □

4.2 Definizione del gruppo di Brauer

Definiamo una relazione di equivalenza sull'insieme delle K-algebre semplici centrali definite sopra (3.37):

$$A \sim B \iff A = \mathcal{M}_n(D),\ B = \mathcal{M}_m(E)\ e\ D \simeq E$$

Cioè due algebre sono in relazione se contengono lo stesso corpo. Per ora prendiamo come rappresentante privilegiato di $[A]$ l'algebra di divisione D.

Vediamo che il prodotto tensore di due algebre semplici centrali è ancora semplice centrale.

Teorema 4.12. *Se A è una K-algebra centrale e B un'algebra contenente K ed entrambe non contengono ideali bilateri non banali allora $A \otimes_K B$ non ha ideali bilateri non banali. Inoltre $Z(A \otimes_K B) = 1 \otimes_K Z(B)$.*

Dimostrazione. Dimostriamo prima la relazione tra i centri delle due algebre. Prendiamo $\{b_i\}_{i \in I}$ base di B quindi ogni elemento x di $A \otimes B$ si scrive in modo unico nel seguente modo:

$$x = \sum_{i \in I} a_i \otimes b_i$$

Supponiamo che x appartenga al centro allora $(a \otimes 1)x = x(a \otimes 1) \implies \sum_{i \in I} aa_i \otimes b_i = \sum_{i \in I} a_i a \otimes b$ e questo implica che ogni $a_i \in Z(A) = K$, quindi x è della forma $1 \otimes b$ con $b \in Z(B)$. Viceversa è ovvio che $1 \otimes Z(B) \subseteq Z(A \otimes B)$.

Dimostriamo ora che $A \otimes B$ non ha ideali bilateri. Supponiamo per assurdo che esista I ideale bilatero $0 \neq I \subsetneq A \otimes B$. Scegliamo $x \in I$ diverso da zero tale che la scrittura $x = \sum_{i=1}^{r} a_i \otimes b_i$ abbia il numero minimo di addendi ($r > 0$ minimo), cio implica che $\{a_i\}_{i \leq r}$ e $\{b_i\}_{i \leq r}$ sono successioni di elementi linearmente indipendenti. Poichè A non ha ideali bilateri allora

$Aa_1A = A$ cioè esistono $\{u_i\}$ e $\{v_i\}$ tali che $\sum_{i\leq r} u_i a_1 v_i = 1$. Chiamiamo $y = \sum_{i\leq r}(u_i \otimes 1)x(v_i \otimes 1) = 1 \otimes b + \sum_{i=2}^{r} a'_i \otimes b_i$, per ogni $a \in A \quad (a \otimes 1)y - y(a \otimes 1) = \sum_{i=2}^{r}(aa'_i - a'_i a) \otimes b_i \in I$. Per la minimalità di r abbiamo che ogni addendo è nullo cioè $a'_i \in Z(A) = K$ per ogni indice i di conseguenza $r = 1$ e $y = 1 \otimes b$ ma allora poiché B non ha ideali bilateri allora $1 \otimes 1 \in I$ e questo porta all'assurdo perché I è proprio. □

Corollario 4.13. *Il prodotto tensore di due algebre semplici centrali è un'algebra semplice centrale.*

Dimostrazione. Per il teorema 3.30 nel caso di algebre finite non avere ideali bilateri è equivalente ad essere semplice. Inoltre l'ipotesi $Z(B) = K$ implica che $A \otimes B$ è centrale. □

Finalmente diamo la definizione del gruppo di Brauer.

Definizione 4.14 (Gruppo di Brauer)**.** Per ogni campo K definiamo il gruppo abeliano

$$\mathrm{Br}(K) = \{[A] \mid A \textit{ è algebra semplice centrale}\}$$

con l'operazione definita da $[A] \cdot [B] = [A \otimes_K B]$.

Proposizione 4.15. *La definizione (4.14) del gruppo di Brauer è ben posta.*

Dimostrazione. Verifichiamo che il prodotto $\cdot$ sia ben definita innanzitutto il corollario 4.13 $A \otimes_K B$ è semplice centrale. Vediamo che non dipende dalla classe di equivalenza, se $A = \mathcal{M}_n(D)$ allora $[A] \cdot [B] = [\mathcal{M}_n(D) \otimes_K B] = [M_n(D \otimes_K B)] = [D \otimes_K B]$ dove per la secondo uguaglianza abbiamo usato la proposizione 4.10. Inoltre l'operazione è commutativa perché lo è il prodotto tensore di algebre.

L'elemento neutro del prodotto è $[K]$ infatti la proposizione 4 implica che $[A] \cdot [K] = [A]$. L'associatività discende direttamente dall'associatività del prodotto tensore. Per dimostrare l'esistenza dell'inverso ci serve il seguente lemma.

Lemma 4.16. *Se A è una K-algebra semplice centrale e $\dim_K A = n$ allora $A \otimes_K A^{opp} \simeq \mathcal{M}_n(K)$*

Dimostrazione. Se definiamo l'azione di $A \otimes A^{opp}$ su A data da $(a \otimes b)x = axb$ (si comporta bene con la composizione) ed è un omomorfismo di anelli K-lineare. Essendo $A \otimes_K A$ un'algebra semplice centrale, ogni suo elemento non nullo induce un endomorfismo di A non nullo, quindi $A \otimes A^{opp} \subseteq \mathrm{End}_K(A) \simeq \mathcal{M}_n(K)$. Guardando le diminsioni su K come K-spazi vettoriali si ottiene l'uguaglianza infatti $\dim_K A \otimes A^{opp} = \dim_K A \cdot \dim_K A^{opp} = n^2 = \dim_K (\mathcal{M}_n(K))$. □

Osservando che se A è semplice centrale allora lo è anche A^{opp}, il lemma implica banalmente che $[A]\cdot[A^{opp}] = [K]$ e quindi l'inverso di $[A]$ è $[A^{opp}]$. □

Forniamo alcuni esempi di gruppi di Brauer senza darne dimostrazione immediata.

Esempio 3.

- Se K è algebricamente chiuso $\mathrm{Br}(K) = 0$.
- $\mathrm{Br}(\mathbb{R}) = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.
- Ogni campo finito F ha gruppo di Brauer banale ($\mathrm{Br}(F) = 0$).
- Se K è un campo locale allora $\mathrm{Br}(K) = {}^{\mathbb{Q}}\!/_{\mathbb{Z}}$.

Osserviamo che se K è algebricamente chiuso allora la sola algebra di divisione finita su K è K stesso. Infatti se esistesse $x \in D \neq K$ allora $K(x)$ sarebbe un estensione di campi di dimesione finita su K, ma ciò e assurdo perché K è algebricamente chiuso. Quindi abbiamo dimostrato il primo esempio.

4.3 Campi di spezzamento

Per uno studio più approfondito di algebre di divisione e gruppo di Brauer bisogna introdurre i campi di spezzamento di algebre e studiarne le loro proprietà. Cosa che faremo in questa parte e tornerà utile in seguito soprattutto per la costruzione di alcune algebre.

Osservazione 4.17. *Data un estensione di campi ${}^{L}\!/_{K}$ esiste un omomorfismo di gruppi $\varphi : \mathrm{Br}(K) \longrightarrow \mathrm{Br}(L)$ tale che:*

$$\varphi([A]) = [A \otimes_K L]$$

Dimostrazione. Verifichiamo che la funzione φ è ben definita, infatti per il teorema 4.12 $A \otimes_K L$ è un'algebra semplice e il centro è L. Inoltre la funzione φ non dipende dal rappresentante scelto, basta verificare che se A è un'algebra di matrici su un corpo D allora $[A \otimes_K L] = [D \otimes_K L]$. L'isomorfismo $\mathcal{M}_n(D) \otimes_K L \simeq \mathcal{M}_n(D \otimes_K L)$ dimostra che la funzione φ è ben definita. Infine verifichiamo che è un isomorfismo di gruppi. Date due algebre semplici centrali A, B verifichiamo che $\varphi([A][B]) = \varphi([A])\varphi([B])$, infatti $(A \otimes_K B) \otimes_K L = (A \otimes_K L) \otimes_L (B \otimes_K L)$ quindi φ è un omomorfismo. □

Definizione 4.18. Un campo L si dice di spezzamento per una K-algebra A se $[A] \in \ker \varphi$ cioè se $A \otimes_K L \simeq \mathcal{M}_n(L)$

Osserviamo che, per definizione, essere un campo di spezzamento è proprietà di classe.

Enunciamo un noto teorema per poter parlare di composto di due campi. Nel caso in cui due campi E e L sono contenuti in un altro campo F per definire il composto basta definirlo come l'intersezione di tutti i campi contenuti in F che contengono E ed L. In questo caso il composto è unico. In generale è necessario il seguente teorema ma non abbiamo l'unicità.

Teorema 4.19. *Dati due campi E ed L contenenti lo stesso campo K allora esiste il campo composto (denotato con EL) nel quale si immergono i due campi.*

Dimostrazione. Prendiamo in considerazione l'algebra $L \otimes_K E$, essa vista come anello commutativo ha un ideale bilatero massimale m. Definiamo il composto come il quoziente ${}^{L \otimes_K E}\!/_{m}$ e verifichiamo che E ed L si immergono in ${}^{L \otimes_K E}\!/_{m}$ che è un campo per massimalità di m. Prendiamo in considerazione l'immersione $\varphi : L \longrightarrow L \otimes_K E$ e la componiamo con la proiezione al quoziente π, l'omomorfismo $\pi \circ \varphi$ è un omomorfismo di campi e se non è nullo è un isomorfismo. Verifichiamo che non è nullo perché l'unità di L viene mandata nell'unità di $L \otimes_K E$ che non è contenuta nel nucleo della proiezione. In conclusione il campo L si immerge in ${}^{L \otimes_K E}\!/_{m}$ e analogamente si immerge E. □

Enunciamo utili fatti sulle algebre semplici centrali.

Proposizione 4.20. *La dimensione di un algebra semplice centrale* $\dim_K A$ *è un quadrato.*

Dimostrazione. Per ogni algebra A esiste un campo di spezzamento, infatti $A \otimes_K \overline{K} = M_n(\overline{K})$ e sapendo che $\dim_K A = \dim_{\overline{K}} A \otimes_K \overline{K} = n^2$ si conclude che $\deg_K A$ è sempre un intero positivo. □

Definizione 4.21 (grado)**.** Si dice grado di un algebra semplice centrale l'intero $\deg_K A = \sqrt{\dim_K A}$.

Definizione 4.22 (indice di Schur)**.** Data A una K-algebra semplice centrale definiamo l'indice di Schur $\mathrm{ind}_K(A) = \deg_K(D)$ con A algebra di matrici sul corpo D.

Notare che la definizione precedente non dipende dal corpo D ma solo dalla sua dimensione su K che è invariante per isomorfismo e che l'indice è sempre intero.

Proposizione 4.23. *Per ogni A algebra semplice centrale e per ogni campo di spezzamento L si ha che* $\mathrm{ind}_K A \mid \dim_K L$.

Dimostrazione. Poichè per il teorema di Wedderburn (3.36) $A = \mathcal{M}_m(D)$, $\operatorname{ind}_K A = \operatorname{ind}_K D$ e L è campo di spezzamento anche per D perché è una proprietà sulle classi ($[A] = [D]$) allora ci possiamo ridurre al caso in cui $A = D$ algebra di divisione. Per definizione di campo di spezzamento $D \otimes_K L = \mathcal{M}_n(L)$ (con $n = \operatorname{ind}_K D$) che ha un azione naturale su $L^{\oplus n}$, in particolare è anche un D-modulo e vale la seguente relazione tra le dimensioni.

$$n \dim_K L = \dim_K L^{\oplus n} = \dim_K D \dim_D L^{\oplus n} = n^2 \dim_D L^{\oplus n}$$

Da cui si ottiene che $\operatorname{ind}_K D = n \mid \dim_K L$. □

Teorema 4.24. *Sia D un'algebra di divisione (con $n = \operatorname{ind}_K D$) e L un sottocampo massimale allora $\dim_K L = n$ e L è un campo di spezzamento.*

Dimostrazione. Definiamo $A = D \otimes_K L$; si tratta di una L-algebra semplice centrale per il teorema 4.12. Il corpo D è un A-modulo sinistro semplice con l'azione indotta da quella di $D \otimes_K D^{opp} \supset A$ (cioè $(d \otimes l)x = dxl$), ci chiediamo quali sono gli endomorfismi A lineari di D. Sicuramente formano un corpo contenente L e sono contenuti in D perché:

$$L \subseteq \operatorname{End}_A^{opp} D \subseteq \operatorname{End}_D^{opp} D = D$$

Inoltre se esistesse $x \in D \setminus L$ si avrebbe che x commuta con gli elementi di L quindi $L(x)$ sarebbe un sottocampo di D ma ciò è assurdo per massimalità di L. Abbiamo ottenuto che $L = \operatorname{End}_A^{opp} D$ e utiliziamo il teorema di struttura (3.36) per ottenere che $D \otimes_K L = A = \operatorname{End}_L(D)$ quindi L è campo di spezzamento. Ora ragionando sulle dimensioni si ottiene che

$$\dim_K D = \dim_L(D \otimes_K L) = \dim_L(\operatorname{End}_L D) = (\dim_L D)^2$$

Da cui $\dim_L D = \operatorname{ind}_K D = n$ e moltiplicando per $\dim_K L$ si ottiene che $n \dim_K L = \dim_K L \dim_L D = \dim_K D = n^2$ da cui la prima parte della tesi. □

Teorema 4.25 (di Skolem-Noether)**.** *Sia A un'algebra semplice centrale e B una sotto-algebra semplice. Dato $f : B \longrightarrow A$ un omomorfismo di algebre allora esiste a invertibile tale che $f(x) = axa^{-1}$ per ogni $x \in B$.*

Dimostrazione. Sia $R = B \otimes A^{opp}$ è una K-algebra semplice per il teorema 4.12, A è un R modulo dato dalla moltiplicazione $(b \otimes a)x = bxa$ e A' un altro R modulo dato dall'azione di R su A definita da $(b \otimes a)x = f(b)xa$. Notiamo che A e A' sono due moduli su R con la stessa dimensione su K quindi isomorfi ($A \simeq V^{\oplus r} \simeq A'$). Esiste un isomorfismo $\varphi : A \longrightarrow A'$ di R moduli, l'omomorfismo è R-lineare quindi vale $\varphi(bxa) = f(b)\varphi(x)a$. Imponendo $b = 1$ si ottiene che $\varphi \in \operatorname{End}_A(A) \simeq A$, esiste $u \in A^*$ tale che $\varphi(x) = ux$ per ogni elemento x in A. In particolare imponendo $x = 1$ e $a = 1$ si ottiene che $ub = \varphi(b) = f(b)\varphi(1) = f(b)u$ e poichè u è invertibile otteniamo $f(b) = ubu^{-1}$ per ogni elemento b in B. □

Definizione 4.26. Dato un anello R e un sottoinsieme S definiamo il centralizzatore di S in R è $C_R(S) = \{x \in R \mid xs - sx = 0 \quad \forall\, s \in S\}$

E' un fatto noto che il centralizzatore sia sempre un sottoanello contenente il centro.

Proposizione 4.27. *Date due K-algebre A e B e due sottospazzi vettoriali A' e B' vale che*

$$C_{A\otimes_K B}(A' \otimes_K B') = C_A(A') \otimes_K C_B(B')$$

dove con $A' \otimes_K B'$ si intende l'insieme $\{\sum_i a_i \otimes b_i \mid a_i \in A' \quad b_i \in B'\}$.

Dimostrazione. Dimostriamo la doppia inclusione. La prima inclusione $\supseteq$ è una facile verifica sui generatori di $C_A(A') \otimes_K C_B(B')$ che denoteremo $a \otimes b$

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

L'altra inclusione si dimostra prendendo $x \in C_{A\otimes B}(A' \otimes_K B')$ e scrivendolo come $x = \sum_{i\leq n} a_i \otimes b_i$ con gli a_i linearmente indipendenti su K. Per ogni $b' \in B'$ vale

$$0 = (1 \otimes b')x - x(1 \otimes b') = \sum_{i\leq n} a_i \otimes (b'b_i - b_ib')$$

che implica per indipendenza lineare degli a_i che $b'b_i - b_ib' = 0$ quindi ogni $b_i \in C_B(B')$ cioè $C_{A\otimes_K B}(A' \otimes B') \subseteq A \otimes C_B(B')$ e per simmetria di A e B si ottiene che

$$C_{A\otimes_K B}(A' \otimes_K B') \subseteq A \otimes_K C_B(B') \cap C_A(A') \otimes_K B = C_A(A') \otimes_K C_B(B')$$

□

Lemma 4.28. *Data una K-algebra A e siano A_r e A_l i sottoanelli di $\mathrm{End}_K A$ degli elementi del tipo $R_a(x) = xa$ con $a \in A$ e $L_a(x) = ax$ (moltiplicazione a destra e a sinistra) vale che $C_{\mathrm{End}\,A}(A_r) = A_l$ e $C_{\mathrm{End}\,A}(A_l) = A_r$.*

Dimostrazione. Ovviamente $L_aR_b = R_bL_a$ quindi $A_l \subseteq C(A_r)$. Viceversa se $f \in C(A_r)$ allora $f(xa) = f(x)a$ per ogni a e x, in particolare per $x = 1$ si ha che $f(a) = f(1)a$ quindi $f = R_{f(1)} \in A_l$ □

Teorema 4.29 (del centralizzatore)**.** *Sia A un'algebra semplice centrale e B una sottoalgebra semplice allora $C_A(C_A(B)) = B$ e $C_A(B)$ è semplice.*

Dimostrazione. Dimostriamo prima il teorema nel caso particolare in cui $A = \mathrm{End}_K(B)$ allora per il lemma 4.28 $C_A(B) \simeq C_A(B_l) = B_r \simeq B^{opp}$ e quindi $C_A(B)$ è semplice perché lo è B. Inoltre $C_A(C_A(B)) = C_A(B_r) = B_l$. Per il caso generale prendiamo l'algebra semplice centrale $A \otimes_K \mathrm{End}_K(B)$,

ci sono due modi di immergere B in $A \otimes_K \mathrm{End}_K(B)$ il primo indotto da $B \subset A$ e il secondo da $B_l \subset \mathrm{End}_K B$ poichè le immagini sono isomorfe allora per il teorema di Skolem-Noether sono coniugate. Per questo sono coniugati anche i loro centralizzatori $C_{A\otimes \mathrm{End}(B)}(1 \otimes B)$ e $C_{A\otimes \mathrm{End}(B)}(B \otimes 1)$. Inoltre per il lemma 4.28 vale che $C_{A\otimes \mathrm{End}(B)}(B \otimes 1) \simeq C_A(B) \otimes_K \mathrm{End}_K B$ e che $C_{A\otimes \mathrm{End}(B)}(1\otimes B) \simeq A\otimes_K C_{\mathrm{End}\, B}(B)$ quest'ultima è un algebra semplice perché $C_{\mathrm{End}\, B}(B)$ è semplice per quanto dimostrato nella prima parte. Abbiamo quindi dimostrato che $C_A(B) \otimes_K \mathrm{End}_K B$ è semplice e quindi lo è $C_A(B)$. Manca ora da dimostrare che $C_A(C_A(B)) = B$, vale che

$$C_{A\otimes \mathrm{End}(B)}(C_{A\otimes \mathrm{End}(B)}(B \otimes 1)) \simeq C_A(C_A(B)) \otimes_K C_{\mathrm{End}\, B}(\mathrm{End}_K B) \simeq \\ \simeq C_A(C_A(B)) \otimes_K K$$

$$C_{A\otimes \mathrm{End}(B)}(C_{A\otimes \mathrm{End}(B)}(1 \otimes B)) \simeq C_A(A) \otimes_K C_{\mathrm{End}\, B}(C_{\mathrm{End}\, B}(B)) \simeq \\ \simeq K \otimes_K B$$

Dove abbiamo usato il caso particolare già dimostrato e il fatto che A è centrale su K. I due membri di sinistra sono isomorfi perché sono i centralizzatori di due sottoalgebre coniugate e quindi si ottiene l'isomorfismo. E' ovvio che $B \subseteq C_A(C_A(B))$ e per dimensione su K si ottiene l'uguaglianza. □

Nella dimostrazione abbiamo detto che $C_A(B) \otimes_K \mathrm{End}_K B \simeq A \otimes_K B^{opp}$ quindi guardando le dimensioni si ottiene che

$$\dim_K C_A(B) \cdot \dim_K B = \dim_K A \tag{4.1}$$

Corollario 4.30. *Data un algebra di divisione D il campo L è massimale se e solo se $C_D(L) = L$.*

Dimostrazione. Se L è massimale ed esiste $x \in C_D(L)$ allora $L(x)$ è un campo contenente L quindi coincide con L cioè $L = C_D(L)$. Viceversa supponendo $C_D(L) = L$, se un campo F contiene L allora $F \subseteq C_D(L) = L$ da cui $F = L$ e L è massimale (per fare questa freccia non abbiamo usato che D sia di divisione). □

Mettendo assieme l'osservazione e l'equazione 4.1 si ottiene che per un campo massimale L vale $\dim_K L = \mathrm{ind}_K D$, cosa che sapevamo già per il teorema 4.24 ma dimostrata in modo diverso.

Teorema 4.31. *Sia D una K-algebra di divisione diversa da K allora esiste $x \in D \setminus K$ separabile su K.*

Dimostrazione. La caratteristica di K è ($p = Char K$) positiva altrimenti il risultato è banale. Supponiamo per assurdo che ogni elemento $x \in D$ è puramente inseparabile su K allora esiste un intero tale che $x^{p^{n(x)}} \in K$ ($n(x)$

è il minimo intero che soddisfa la condizione). In particolare esiste x tale che $n(x)$ sia positivo (perché $D \neq K$), chiamiamo $a = x^{p^{n(x)-1}}$ e abbiamo che $a^p \in K$. Sia $\delta : D \longrightarrow D$ definita da

$$\delta(t) = ta - at$$

una funzione non nulla perchè $a \notin K = Z(D)$. Per induzione si dimostra che $\delta^{(n)}(t) = \sum_{i=0}^{n}(-1)^i \binom{n}{i} a^i t a^{n-i}$ e in particolare per $n = p$ si ha che $\delta^{(p)}(t) = ta^p - a^p t = 0$ perché $a^p \in K = Z(D)$. Quindi esiste $y \in D$ e $k \geq 2$ tale che $x := \delta^{(k-1)}(y) \neq 0$ e che $\delta^{(k)}(y) = 0$. Sia $w = \delta^{(k-2)}(y)$ e $c = wx^{-1}a$ cerchiamo una relazione tra a e c, vale che $a = 1 \cdot a = (wa - aw)x^{-1}a = wax^{-1}a - ac = ca - ac$ dove nella seconda uguaglianza abbiamo usato che $x = wa - aw$ e nella terza che a e x commutano. Otteniamo quindi l'uguaglianza $c = 1 + aca^{-1}$ e applicando $n(c)$ volte l'omomorfismo di Frobenius otteniamo che $c^{p^{n(c)}} = 1 + (aca^{-1})^{p^{n(c)}} = 1 + ac^{p^{n(c)}}a^{-1} = 1 + c^{p^{n(c)}}$ da cui l'assurdo che $1 = 0$. □

Corollario 4.32. *Ogni corpo D ha un sottocampo massimale che è separabile.*

Dimostrazione. Sia L il sottocampo massimale tra quelli separabili. Sappiamo che $L = C_D(L)$ se e solo se è massimale per il corollario 4.30, quindi supponiamo per assurdo che $L \subsetneq C_D(L)$ e abbiamo che $C_D(L)$ è un corpo centrale su L (perchè $L = C_D(C_D(L))$ per il teorema 4.29). Ma per il teorema appena dimostrato esiste $x \in C_D(L) \setminus L$ separabile e in particolare $L(x)$ è un sottocampo separabile contenente L ma ciò è assurdo per la massimalità di L tra i sottocampi separabili. □

Nella dimostrazione sono stati dati per noti alcuni teoremi della teoria dei campi (moltiplicatività del grado, automorfismo di Frobenius ed esistenza di un sottocampo massimale separabile). Gli enunciati precisi e le dimostrazioni si trovano nel libro di Lang [4, pp 223-247].

Teorema 4.33. *Per ogni elemento di* $\mathrm{Br}(K)$ *esiste una algebra semplice centrale A con sottocampo massimale L di Galois con $[A : K] = [L : K]^2$.*

Dimostrazione. Dato il rappresentante della classe di equivalenza che è un corpo D per il corollario 4.32 ha un sottocampo massimale separabile L ($n = [L : K]$), chiamiamo E la chiusura di Galois di L ($m = [E : L]$). L'algebra $A = D \otimes_K \mathcal{M}_m(K)$ è semplice centrale e $[A] = [D]$, inoltre $E \subseteq A$ perché $A \supseteq L \otimes_K \mathcal{M}_m(K) \simeq \mathcal{M}_m(L) \supseteq E$ dove l'ultima inclusione è data dalla rappresentazione regolare di E su L. Inoltre guardando le dimensioni su K si ottiene $[A : K] = [L : K]^2$. □

Corollario 4.34. *Ogni algebra ha un campo di spezzamento di Galois.*

Dimostrazione. La definizione di campo di spezzamento (4.18) non dipende dall'algebra ma solo dalla sua calsse. Perciò scegliamo D algebra di divisione equivalente e per il teorema 4.31 esiste sottocampo massimale separabile. Esso è anche di spezzamento per il teorema 4.24, infine prendendone la chiusura di Galois rimane ancora campo di spezzamento e per di più è di Galois. □

4.4 Polinomio caratteristico

In questa sezione analizziamo il polinomio caratteristico, norma e traccia di un elemento di una C.S.A. ed enunceremo proprietà utili. In seguito definiamo il polinomio caratteristico ridotto e conseguentemente la norma ridotta e la traccia ridotta e vediamo la relazione tra polinomio caratteristico e polinomio caratteristico ridotto.

Definizione 4.35 (polinomio caratteristico)**.** Dato $a \in A$ algebra, ricordando l'immersione di $A_l \subset \mathrm{End}_K A$ possiamo definire il polinomio caratteristico di a (pc_a) come il polinomio caratteristico dell'applicazione K-lineare $x \mapsto ax$.

Definizione 4.36 (Norma e traccia)**.** Sia $\mathrm{pc}_a(x) = \sum_{i \leq n} c_i x^i$ si definisce

- Norma di a $\mathrm{N}(a) = (-1)^n c_0$
- Traccia di a $\mathrm{tr}(a) = -c_{n-1}$

Valgono banalmente tutte le proprietà della norma e della traccia note per le matrici. Altre proprietà interessanti sono le seguenti.

Osservazione 4.37.

1. *Il polinomio caratteristico è invariante per estensione di scalari.*
$$\mathrm{pc}_{A/K}(a) \otimes 1 = \mathrm{pc}_{A \otimes L/L}(a \otimes 1)$$
2. *Se L estensione di Galois di K (con gruppo G) possiamo caratterizzare norma e traccia con:*
$$\mathrm{N}_{L/K}(a) = \prod_{\sigma \in G} \sigma(a) \qquad e \qquad \mathrm{tr}_{L/K}(a) = \sum_{\sigma \in G} \sigma(a)$$
3. *Siano $r = [L : K]_s$ e $q = [L : K]_i$ rispettivamente il grado di separabilità e inseparabilità, vale:*
$$\mathrm{N}_{L/K}(a) = \left(\prod_{\sigma} \sigma(a) \right)^q \qquad e \qquad \mathrm{tr}_{L/K}(a) = q \sum_{\sigma} \sigma(a)$$
con σ che varia tra tutte le immersioni di L nella chiusura algebrica di K.

4. Vale la proprietà transitiva di traccia e norma con le torri di estensioni:

$$\mathrm{N}_{F/K}(a) = \mathrm{N}_{L/K}\left(\mathrm{N}_{F/L}(a)\right) \qquad e \qquad \mathrm{tr}_{F/K}(a) = \mathrm{tr}_{L/K}\left(\mathrm{tr}_{F/L}(a)\right)$$

Dimostrazione.

1. $\mathrm{pc}_{A/K}(a) \otimes 1 = \det_{A/K}(x\,\mathrm{Id}_A - L_a) \otimes 1 = \det_{A/K}(x\,\mathrm{Id}_{A\otimes L} - L_a \otimes 1) = \mathrm{pc}_{A\otimes L/L}(a \otimes 1)$

2. Prendiamo in considerazione l'omomorfismo di K-algebre $L \otimes_K L \simeq L^n$ con la mappa che manda $x \otimes 1 \mapsto (\sigma(x))_{\sigma\in G}$ ed estesa a tutta l'algebra per L-linearità. In questa base l'omomorfismo $L_a \otimes 1$ è la matrice diagonale con entrate $\sigma(a)$ quindi il polinomio caratteristico è $\mathrm{pc}_a(x) = \prod_{\sigma\in G}(x - \sigma(a))$ da cui la tesi.

3,4. Dimostriamo contemporaneamente l'affermazione (3) e (4). Dimostriamo prima il teorema nei seguenti due casi particolari e poi useremo i risultati ottenuti per dimostrare il caso generale.

Se $a \in K$, essendo il polinomio caratteristico $(x-a)^{rq}$, vale la proprietà (3). Se L è estensione semplice di K cioè $L = K[a]$ vale che il polinomio caratteristico è $\prod_{i\le r}(x - \sigma_i(a))^q$ e quindi anche in questo caso vale la formula (3).

Prendiamo ora in considerazione la seguente torre di estensioni $K \subset K[a] \subset L$ e tentiamo di dimostrare la transitività della norma e della traccia. Per comodità sia $n = \big[L : K[a]\big]$, $q = \big[K[a] : K\big]_i$ e $r = \big[K[a] : K\big]_s$:

$$\begin{aligned}\mathrm{tr}_{L/K}(a) &= n\,\mathrm{tr}_{K[a]/K}(a) = \mathrm{tr}_{K[a]/K}(na) = \\ &= \mathrm{tr}_{K[a]/K}\left(\mathrm{tr}_{L/K[a]}(a)\right) = q\sum_{i=1}^{r}\sigma_i(na)\end{aligned}$$

$$\begin{aligned}\mathrm{N}_{L/K}(a) &= \mathrm{N}_{K[a]/K}(a)^n = \mathrm{N}_{K[a]/K}(a^n) = \\ &= \mathrm{N}_{K[a]/K}\left(\mathrm{N}_{L/K[a]}(a)\right) = \left(\prod_{i=1}^{r}\sigma_i(a^n)\right)^q\end{aligned}$$

Vogliamo ora dimostrare la transitività della formula della traccia e della norma che sappiamo coincidere con la traccia e la norma solo in casi particolari. Data la torre di estensioni $K \subset L \subset F$ con grado $r_1 = [L : K]_s$, $r_2 = [F : L]_s$, $q_1 = [L : K]_i$ e $q_2 = [F : L]$ con σ_i immersioni di L in $\bar{K}$ su K e τ_j immersioni di F in $\bar{K}$ su L. Ricordando le proprietà basilari dei campi otteniamo che $r_1 r_2 = [F : K]_s$, $q_1 q_2 = [F : K]_i$ e

che le immersioni di F in $\overline{K}$ su K sono tutte e sole quelle della forma $\sigma'_i \circ \tau_j$ dove σ'_i è un estensione di σ_i.

$$q_1 q_2 \sum_{i,j} \sigma'_i(\tau_j(a)) = q_1 \sum_i \sigma_i\Big(q_2 \sum_j \tau_j(a)\Big)$$

$$\Big(\prod_{i,j} \sigma'_i(\tau_j(a))\Big)^{q_1 q_2} = \Big(\prod_i \sigma_i\Big(\prod_j \tau_j(a)\Big)^{q_1}\Big)^{q_2}$$

Abbiamo dimostrato la proposizione (3) nel caso generale. Inoltre vale anche la proposizione (4) perché abbiamo dimostrato che vale per la formula della proposizione (3).

□

Definizione 4.38. La forma traccia di L su K è la forma K-bilineare simmetrica data da

$$\langle a, b\rangle = \mathrm{tr}_{L/K}(ab)$$

Dimostrazione. La bilinearità è ovvia dalla bilinearità del prodotto e dalla linearità della traccia. La forma è simmetrica perché $\mathrm{tr}(a_l b_l) = \mathrm{tr}(b_l a_l)$. □

Definizione 4.39 (polinomio caratteristico ridotto)**.** Per definire il polinomio caratteristico ridotto (pcr) di $a \in A$ (algebra semplice centrale su K) fissiamo un campo L di spezzamento di A e consideriamo l'isomorfismo $\varphi : A \otimes_K L \longrightarrow \mathcal{M}_n(L)$ (con $n^2 = [A : K]$).

Definiamo $\mathrm{pcr} : A \longrightarrow K[x]$ la funzione definita da $\mathrm{pcr}(a) = \mathrm{pc}(\varphi(a \otimes 1))$ dove pc è il consueto polinomio caratteristico sulle matrici a coefficienti in L.

Proposizione 4.40. *La definizione di polinomio caratteristico ridotto è ben posta.*

Dimostrazione.

- dimostriamo che pcr non dipende dalla funzione φ scelta. Per far ciò prendiamo un altro isomorfismo ψ e verifichiamo che il risultato è lo stesso. $\varphi \circ \psi^{-1}$ è un automorfismo di $\mathcal{M}_n(L)$ e per il teorema di Skolem-Noether (4.25), ricordando che $\mathcal{M}_n(L)$ è algebra semplice centrale, l'automorfismo è indotto dal coniugio per un elemento invertibile x. E' noto che il polinomio caratteristico è invariante per coniugio ($\mathrm{pc}(a) = \mathrm{pc}(xax^{-1})$) e ciò dimostra che pcr non dipende da φ.

- pcr non dipende dalla scelta del campo di spezzamento L. Basta dimostrare che se $F \supset L$ induce lo stesso polinomio caratteristico ridotto, perché per dimostrare il caso generale in cui si ha un altro

campo di spezzamento E, basta scegliere $F = LE$ [1] e applicare due volte la dimostrazione su $F \supset L$ e $F \supset E$. Sappiamo che il polinomio caratteristico di una matrice $n \times n$ a coefficienti in L non dipende se immersa in $\mathcal{M}_n(L)$ o in $\mathcal{M}_n(F) = \mathcal{M}_n(L) \otimes_L F$. Ricordiamo che $A \otimes_K F = (A \otimes_K L) \otimes_L F = \mathcal{M}_n(L) \otimes_L F$ perché L è di spezzamento per A. Mettendo assieme le due affermazioni precedenti e il fatto che il polinomio non dipende dal'isomorfismo si ottiene che $\mathrm{pc}(\varphi(a \otimes 1_L)) = \mathrm{pc}(\psi(a \otimes 1_F))$.

- Vogliamo ora dimostrare che pcr è ben definito in quanto l'immagine è in $K[x]$ e non in $L[x]$. Per prima cosa scegliamo L campo di spezzamento di Galois (possiamo farlo per il corollario 4.34). Per ogni $\sigma \in \mathrm{Gal}_K(L)$ abbiamo l'estensione $\sigma^* : \mathcal{M}_n(L) \longrightarrow \mathcal{M}_n(L)$ che agisce sui coefficienti della matrice. Sia $\psi = \sigma^* \circ \varphi \circ (\mathrm{Id} \otimes \sigma^{-1})$ un L-isomorfismo, poiché il polinomio caratteristico ridotto non dipende dalla scelta dell'isomorfismo vale che:

$$\begin{aligned}\mathrm{pcr}(a) = \mathrm{pc}(\psi(a \otimes 1)) = \mathrm{pc}(\sigma^*(\varphi(\mathrm{Id}\, a \otimes \sigma^{-1}1)))) = \\ = \sigma\, \mathrm{pc}(\varphi(a \otimes 1)) = \sigma\, \mathrm{pcr}(a)\end{aligned}$$

  ciò dimostra che $\mathrm{pcr}(a) \in L^G[x] = K[x]$.

□

Enunciamo qualche proprietà interessante del polinomio caratteristico ridotto.

Osservazione 4.41. *Valgono le seguenti proprietà:*

1. *(Hamilton-Caley)* $\mathrm{pcr}_a(a) = 0$ *per ogni* $a \in A$.
2. pcr *è invariante per isomorfismo di algebre.*
3. pcr *è invariante per estensioni di scalari.*

Dimostrazione.

1. Sia $\mathrm{pcr}_a = \sum_{i \leq n} c_i x^i$ per il teorema di Hamilton-Caley sulle matrici vale che

   $$0 = \mathrm{pc}_{\varphi(a \otimes 1)}(\varphi(a \otimes 1)) = \sum\nolimits_{i \leq n} c_i (\varphi(a \otimes 1))^i = \varphi\left(\left(\sum\nolimits_{i \leq n} c_i a^i\right) \otimes 1\right)$$

   Quindi per l'iniettività di φ si ottiene che $\mathrm{pcr}_a(a) = 0$.

2. la dimostrazione è la stessa della prima parte della buona definizione del polinomio caratteristico ridotto.

[1] Il composto di due campi esiste per il teroema 4.19

3. la dimostrazione è analoga a quella dell'estensione del campo di spezzamento della buona definizione di pcr.

□

Definiamo ora norma e traccia ridotte ed elenchiamo loro proprietà.

Definizione 4.42 (Norma e traccia ridotte)**.** Sia $\mathrm{pcr}_a = \sum_{i\leq n} c_i x^i$ chiamiamo norma ridotta $\mathrm{Nrd}(a) = (-1)^n c_0$ e traccia ridotta $\mathrm{trd}(a) = -c_{n-1}$.

Osservazione 4.43. *Valgono le seguenti proprietà note della traccia e della norma:*

1. $\mathrm{trd}(ab) = \mathrm{trd}(ba)$
2. $\mathrm{trd}(a+b) = \mathrm{trd}(a) + \mathrm{trd}(b)$
3. $\mathrm{trd}(ka) = k\,\mathrm{trd}(a)$ *con* $k \in K$
4. $\mathrm{Nrd}(ab) = \mathrm{Nrd}(a)\,\mathrm{Nrd}(b)$
5. $\mathrm{Nrd}(ka) = k^n\,\mathrm{Nrd}(a)$ *con* $k \in K$
6. $\mathrm{Nrd}(a) \neq 0 \iff a \in A^*$
7. *La norma e la traccia ridotte sono invarianti per isomorfismo di algebre ed estensione di scalari.*

Dimostrazione. Le dimostrazioni dei fatti precedenti consistono nell'applicare le definizioni e le proprietà relative su traccia e norma matriciali.

1. $\mathrm{trd}(ab) = \mathrm{tr}(\varphi(ab\otimes 1)) = \mathrm{tr}(\varphi(a\otimes 1)\varphi(b\otimes 1)) = \mathrm{tr}(\varphi(b\otimes 1)\varphi(a\otimes 1)) = \mathrm{tr}(\varphi(ba\otimes 1)) = \mathrm{trd}(ba)$
2. $\mathrm{trd}(a+b) = \mathrm{tr}(\varphi((a+b)\otimes 1)) = \mathrm{tr}(\varphi(a\otimes 1)) + \mathrm{tr}(\varphi(b\otimes 1)) = \mathrm{trd}(a) + \mathrm{trd}(b)$
3. $\mathrm{trd}(ka) = \mathrm{tr}(\varphi(ka\otimes 1)) = k\,\mathrm{tr}(\varphi(a\otimes 1)) = k\,\mathrm{trd}(a)$
4. $\mathrm{Nrd}(ab) = \det(\varphi(ab\otimes 1)) = \det(\varphi(a\otimes 1))\det(\varphi(b\otimes 1)) = \mathrm{Nrd}(a)\,\mathrm{Nrd}(b)$
5. $\mathrm{Nrd}(ka) = \det(\varphi(ka\otimes 1)) = k^n \det(\varphi(a\otimes 1)) = k^n\,\mathrm{Nrd}(a)$
6. Se $a \in A^*$ esiste b tale che $ab = 1$ quindi $\mathrm{Nrd}(a)\,\mathrm{Nrd}(b) = 1$ da cui $\mathrm{Nrd}(a) \neq 0$. Viceversa $0 \neq \mathrm{Nrd}(a) = \det(\varphi(a\otimes 1))$ cioè $\varphi(a\otimes 1)$ è invertibile in $\mathcal{M}_n(L)$ quindi esiste $u \in A\otimes_K L$ tale che $\varphi(a\otimes 1)\varphi(u) = \mathrm{Id}$ cioè $(a\otimes 1)u = 1$. Sapendo che in A tutti gli elementi sono invertibili o divisori di zero otteniamo che $a \in A^*$ perchè non può essere divisore di zero.

7. E' immediata conseguenza del fatto che pcr è invariante per isomorfismo ed estensioni di scalari.

□

Enunciamo ora le proprietà che legano il polinomio caratteristico col polinomio caratteristico ridotto e di conseguenze proprietà di norma e traccia.

Teorema 4.44. *Data una K-algebra semplice centrale A e un suo elemento a, vale che* $\mathrm{pc}_a(x) = \mathrm{pcr}_a^n(x)$ *dove* $n = \dim_K A$.

Dimostrazione. Sia L campo di spezzamento di A, per definizione di campo di spezzamento si ha che $A \otimes_K L \simeq \mathcal{M}_n(L)$ dove $n = \dim_K(A)$. Inoltre sia $I = L^n$ un ideale sinistro minimale di $A \otimes_K L$ cioè unico modulo semplice su A allora $A \otimes_K L \simeq I^n$ come modulo su A. Dunque

$$\mathrm{pcr}(a) = \mathrm{pc}_{A \otimes L \diagup L}(a_l \otimes \mathrm{Id}) = \mathrm{pc}(a_l)^n$$

dove si è scelto un particolare omomorfismo φ. Abbiamo dunque dimostrato che $\mathrm{pc}_a(x) = (\mathrm{pcr}_a(x))^n$. □

Corollario 4.45. *Facile conseguenza è che*

$$\mathrm{N}(a) = \mathrm{Nrd}(a)^n \qquad e \qquad \mathrm{tr}(a) = n\,\mathrm{trd}(a)$$

Capitolo 5

Factor set

5.1 definizioni

Definiamo in generale i factor set e poi useremo solo un caso particolare sulle algebre.

Data una successione esatta di gruppi con A sottogruppo normale di G ($A \triangleleft G$)

$$e \longrightarrow A \longrightarrow G \longrightarrow B \longrightarrow e$$

Si può segliere per ogni $b \in B$ un rappresentante in G che chiameremo $u(g)$, inoltre G agisce su A in modo canonico tramite coniugio, quindi si può definire l'azione β di B su A definita da $\beta_b(a) = u(b)au(b)^{-1}$. Si può vedere che $\beta : B \longrightarrow {}^{Aut\ A}\!/_{Inn\ A}$ poichè $\beta(B) \cap Inn\ A = \mathrm{Id}$.

Usando la relazione $u(b_1)u(b_2) = a_{1,2}u(b_1b_2)$ con $a_{1,2} \in A$ e (con un piccolo abuso di notazione) chiamare il coniugio per elementi di A ancora β_a, si ottiene che

$$\beta_{b_1}\beta_{b_2} = \beta_{a_{1,2}}\beta_{b_1b_2} \tag{5.1}$$

Inoltre devono valere le seguenti relazioni

$$u(b_1)u(b_2)u(b_3) = u(b_1)a_{b_2,b_3}u(b_2b_3) = \beta_{b_1}(a_{b_2,b_3})\, a_{b_1,b_2b_3}\, u(b_1b_2b_3)$$

$$u(b_1)u(b_2)u(b_3) = a_{b_1,b_2}u(b_1b_2)u(b_3) = a_{b_1,b_2}\, a_{b_1b_2,b_3}\, u(b_1b_2b_3)$$

che assieme forniscono la seguente relazione:

$$\beta_{b_1}(a_{b_2,b_3})\, a_{b_1,b_2b_3} = a_{b_1,b_2}\, a_{b_1b_2,b_3} \tag{5.2}$$

Inoltre vogliamo definire un prodotto su $A \times B$ che sia quello di G per questo la mappa che manda $A \times B \longrightarrow G$ data da $(a, b) \mapsto au(b)$ allora è naturale definire il prodotto tra le coppie nel seguente modo $(a, b)\cdot(a_1, b_1) = au(b)a_1u(b_1) = a\,\beta_b(a_1)a_{b,b_1}u(bb_1) = (a\,\beta_b(a_1)a_{b,b_1}, bb_1)$.

Per fare ciò diamo la definizione di factor set che generalizza quella del prodotto semidiretto tra gruppi.

Definizione 5.1. Dati due gruppi A e B e due funzioni $f : B \times B \longrightarrow A$ e $\varphi : B \longrightarrow Aut\ A$ tali che soddisfano le proprietà 5.1 e 5.2 cioè:

$$\varphi_{b_1}\varphi_{b_2}(a) = f(b_1, b_2)\varphi_{b_1 b_2}(a)f(b_1, b_2)^{-1} \tag{5.3}$$

$$\varphi_{b_1}(f(b_2, b_3))f(b_1, b_2 b_3) = f(b_1, b_2)f(b_1 b_2, b_3) \tag{5.4}$$

Esiste il gruppo $A \times B$ dato dall'operazione

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1\varphi_{b_1}(a_2)f(b_1, b_2), b_1 b_2)$$

e chiamiamo f il factor set su B di A.

Notiamo che esiste l'immersione di A in $A \times B$, l'immagine è normale ed esiste la proiezione su B che sono omomorfismi di gruppi.

Nel caso che tratteremo prendiamo L/K un estensione di Galois e come A prendiamo L^*, come B il suo gruppo di Galois ($G = Gal_K(L)$) e come φ l'immersione naturale di $\mathrm{Gal}_K(L^*) \hookrightarrow Aut(L^*)$. Poiché L^* è un gruppo abeliano e φ un omomorfismo la condizione 5.1 è sempre soddisfatta, quindi d'ora in poi un factor set f sarà una funzione da $G \times G$ in L^* che soddisfa la condizione 5.2:

$$\sigma(f(\tau, \nu))f(\sigma, \tau\nu) = f(\sigma, \tau)f(\sigma\tau, \nu) \tag{5.5}$$

Poichè d'ora in poi prendiamo in considerazione le applicazioni sulle algebre semplici centrali supponiamo che l'estensione L/K finita di dimensione $n = \dim_K L$.

Definizione 5.2. Sia L/K un estensione di Galois e f un factor set allora $A = (L, K, f)$ è una K-algebra definita da $A = \{\sum_{\sigma \in G} l_\sigma x_\sigma \mid l_\sigma \in L\}$ come K-spazio vettoriale e il prodotto definito da :

1. $x_\sigma l = \sigma(l)x_\sigma$
2. $x_\sigma x_\tau = f(\sigma, \tau)x_{\sigma\tau}$

Inoltre A è semplice centrale su K con sottocampo massimale L.

Dimostrazione. La moltiplicazione è definita su x_σ ed estesa a tutta l'algebra, per questo basta verificare l'associatività solo sui generatori x_σ. Come gruppi moltiplicativi i monomi in A e $L^* \times G$ sono isomorfi, quindi l'associatività del prodotto discende direttamente dall'associatività del prodotto in $L^* \times G$. L'elemento neutro è $f(e, e)^{-1}x_e$ per provarlo dobbiamo prima dimostrare che se f è un factor set allora

$$f(e, \sigma) = f(e, e) \qquad e \qquad f(\sigma, e) = \sigma f(e, e)$$

che discendono dalla proprietà 2 della definizione ponendo nel primo caso $\sigma = \tau = e$ e nel secondo $\tau = \nu = e$. Verifichiamo che $f(e,e)^{-1}x_e$ sia l'elemento neutro sia a destra che a sinistra solo sui generatori:

$$f(e,e)^{-1}x_e k x_\sigma = f(e,e)^{-1}k x_e x_\sigma = k f(e,e)^{-1} f(e,\sigma)x_\sigma = k x_\sigma$$

$$k x_\sigma f(e,e)^{-1}x_e = k\sigma(f(e,e)^{-1})x_\sigma x_e = k\sigma(f(e,e))^{-1} f(\sigma,e)x_\sigma = k x_\sigma$$

.

Identifichiamo L con Lx_e e dimostriamo che è sottocampo massimale. Per dimostrarlo vediamo che $C_A(L) = L$ e poi applichiamo il corollario 4.30. Se $a = \sum_{\sigma\in G} k_\sigma x_\sigma \in C_A(L)$ allora $ak - ka = 0\ \forall\, k \in L$ cioè $\sum_{\sigma\in G}(\sigma(k) - k)k_\sigma x_\sigma = 0$ da cui per lineare indipendenza degli x_σ $(\sigma(k) - k)k_\sigma = 0$ cioè $k_\sigma = 0$ per ogni $\sigma \neq \mathrm{Id}$ e $a \in L$. Il centro di A è contenuto in L e fissato da ogni σ (commuta con x_σ) quindi $Z(A) = L^G = K$.

Per dimostrare che A è semplice verifichiamo che non ha ideali bilateri non banali. Per assurdo esiste I ideale bilatero non banale e sia $u \neq 0$ uno degli elementi dell'ideale che hanno scrittura di lunghezza minima in termini dei generatori x_σ. L'elemento u si può scrivere come $u = \sum_{\sigma\in G} k_\sigma x_\sigma$, sia τ tale che $k_\tau \neq 0$ possiamo moltiplicare a destra per $x_{\tau^{-1}}$ e ottenere un nuovo elemento u con la stessa lunghezza e $k_e \neq 0$. Per ogni $k \in L$ vale che $uk - ku \in I$ e la lunghezza della scrittura è strettamente minore di quella di u quindi $uk - ku = 0$ da cui $u \in C_A(L) = L$ cioè u è invertibile e $I = A$. □

Inoltre vale che $\dim_K A = \dim_L A \dim_K L = |G|^2 = n^2$

5.2 Equivalenza

Definiamo una relazione di equivalenza sui factor set in modo tale che due factor set siano equivalenti se e solo se generano algebre isomorfe.

Definizione 5.3 (equivalenza di factor set)**.** Due factor set f, g sono equivalenti ($\sim$) se esiste $\lambda : G \longrightarrow L^*$ tale che per ogni coppia di elementi in G vale:

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

Dimostrazione. $\sim$ è una relazione di equivalenza perché è riflessiva ($\lambda = 1$), simmetrica e transitiva. Ponendo $\mu = \frac{1}{\lambda}$ si ha che

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

e dati f, g, h factor set e λ, μ le funzioni relative a $f \sim g$ e $g \sim h$ allora $\rho = \lambda\mu$ induce l'equivalenza tra f e h. □

Chiamiamo un factor set normalizzato se $\forall \sigma \in G \ f(\sigma, e) = f(e, \sigma) = 1 \in L$ inoltre ogni factor set è equivalente a uno normalizzato. Scegliendo $\lambda_\sigma = \sigma(f(e,e)^{-1})$ si ottiene:

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

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

Enunciamo e dimostriamo il teorema che mette in corrispondenza algebre e factor set.

Teorema 5.4. *I due factor set f, g sono equivalenti se e solo se generano algebre equivalenti.*

$$f \sim g \iff (L, K, f) \simeq (L, K, g)$$

Dimostrazione.

- Supponiamo $f \sim g$ allora cerchiamo una mappa tra le due algebre. Data la base della prima algebra $\{x_\sigma\}_{\sigma \in G}$ e λ la funzione indotta da $\sim$, poniamo $y_\sigma = \lambda_\sigma x_\sigma$. Verifichiamo che y_σ soddisfa le relazioni dei generatori di (L, K, g): $y_\sigma k = \lambda_\sigma x_\sigma k = \sigma(k)\lambda_\sigma x_\sigma = \sigma(k) y_\sigma$ inoltre $y_\sigma y_\tau = \lambda_\sigma x_\sigma \lambda_\tau x_\tau = \lambda_\sigma \sigma(\lambda_\tau) f(\sigma, \tau) x_{\sigma\tau} = \sigma(\lambda_\tau)\lambda_\sigma \lambda_{\sigma\tau}^{-1} f(\sigma, \tau) y_{\sigma\tau} = g(\sigma, \tau) y_{\sigma\tau}$. Ciò conclude la prima implicazione.

- Viceversa se le algebre sono isomorfe su K possiamo trovare un isomorfismo di algebre $\varphi : (L, K, f) \longrightarrow (L, K, g)$ che fissa L, ciò è possibile componendo l'isomorfismo dato con un opportuno automorfismo di L su K esteso a tutta l'algebra. Inanzitutto dimostriamo che $\varphi(x_\sigma) = \lambda_\sigma y_\sigma$ con $\lambda_\sigma \in L$: fissato σ sia $\varphi(x_\sigma) = \sum_{\tau \in G} \lambda_\tau y_\tau$ e otteniamo che

$$0 = \varphi(x_\sigma)k - \varphi(x_\sigma)k = \varphi(x_\sigma k) - \sum_{\tau \in G} \lambda_\tau y_\tau k =$$

$$= \varphi(\sigma(k) x_\sigma) - \sum_{\tau \in G} \tau(k)\lambda_\tau y_\tau = \sum_{\tau \in G} \sigma(k)\lambda_\tau y_\tau - \sum_{\tau \in G} \tau(k)\lambda_\tau y_\tau =$$

$$= \sum_{\tau \in G} (\sigma(k) - \tau(k))\lambda_\tau y_\tau$$

  quindi per indipendenza lineare dei y_τ otteniamo che l'unico $\lambda_\tau \neq 0$ è per $\tau = \sigma$. Infine verifichiamo che λ induce la relazione di equivalenza tra f e g:

$$f(\sigma, \tau)\varphi(x_{\sigma\tau}) = \varphi(f(\sigma, \tau) x_{\sigma\tau}) = \varphi(x_\sigma)\varphi(x_\tau) = \lambda_\sigma \sigma(\lambda_\tau) y_\sigma y_\tau =$$

$$= \lambda_\sigma \sigma(\lambda_\tau) g(\sigma, \tau) y_{\sigma\tau} = \sigma(\lambda_\tau)\lambda_\sigma \lambda_{\sigma\tau}^{-1} \varphi(x_{\sigma\tau})$$

  da cui la tesi.

□

Vogliamo ora dimostrare che per ogni C.S.A. esiste un'altra algebra equivalente della forma (L, K, f).

Teorema 5.5. *Per ogni A K-algebra semplice centrale esiste L estensione di Galois di K e f factor set tali che $[A] = [(L, K, f)]$.*

Dimostrazione. Per il teorema 4.33 posso trovare un algebra B nella stessa classe con sottocampo massimale L di Galois su K e dimensione $[B : K] = [L : K]^2$, voglio dimostrare che $B \simeq (L, K, f)$ per un opportuno f. Per ogni automorfismo di Galois si ha un immersione di L algebra semplice in B C.S.A. quindi applicando il teorema di Skolem-Noether (4.25) esiste $x_\sigma \in B$ tale che $\sigma(k) = x_\sigma k x_\sigma^{-1}$ cioè $x_\sigma k = \sigma(k) x_\sigma$. Dimostriamo che x_σ sono linearmente indipendenti su L per assurdo. Se esistesse una combinazione lineare $\sum_{i \leq n-1} k_i x_i = x_n$ con $k_i \neq 0$ dimostriamo l'assurdo per induzione sul numero di elementi diversi da zero della combinazione (n). Il passo base è vero per $n = 1$, per il passo induttivo dimostriamo $n \implies n + 1$: $1 = \sum_{i \leq n} k_i x_i x_{n+1}^{-1}$ quindi scrivendo $0 = 1k - k1$ con $k \in L$ si ottiene $0 = \sum_{i \leq n} k_i (\sigma_i(\sigma_{n+1}^{-1}(k)) - k) x_i$ che ha coefficienti nulli per passo induttivo per ogni k, ma ciò è assurdo perché $\sigma_i \circ \sigma_{n+1} \neq \mathrm{Id}$. Ciò dimostra che $\big[L[\{x_\sigma\}] : K\big] = |G|^2$, quindi abbiamo che $B = L[\{x_\sigma\}]$ è L spazio vettoriale con base $x : G \longrightarrow B$. Vediamo ora come si comporta il prodotto di due elementi della base definendo $f(\sigma, \tau) = x_\sigma x_\tau x_{\sigma\tau}^{-1}$. Notiamo che $f : G \times G \longrightarrow L^*$ perché per ogni $k \in L$ $x_\sigma x_\tau x_{\sigma\tau}^{-1} k = k x_\sigma x_\tau x_{\sigma\tau}^{-1}$ quindi $f(\sigma, \tau) \in C_B(L) = L$. Il fatto che f è un factor set è immediata conseguenza dell'associatività di B: $\sigma(f(\tau, \nu)) f(\sigma, \tau\nu) x_{\sigma\tau\nu} = x_\sigma (x_\tau x_\nu) = (x_\sigma x_\tau) x_\nu = f(\sigma, \tau) f(\sigma\tau, \nu) x_{\sigma\tau\nu}$ da cui l'equazione del factor set 5.5. □

5.3 Prodotti

Avendo nel gruppo di Brauer un prodotto fra algebre, cerchiamo un prodotto tra factor set che induca sulle algebre generate il prodotto del gruppo. Diamo la seguente definizione:

Definizione 5.6 (prodotto di factor set)**.** Dati due factor set f, g il prodotto fg è definito da $fg(\sigma, \tau) = f(\sigma, \tau) g(\sigma, \tau)$.

Inoltre l'insieme dei factor set col prodotto è un gruppo che denotiamo con $Z^2(G, L^*)$.

Dimostrazione. La dimostrazione che il prodotto di due factor set è ancora un factor set discende immediatamente dalla definizione di factor set e dalla commutatività di L^*. La funzione $\mathbb{1}$ è l'elemento neutro e l'inverso di f è $\frac{1}{f}$. □

Osservazione 5.7. *I factor set equivalenti a* $\mathbb{1}$ *sono un sottogruppo di* $Z^2(G, L^*)$ *che chiameremo* $B^2(G, L^*)$.

Dimostrazione. Se f, g sono equivalenti a $\mathbb{1}$ allora

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

quindi è equivalente a $\mathbb{1}$. Lo stesso vale per l'inverso:

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

□

Il nostro scopo è dimostrare che $[(L, K, f)][(L, K, g)] = [(L, K, fg)] \in \mathrm{Br}(K)$ per fare ciò servono un po' di lemmi che andiamo ad enunciare.

Lemma 5.8. *Vale che le due algebre* $(L, K, \mathbb{1})$ *e* $\mathcal{M}_n(K)$ *con* $n = [L : K]$ *sono isomorfe.*

Dimostrazione. Siano x_σ i generatori dell'algebra $(L, K, \mathbb{1})$ come nel teorema 5.5, ogni elemento è della forma $x = \sum_{\sigma\in G} k_\sigma x_\sigma$. Definiamo la mappa $\varphi : (L, K, \mathbb{1}) \longrightarrow \mathrm{End}_K(L)$ definita da $x \mapsto T_x$ dove $T_x(k) = \sum k_\sigma\sigma(k)$. $T_x \in \mathrm{End}_K(L)$ perché combinazione lineare di endomorfismi e φ è un omomorfismo di algebre perché $T_{x_\sigma}T_{x_\tau}(k) = \sigma(\tau(k)) = T_{x_\sigma x_\tau}(k) = T_{\mathbb{1}(\sigma,\tau)x_{\sigma\tau}}(k)$. φ è iniettivo perché (L, K, f) è un algebra semplice (definizione 5.2) e suriettivo perché le due algebre hanno la stessa dimensione su K. □

Lemma 5.9. *Data un'algebra semplice centrale* A *e un suo elemento idempotente* e *(*$e^2 = e$*) si ha che* $[A] = [eAe] \in \mathrm{Br}(K)$.

Dimostrazione. Per il teorema di Wedderburn (3.36) si ha che

$$A \simeq \mathcal{M}_n(D) \simeq \mathcal{M}_n(K) \otimes_K D$$

il polinomio minimo di e è $t^2 - t$ da cui si ottiene che, con un opportuno campio di base, $e = \begin{pmatrix} \mathrm{Id}_r & 0 \\ 0 & 0 \end{pmatrix}$. La tesi segue banalmente dal fatto che $eAe = e\mathcal{M}_n(D)e = \begin{pmatrix} \mathcal{M}_r(D) & 0 \\ 0 & 0 \end{pmatrix} \simeq \mathcal{M}_r(D)$. □

Lemma 5.10. *Come da convenzione* L/K *estensione di Galois con gruppo* G *vale che*

$$L \otimes_K L = \bigoplus_{\sigma\in G} e_\sigma(L \otimes_K 1) = \bigoplus_{\sigma\in G} e_\sigma(1 \otimes_K L)$$

con e_σ *sistema di idempotenti minimali e ortogonali tali che* $e_\sigma(k \otimes 1) = e_\sigma(1 \otimes \sigma(k))$.

Dimostrazione. Poiché L è separabile su K per il teorema dell'elemento primitivo esiste $a \in L$ tale che $L = K[a]$ con polinomio minimo:

$$p(x) = (x - \sigma(a))q_\sigma(x) = \prod_{\sigma \in G}(x - \sigma(a))$$

Definiamo in $L \otimes_K L$ (algebra commutativa) i polinomi $\tilde{p} = \prod_{\sigma\in G}(x - 1 \otimes \sigma(a))$ e $\tilde{q}_\sigma = \prod_{\tau\neq\sigma}(x - 1 \otimes \tau(a))$ osservando che vale la relazione $\tilde{p}_\sigma(x) = (x - 1 \otimes \sigma(a))\tilde{q}_\sigma(x)$. Un osservazione importante per la dimostrazione è che $\tilde{p}(x\otimes 1) = \prod_{\sigma\in G}(x\otimes 1 - 1\otimes\sigma(a)) = \sum_{i\leq n} x^i \otimes c_i = \sum_{i\leq n} c_i x^i \otimes 1 = p(x)\otimes 1$. Notando che $1 \otimes q_\sigma(\sigma(a))$ è invertibile in $L \otimes_K L$ definiamo:

$$e_\sigma = \frac{\tilde{q}_\sigma(a \otimes 1)}{1 \otimes q_\sigma(\sigma(a))}$$

poiché $0 = p(a) \otimes 1 = \tilde{p}(a \otimes 1) = (a\otimes 1 - 1\otimes\sigma(a))\tilde{q}_\sigma(a \otimes 1)$ allora l'elemento $(a \otimes 1 - 1 \otimes \sigma(a))e_\sigma$ è nullo cioè $e_\sigma(a \otimes 1) = e_\sigma(1 \otimes \sigma(a))$ da cui $e_\sigma(a^r \otimes 1) = e_\sigma(a \otimes 1)^r = e_\sigma(1 \otimes \sigma(a))^r = e_\sigma(1 \otimes \sigma(a^r))$ per ogni r. Inoltre per linearità per ogni $x \in L$ vale:

$$e_\sigma(x \otimes 1) = e_\sigma(1 \otimes \sigma(x))$$

Dimostriamo ora che e_σ è idempotente.

$$e_\sigma^2 = e_\sigma \frac{\tilde{q}_\sigma(a \otimes 1)}{1 \otimes q_\sigma(\sigma(a))} = e_\sigma \frac{\tilde{q}_\sigma(1 \otimes \sigma(a))}{1 \otimes q_\sigma(\sigma(a))} = e_\sigma \frac{1 \otimes q_\sigma(\sigma(a))}{1 \otimes q_\sigma(\sigma(a))} = e_\sigma$$

Verifichiamo ora l'ortogonalità degli idempotenti

$$e_\sigma e_\tau = \frac{\tilde{q}_\sigma(a \otimes 1)}{1 \otimes q_\sigma(\sigma(a))} \frac{\tilde{q}_\tau(a \otimes 1)}{1 \otimes q_\tau(\tau(a))} = \tilde{p}(a \otimes 1)c = 0$$

Infine $e_\sigma(L \otimes_K L)$ sono n distinti L-sottospazi ortogonali di $L \otimes_K L$ quindi generano. Ogni sottospazio è di dimensione 1 su L quindi ogni e_σ è idempotente minimale. □

Possiamo ora enunciare il teorema che mette in corrispondenza il prodotto del gruppo di Brauer con quello dei factor set.

Teorema 5.11. *Fissata un'estensione di Galois L su K e due factor set f, g si ha che*

$$(L, K, f) \otimes_K (L, K, g) \simeq (L, K, fg) \otimes_K \mathcal{M}_n(K)$$

cioè $[(L, K, f)][(L, K, g)] = [(L, K, fg)]$.

Dimostrazione. Sia $L \otimes_K L \subset (L, K, f) \otimes_K (L, K, g)$ applicando il lemma 5.10 si trovano e_σ idempotenti minimali ortogonali (chiamiamo per semplicità $e = e_{\mathrm{Id}}$), inoltre abbiamo x_σ e y_σ i generatori con cui si è costruita

l'algebra. Cerchiamo elementi del prodotto tensore che si comportano come i generatori di (L, K, fg):

$$e(x_\sigma \otimes y_\tau)e = e(x_\sigma \otimes y_\tau)\frac{\tilde{q}(a \otimes 1)}{1 \otimes q(a)} = e\frac{\tilde{q}_\tau(\sigma(a) \otimes 1)}{1 \otimes q_\tau(\tau(a))}(x_\sigma \otimes y_\tau) =$$

$$= e\frac{\tilde{q}_\tau(1 \otimes \sigma(a))}{1 \otimes q_\tau(\tau(a))}(x_\sigma \otimes y_\tau) = e\frac{1 \otimes q_\tau(\sigma(a))}{1 \otimes q_\tau(\tau(a))}(x_\sigma \otimes y_\tau)$$

quindi se $\sigma \neq \tau$ allora $q_\tau(\sigma(a)) = 0$ e $e(x_\sigma \otimes y_\tau)e = 0$ altrimenti vale $e(x_\sigma \otimes y_\sigma)e = e(x_\sigma \otimes y_\sigma) = (x_\sigma \otimes y_\sigma)e$. [1] Denoteremo $e(x_\sigma \otimes y_\sigma)e = w_\sigma$ e identificheremo L con il campo isomorfo $e(L \otimes 1)e \subset (L, K, f) \otimes_K (L, K, g)$, verifichiamo che $L[\{w_\sigma\}_{\sigma \in G}]$ è la copia di (L, K, fg) che cerchiamo. Per prima cosa vediamo come commutano gli elementi di K e i generatori w_σ: $w_\sigma e(k \otimes 1)e = e(x_\sigma \otimes y_\sigma)(k \otimes 1)e = e(x_\sigma k \otimes y_\sigma)e = e(\sigma(k) \otimes 1)(x_\sigma \otimes y_\sigma)e = e(\sigma(k) \otimes 1)ew_\sigma$. Infine verifichiamo che $w_\sigma w_\tau = (fg)(\sigma, \tau)w_{\sigma,\tau}$:

$$w_\sigma w_\tau = e(x_\sigma x_\tau \otimes y_\sigma y_\tau)e = e(f(\sigma, \tau)x_{\sigma\tau} \otimes g(\sigma, \tau)y_{\sigma\tau})e =$$

$$= e(f(\sigma, \tau) \otimes 1)(1 \otimes g(\sigma, \tau))ew_{\sigma\tau} = e((fg)(\sigma, \tau) \otimes 1)ew_{\sigma\tau}$$

Abbiamo quindi dimostrato che $e(L, K, f) \otimes_K (L, K, g)e \simeq (L, K, fg)$ quindi per il lemma 5.9 segue la tesi. □

Vogliamo descrivere come si comportano i factor set e le algebre da loro generate rispetto alle estensioni di campo (di Galois) allo scopo di descrivere il gruppo di Brauer con i factor set. Per fare ciò enunciamo il seguente teorema senza darne dimostrazione.

Teorema 5.12. *Sia $F \supset L \supset K$ una torre di estensione di Galois con gruppi $G = \mathrm{Gal}_K(F)$, $H = \mathrm{Gal}_L(F)$ e $G/H = \mathrm{Gal}_K(L)$ e sia $f : G/H \times G/H \longrightarrow L^*$ vale che, definendo $g : G \times G \longrightarrow F^*$ come $g(\sigma, \tau) = f(\bar{\sigma}, \bar{\tau})$*

$$[(L, K, f)] = [(F, K, g)]$$

Dimostrazione. La dimostrazione si può trovare in *Maximal Orders* [8, p 249 Teorema 29.16]. □

Definizione 5.13. Denotiamo con $\mathrm{Br}(L, K)$ (con L estensione di Galois di K) il sottogruppo di $\mathrm{Br}(K)$ delle algebre semplici centrali aventi L come campo di spezzamento.

[1] Una verifica alternativa del fatto appena dimostrato cioè $e(x_\sigma \otimes y_\tau)e = \delta_{\sigma,\tau}e(x_\sigma \otimes y_\tau)$ si ottine dimostrando che $e(1 \otimes x_\sigma) = (1 \otimes x_\sigma)e_\sigma$ e $(1 \otimes y_\tau)e = e_\tau(1 \otimes y_\tau)$ tramite un facile conto e poi usando l'ortogonalità dei e_σ si ottiene che $e(x_\sigma \otimes y_\tau)e = e(x_\sigma \otimes 1)(1 \otimes y_\tau)e = (1 \otimes x_\sigma)e_\sigma e_\tau(1 \otimes y_\tau) = \delta_{\sigma,\tau}(x_\sigma \otimes y_\sigma)e_\sigma = \delta_{\sigma,\tau}e(x_\sigma \otimes y_\sigma)$.

Mettendo assieme i teoremi di questo capitolo si ottiene che $\mathrm{Br}(L,K) \simeq \{[(L,K,f)],\cdot\}$ come gruppo e che l'inclusione di $\mathrm{Br}(L,K)$ in $\mathrm{Br}(F,K)$ corrisponde all'inclusione data dalla mappa del teorema 5.12 ($[(L,K,f)] \mapsto [(F,K,g)]$). Sapendo che le estensioni di Galois finite di un campo K sono un poset diretto, si è dimostrato che

$$\mathrm{Br}(K) \simeq \varinjlim \mathrm{Br}(L,K)$$

Dove il prodotto nel limite diretto è definito, dati $[A] \in \mathrm{Br}(L,K)$ e $[B] \in \mathrm{Br}(F,K)$, dalla composizione dell'immersione in $\mathrm{Br}(LF,K)$ col prodotto in $\mathrm{Br}(LF,K)$, quindi l'isomorfismo è un isomorfismo di gruppi.

5.4 Algebre Cicliche

In questa sezione andremo a specificare i factor set nel caso in cui il gruppo di Galois G è ciclico. Come notazione useremo che il generatore del gruppo sarà σ ($\langle\sigma\rangle = G$).

Finora non abbiamo esibito esempi di factor set, ora che ci siamo ristretti ad un caso più semplice possiamo fornire il seguente esempio.

Proposizione 5.14. *La funzione $f : G \times G \longrightarrow L^*$ definita da*

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

è un factor set per ogni a invertibile.

Notare che nella definizione della funzione f gli indici i e j sono minori di $n = |G|$.

Dimostrazione. Vogliamo provare che per ogni intero i, j e k minori di n vale la formula

$$f(\sigma^i,\sigma^j)f(\sigma^{i+j},\sigma^h) = f(\sigma^j,\sigma^h)f(\sigma^i,\sigma^{j+h}) \tag{5.6}$$

facendo attenzione che gli esponenti sono intesi modulo n. Osserviamo che sia il membro sinistro che quello destro dell'equazione 5.6 possono assumere solo i valori $1, a$ e a^2. Inoltre l'equazione 5.6 è simmetrica perché per questa funzione f vale $f(\sigma,\tau) = f(\tau,\sigma)$. Quindi ci basta dimostrare che se la parte sinistra dell'equazione 5.6 assume il valore 1 (rispettivamente a^2) allora la parte destra assume lo stesso valore. Poi per simmetria vale il se e solo se e nei casi restanti entrambi i membri assumono il valore a.

- Se $1 = f(\sigma^i,\sigma^j)f(\sigma^{i+j},\sigma^h)$ allora vale che $i+j < n$ e di conseguenza anche $i+j+h < n$. In particolare vale che $j+h < n$ quindi $f(\sigma^j,\sigma^h) = 1$ e $f(\sigma^i,\sigma^{j+h}) = 1$ che è la tesi.

- Prendiamo in considerazione il caso $a^2 = f(\sigma^i, \sigma^j) f(\sigma^{i+j}, \sigma^h)$ si deduce che $i + j \geq n$ e anche che $(i + j - n) + h \geq n$. Poiché $i + j + h \geq 2n$ e che $i < n$ si ha $j + h \geq n$ che implica $f(\sigma^j, \sigma^h) = a$. Infine poichè $i+(j+h-n) \geq n$ anche $f(\sigma^i, \sigma^{j+h}) = a$ e ciò conclude la dimostrazione.

□

Teorema 5.15. *Ogni factor set f è equivalente a uno della forma:*

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

Con $a = \prod_{i<n} f(\sigma^i, \sigma) \in K^*$.

Dimostrazione. Nell'algebra $A = (L, K, f)$ cerchiamo dei generatori che abbiano come factor set g e quindi avremo $(L, K, f) = (L, K, g)$ dunque f e g sono equivalenti. Sia x_σ l'elemento di A tale che $x_\sigma k = \sigma(k) x_\sigma$ ha anche la proprietà che $x_\sigma^i k = \sigma^i(k) x_\sigma^i$. Cerchiamo una relazione tra x_σ^k e x_{σ^k}: $x_\sigma^k = \prod_{i \leq k} x_\sigma = \left(\prod_{i<k} f(\sigma^i, \sigma)\right) x_{\sigma^k}$ in particolare per $k = n$ si ottiene che $x_\sigma^n = a = \prod_{i<n} f(\sigma^i, \sigma) \in K^*$ poiché, commutando con x_σ, a appartiene al centro dell'algebra. Abbiamo dimostrato che $A = L[\{x_\sigma^i\}_{i<n}]$ e verificato che il factor set relativo è proprio g. □

D'ora in poi denoteremo nel caso di algebre cicliche (L, K, g) con (L, K, σ, a) dato che g è univocamente determinato da σ e da a. L'algebra può anche essere pensata come $L[x]$ (come algebra) con $x^n = a$ e $xk = \sigma(k)x$.

Proposizione 5.16. *Se $(s, n) = 1$ allora $(L, K, \sigma, a) \simeq (L, K, \sigma^s, a^s)$.*

Dimostrazione. $L[x] = L[y]$ con $y = x^s$ (usando l'ipotesi $(s, n) = 1$) e vale che $y^n = x^{sn} = a^s$ e che $yk = x^s k = \sigma^s(k) x^s = \sigma^s(k) y$. E'evidente che le due algebre sono isomorfe. □

Proposizione 5.17. *Vale che $(L, K, \sigma, 1) \simeq \mathcal{M}_n(K)$.*

Dimostrazione. Segue banalmente dal lemma 5.8 dato che $(L, K, \sigma, 1) \simeq (L, K, \mathbb{1}) \simeq \mathcal{M}_n(K)$ □

Proposizione 5.18. *In $\mathrm{Br}(K)$ vale che:*

$$[(L, K, \sigma, a)][(L, K, \sigma, b)] = [(L, K, \sigma, ab)]$$

Dimostrazione. Prendendo i due factor set relativi f e g per il teorema 5.11 l'algebra prodotto è generata dal prodotto dei factor set che è della forma ciclica ab. □

Proposizione 5.19. *Le algebre (L, K, σ, a) e (L, K, σ, b) sono isomorfe se e solo se esiste $c \in L^*$ tale che $b = \mathrm{N}(c)a$.*

Dimostrazione. Se $b = \mathrm{N}(c)a$ e x il generatore di (L, K, σ, a) allora $y = cx$ è il generatore di (L, K, σ, b) infatti $yk = cxk = c\sigma(k)x = \sigma(k)y$ inoltre $y^n = (cx)^n = \left(\prod_{i=0}^{n-1} \sigma^i(c)\right) x^n = \mathrm{N}(c)a = b$, quindi le due algebre sono isomorfe. Viceversa se le due algebre sono isomorfe per il teorema 5.4 i factor set sono equivalenti cioè esiste $\lambda : {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \longrightarrow L^*$ tale che

$$g(\sigma^i, \sigma^j) = \sigma^i(\lambda_j)\lambda_i\lambda_{i+j}^{-1} f(\sigma^i, \sigma^j)$$

Si ottiene immediatamente con $j = 0$ che $\sigma^i(\lambda_0) = 1$ cioè $\lambda_0 = 1$ e ponendo $j = 1$ e $i < n-1$ si ottiene che $\lambda_{i+1} = \lambda_i\sigma^i(\lambda_1)$ e per induzione si ottiene che $\lambda_k = \prod_{i=0}^{k-1} \sigma^i(\lambda_1)$. Per concludere imponiamo $j = 1$ e $i = n-1$ e ottieniamo che $b = \sigma^{n-1}(\lambda_1)\lambda_{n-1}\lambda_0^{-1}a = \mathrm{N}(\lambda_1)a$. □

Vediamo ora il teorema che illustra il comportamento di algebre cicliche in caso di torri di estensioni.

Teorema 5.20. *Data la torre di estensioni $F \supset L \supset K$ (con $n = [L : K]$ e $m = [F : L]$) e il gruppo ciclico $G = \mathrm{Gal}_K(F) = \langle\sigma\rangle$. Sia $H = \mathrm{Gal}_L(F) = \langle\sigma^n\rangle$ e ${}^{G}\!/_{H} = \mathrm{Gal}_K(L) = \langle\bar{\sigma}\rangle$ con $\bar{\sigma}$ l'immagine di σ nel quoziente, vale che:*

$$[(L, K, \bar{\sigma}, a)] = [(F, K, \sigma, a^m)]$$

Dimostrazione. Il factor set relativo alla prima algebra è

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

Per il teorema 5.12 l'algebra $[(F, K, g)] = [(L, K, f)]$ con

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

Ma per il teorema 5.15 g è equivalente al factor set

$$h(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{se } i + j < nm \\ b & \text{se } i + j \geq nm \end{cases}$$

con $b = \prod_{i=0}^{nm-1} g(\sigma^i, \sigma) = \prod_{i \equiv -1(n)} a = a^m$. Abbiamo dimostrato che:

$$[(L, K, \bar{\sigma}, a)] = [(L, K, f)] = [(F, K, g)] = [(F, K, h)] = [(F, K, \sigma, a^m)]$$

□

Capitolo 6

Campi Locali

Introduciamo ora i campi locali, campi dotati di valutazione discreta e topologia indotta. Inoltre godono di buone proprietà del tipo che estensioni di campi locali è ancora un campo locale ed è anche noto il loro gruppo di Galois. In questa sezione dimostreremo molte di queste proprietà che saranno poi utilizzate nell'ultimo capitolo per calcolarne il gruppo di Brauer.

6.1 Valutazioni discrete

La definizione che daremo è quella di valutazione discreta ma, dato che useremo solo valutazioni discrete, a volte potrà essere omesso l'aggettivo discreto.

Definizione 6.1 (valutazione discreta)**.** Dato un corpo K, una funzione $v : K^* \longrightarrow \mathbb{Z}$ è una valutazione discreta se è un omomorfismo suriettivo di gruppi e vale che:

$$v(x+y) \geq \min(v(x), v(y)) \tag{6.1}$$

per ogni $x, y \in K^*$ tale che $x + y \neq 0$.

Si può anche definire la valutazione v su tutto il corpo K definendo $v(0) = +\infty$ e cambiando dominio e codominio $v : K \longrightarrow \mathbb{Z} \cup \{+\infty\}$. Valgono ancora la proprietà di omomorfismo di gruppi e la disuguaglianza 6.1 con la convenzione che $n + \infty = \infty$ e che $n < +\infty$.

Definizione 6.2 (anello degli interi)**.** Data una valutazione

$$v : K \longrightarrow \mathbb{Z} \cup \{+\infty\}$$

si dice anello degli interi (o di valutazione discreta) l'anello

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$$

Dimostrazione. $\mathcal{O}$ è chiuso per somma perché $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$. $\mathcal{O}$ è chiuso per prodotto perché $v(xy) = v(x)+v(y) \geq 0$. Infine $\mathcal{O}$ contiene l'opposto di ogni elemento (se $x \in \mathcal{O}$ allora $v(-x) = v(-1) + v(x) \geq 0$), quindi $\mathcal{O}$ è anello. □

Proposizione 6.3. *l'anello degli interi $\mathcal{O}$ di un campo è un dominio a ideali principali (PID) locale con generatore dell'ideale principale π.*

Dimostrazione. $\mathcal{O}$ è un dominio perché immerso in un campo. Tutti e soli gli elementi invertibili in $\mathcal{O}$ hanno valutazione nulla, infatti se $v(x) = 0$ allora $v(x^{-1}) = -v(x) = 0$ e $v \in \mathcal{O}$. Inoltre sia π un qualsiasi elemento di valutazione unitaria ($v(\pi) = 1$). Vogliamo dimostrare che $\mathcal{O} = \mathcal{O}^* \sqcup (\pi)$, per ogni x non invertibile abbiamo $0 < v(x) = n$ e calcoliamo $v(x\pi^{-n}) = v(x) - n = 0$ quindi $x\pi^{-n} = u \in \mathcal{O}^*$ cioè $x = \pi^n u$. Da ciò si deduce che $\mathcal{O}$ è PID e anello locale. □

Corollario 6.4. *Ogni elemento di un campo locale x si scrive come prodotto di una potenza di un elemento di valutazione uno π e un elemento invertibile u ($x = u\pi^n$ con n intero).*

Dimostrazione. Per $x \in \mathcal{O}$ la tesi è vera per la dimostrazione precedente con n non negativo. Per un elemento qualsiasi $x = \frac{a}{b}$ basta scrivere $a = u\pi^n$ e $b = v\pi^m$ e quindi si ottiene che $x = (uv^{-1})\pi^{n-m}$ che è la tesi. □

Enunciamo e dimostriamo il viceversa del teorema precedente.

Proposizione 6.5. *Se A è un dominio locale noetheriano tale che l'ideale massimale M è generato du un elemento π non nilpotente allora A è anello di valutazione discreta.*

Dimostrazione. Dimostriamo che $\bigcap_{n\geq 0} M^n = 0$, supponiamo $y \in \bigcap_{n\geq 0} M^n$ allora per ogni n esiste $x_n \in A$ tale che $y = \pi^n x_n$ quindi la successione crescente di ideali $x_n A$ è definitivamente stazionaria perché A è noetheriano. In paricolare esiste N tale che $x_{N+1} = tx_N = t\pi x_{N+1}$ quindi poiché $1 - t\pi$ non è in M allora è inveribile quindi $x_{N+1} = 0$ cioè $y = 0$. In conclusione ogni elemento $z \in A \setminus 0$ si scrive in modo unico come $z = \pi^n u$ con $u \in A^*$ quindi è possibile definire una valutazione discreta $v(z) = n$ su A ed estenderla al campo dei quozienti da cui la tesi. □

Lemma 6.6. *Siano $x_i \in K^*$ campo dotato di una valutazione v finiti elementi tali che per ogni $1 < i \leq n$ si ha $v(x_1) < v(x_i)$ allora*

$$v\left(\sum_{i=1}^{n} x_i\right) = v(x_1)$$

Dimostrazione. Possiamo supporre $x_1 = 1$ perché v è un omomorfismo di gruppi. Sia P l'ideale primo dell'anello degli interi $\mathcal{O}$, poiché $x_1 \notin P$ e $x_i \in P$ allora $\sum_i x_i \notin P$ di conseguenza

$$0 \geq v\left(\sum_i x_i\right) \geq \min_i \{v(x_i)\} = v(x_1) = 0$$

Da cui la tesi. □

Definizione 6.7 (Valore assoluto)**.** Un valore assoluto su un campo K è una funzione $|\cdot|$da K nei reali non negativi tale che:

- $|x| = 0$ se e solo se $x = 0$.
- Per ogni coppia di elementi in K vale $|xy| = |x||y|$.
- Vale la disuguaglianza triangolare cioè $|x + y| \leq |x| + |y|$.

Inoltre se vale la disuguaglianza più forte $|x + y| \leq \max\{|x|, |y|\}$ il valore assoluto si dice ultrametrico.

Mostriamo ora che una valutazione discreta induce un valore assoluto ultrametrico.

Osservazione 6.8. *Una valutazione induce un valore assoluto ultrametrico.*

Dimostrazione. Scelto un reale a compreso tra zero e uno, si definisce il valore assoluto ultrametrico come $|x| = a^{v(x)}$ (con la convenzione che $a^{+\infty} = 0$). Verifichiamo le tre proprietà del valore assoluto ultrametrico. Se $|x| = 0$ allora $v(x) = +\infty$ quindi $x = 0$, il viceversa è ovvio. Inoltre $|xy| = a^{v(xy)} = a^{v(x)+v(y)} = a^{v(x)}a^{v(y)} = |x||y|$. Infine verifichiamo la disuguaglianza ultrametrica $\max\{|x|, |y|\} = a^{\min\{v(x),v(y)\}} \geq a^{v(x+y)} = |x + y|$. □

Abbiamo visto che una valutazione induce un valore assoluto ultrametrico. Un valore assoluto ultrametrico induce a sua volta una topologia τ, ora ci interessiamo alla relazione tra valutazioni e topologie.

Teorema 6.9. *Due valutazioni v_1 e v_2 coincidono se e solo se le topologie indotte τ_1 e τ_2 coincidono.*

Dimostrazione. Dimostriamo la freccia non ovvia, supponendo $\tau_1 = \tau_2$. La successione x^n converge a zero in topologia se e solo se $a^{v(x^n)} \longrightarrow 0$ se e solo se $v(x^n) = nv(x) \longrightarrow +\infty$ se e solo se $v(x) > 0$. Siano π_1 e π_2 i generatori dei rispettivi ideali massimali, allora $v_1(\pi_2) \geq 1$ e $v_2(\pi_1) \geq 1$. Se non valesse l'uguaglianza (per esempio $v_2(\pi_1) > 1$) si avrebbe che $v_2(\pi_1\pi_2^{-1}) = v_2(\pi_1) - v_2(\pi_2) > 0$ quindi $v_1(\pi_1\pi_2^{-1}) > 0$ e $v_1(\pi_2) < 1$ che è assurdo (idem scambiando 1 e 2). Quindi $v_2(\pi_1) = 1$ cioè $v_1 = v_2$ su tutti gli elementi e $v_i(\pi_1\pi_2^{-1}) = 0$. □

Definizione 6.10 (campo dei residui)**.** Data una valutazione v si chiama campo dei quozienti k il quoziente tra l'anello degli interi per il suo ideale massimale.

$$k = \mathcal{O}/(\pi)$$

Definizione 6.11 (Successione di Cauchy)**.** Una successione x_n di elementi di un campo dotato di una valutazione si dice di Cauchy se per ogni $\epsilon > 0$ esiste un intero N tale che per ogni coppia di interi $n, m \geq N$ vale

$$|x_n - x_m| < \epsilon$$

dove la funzione $|\cdot|$ è il valore assoluto ultrametrico indotto da v.

Osservazione 6.12. *La definizione di successione di Cauchy non dipende dalla scelta del parametro a.*

Dimostrazione. Prendiamo due diversi reali $a < b$ nell'intervallo $(0, 1)$ poiché $|x|_a \leq |x|_b$ ogni successione di Cauchy secondo $|\cdot|_b$ è una successione di Cauchy di $|\cdot|_a$. Viceversa vale che $|x|_a = a^{v(x)} = b^{v(x)\frac{\log a}{\log b}} = |x|_b^{\frac{\log a}{\log b}}$. Quindi se $|x_n - x_m|_a < \epsilon$ allora $|x_n - x_m|_b < \epsilon^{\frac{\log b}{\log a}}$ quindi è ancora successione di Cauchy. □

Definizione 6.13 (campo completo)**.** Un campo con una valutazione si dice completo se ogni successione di Cauchy converge a un elemento del campo.

Definizione 6.14 (campo locale)**.** Si dice campo locale un campo K dotato di una valutazione discreta v, completo e con campo residuo k finito.

Definizione 6.15 (intero)**.** Dato un anello A incluso in B un elemento b di B si dice intero se esiste un polinomio monico $f \in A[x]$ tale che $f(b) = 0$.

Proposizione 6.16. *b è intero su A se e solo se $A[b] \subset B$ è un A-modulo finitamente generato.*

Dimostrazione. Se b è intero su A allora l'anello $A[b] = (1, b, \ldots, b^{n-1})_A$ con $n = \deg f$ è finitamente generato. Viceversa se $A[b]$ è finitamente generato allora è generato su A da finiti polinomi $\{f_i(b)\}_{i<k}$ quindi ogni elemento si può scrivere come combinazione lineare dei $f_i(b)$. In particolare sia $m = \max_{i<k}\{deg(f_i)\} + 1$ allora $b^m = \sum_{i<k} a_i f_i(b)$ cioè b è radice del polinomio monico $x^m - \sum_{i<k} a_i f_i(x) \in A[x]$. □

Definizione 6.17 (chiusura integrale)**.** La chiusura integrale di A in B è l'anello degli elementi interi di B su A.

Proposizione 6.18. *La chiusura integrale di un anello noetheriano A in B è un sottoanello di B.*

Dimostrazione. Vogliamo vedere che dati due elementi a e b in B interi su A allora $a+b$, $-a$ e ab sono interi su A. Usando la proposizione 6.16 otteniamo che la tesi è equivalente a dimostrare che se $A[a]$ e $A[b]$ sono A-moduli finitamente generati allora lo sono anche $A[a+b]$, $A[-a]$ e $A[ab]$, ma ciò è banalmente vero. □

Definizione 6.19 (integralmente chiuso)**.** Un anello A si dice integralmente chiuso se coincide con la sua chiusura integrale nel campo dei quozienti.

Sembra un'infelice notazione chiamare gli interi di un campo gli elementi con valutazione non negativa e gli interi su un anello gli elementi con polinomio monico, ma la seguente proposizione afferma che i due anelli coincidono.

Proposizione 6.20. *L'anello degli interi di un campo è integralmente chiuso.*

Dimostrazione. Per assurdo esiste $x \in K \setminus \mathcal{O}$ intero su $\mathcal{O}$, ovviamente si ha che $-m = v(x) < 0$ e che $\sum_{i \leq n} c_i x^i = 0$ da cui $v(x^n) = -nm$ e $v(c_i x^i) > -nm$ per ogni $i < n$. Per il lemma 6.6 $v(0) = -nm$ e ciò è assurdo, quindi ogni intero è in $\mathcal{O}$. □

6.2 Domini di Dedekind

Introduciamo i domini di Dedekind perché vale una buona proprietà; ogni estensione finita ed intera di un dominio di Dedekind è un dominio di Dedekind. Inoltre il localizzato per un primo di un dominio di Dedekind è un anello di valutazione discreta. Questi fatti dimostrati in seguito serviranno ad ottenere importanti teoremi sulle estensioni finite di campi locali.

Definizione 6.21 (dominio di Dedekind)**.** Un anello A è un dominio di Dedekind se ogni ideale si può scrivere in modo unico come prodotto finito di ideali primi.

Proposizione 6.22. *Sia A un dominio di integrità, i seguenti fatti sono equivalenti*

1. *A è Noetheriano e per ogni primo P diverso da zero A_P è un anello di valutazione discreta.*
2. *A è Noetheriano, integralmente chiuso e ogni primo diverso da zero è massimale (dimensione di Krull uno).*
3. *A è un dominio di Dedekind.*

Dimostrazione.

- $3 \Rightarrow 1$ Dimostriamo che l'anello è Noetheriano. Si osserva che se $I \supset J$ allora sia $J = \prod_{i\in\Lambda} P_i$ si ha che $I = \prod_{i\in\Gamma\subset\Lambda} P_i$ quindi una catana di ascendente di ideali è stazionaria perché il numero di fattori primi è finito. Inoltre localizzando per P si ottiene A_P anello locale ed è ancora dominio di Dedekind. Poiché A_P è noetheriano P è generato da un numero finito di elementi $\{p_i\}_{i\leq n}$ e ognuno genera un ideale che è una potenza di P ($(p_i) = P^{n_i}$). Si ottiene infine che $P = (p_i)_{i\leq n} = P^{\min n_i}$ e per unicità della fattorizzazione esiste j tale che $n_j = 1$ che implica $P = (p_j)$. Infine p_j non è nilpotente e applicando la proposizione 6.5 A_P è anello di valutazione.

- $1 \Rightarrow 2$ Dimostriamo che A ha dimensione di Krull uno, prendiamo per assurdo due primi $P \subsetneq Q$ allora A_Q contiene due ideali primi P e Q e applicando la proposizione 6.3 si vede che A_Q non può essere un anello di valutazione contro le ipotesi. Dimostriamo che A è integralmente chiuso. Sia b intero su A allora è intero su A_P per ogni primo. Sappiamo che un anello di valutazione è integralmente chiuso quindi $b \in A_P$ per ogni primo e quidi $b \in A$ (essere integralmente chiuso è proprietà locale).

- $2 \Rightarrow 3$ La seguente dimostrazione è abbastanza lunga e richiede l'introduzione degli ideali frazionari perciò la dimostreremo a parte.

□

Definizione 6.23 (ideale frazionario)**.** Dato A dominio e Q campo dei quozienti un sotto A-modulo I di Q è un ideale frazionario se esiste $d \in A$ con $dI \subset A$.

Equivalentemente si può definire ideale frazionario I un A-modulo della forma cJ con $c \in Q$ e $J \subset A$. Da questa definizione è evidente che se A è Noetheriano allora I è un A-modulo finitamente generato.

Definizione 6.24. Un ideale frazionario I si dice invertibile se esiste un altro ideale frazionario J tale che $IJ = A$.

Definizione 6.25. Chiamiamo l'inverso di I, un sotto A-modulo di Q, il modulo:

$$I^{-1} = (A : I) = \{x \in Q \mid xI \subseteq A\}$$

Ovviamente l'inverso inverte le inclusioni tra ideali ed il prodotto di ideali è monotono rispetto l'inclusione.

Lemma 6.26. *Ogni ideale principale è invertibile e* $(a^{-1}) = (a)^{-1}$.

Dimostrazione. $a^{-1} \in (a)^{-1}$ perché $a^{-1}ab = b \in A$ quindi abbiamo dimostrato l'inclusione $\subseteq$. L'altra inclusione è data da $x \in (a)^{-1}$ se $xa = b \in A$ allora $x = \frac{b}{a} \in (a^{-1})$. □

Corollario 6.27. *Se A Noetheriano allora per ogni A-modulo I in Q I^{-1} è finitamente generato.*

Dimostrazione. Dato $a \in I$ consideriamo l'ideale $(a) \subset I$ allora $(a^{-1}) = (a)^{-1} \supset I^{-1}$ e ricordando che sottomodulo di finitamente generato è finitamente generato (su A noetheriano) allora I^{-1} è finitamente generato. □

Proposizione 6.28. *Se I è invertibile allora I^{-1} è l'unico inverso.*

Dimostrazione. Supponiamo che J tale che $IJ = A$, naturalmente $J \subseteq I^{-1}$. Dimostriamo l'altra inclusione, $A = IJ \subseteq II^{-1} \subseteq A$ quindi $II^{-1} = A$ cioè I^{-1} è un altro inverso. Ma l'inverso è unico perché il prodotto tra ideali è associativo: $J = JII^{-1} = I^{-1}$. □

Lemma 6.29. *In un anelo che soddisfa (2) per ogni ideale frazionario I vale che $A = \{x \in Q \mid xI \subseteq I\} = (I : I)$.*

Dimostrazione. Sia $\{a_i\}_{i \leq n}$ un sistema di generatori e supponiamo $b \in (I : I)$ vogliamo dimostrare che $b \in A$. Per definizione esistono $c_{i,j}$ tali che $ba_i = \sum_{j \leq n} c_{i,j} a_j$ quindi $(b_l - C)x = 0$ sia $p(x) = \det(x \operatorname{Id}_n - C) \in A[x]$ polinomio monico e vale $p(b) = 0$ cioè b intero su A. Essendo A integralmente chiuso $b \in A$. □

Lemma 6.30. *Sia S l'insieme parzialemente ordinato per inclusione degli ideali I in A tale che $I^{-1} \supsetneq A$ allora ogni elemento massimale per inclusione è primo e invertibile.*

Dimostrazione. Dimostriamo che m, un elemento masimale per inclusione, è primo. Siano $a, b \in A$ tali che $a \notin m$ e $ab \in m$ vogliamo dimostrare che $b \in m$. Sia $c \in m^{-1} \setminus A$, per massimalità di m vale che $(m + a)c \not\subseteq A$ altrimenti $c \in (m + a)^{-1} \setminus A$. In particolare $mc + ac \subseteq A + ac$ quindi $ac \notin A$, inoltre $a(bc) \in A$ quindi $ac \in (b)^{-1}$ e $ac \in m^{-1}$. Abbiamo quindi dimostrato che $ac \in (m + b)^{-1}$ e $ac \notin A$ e per massimalità di m in S si ha che $m = m + (b)$ da cui $b \in m$. Dimostriamo che m è invertible, $mm^{-1} \neq m$ perché altrimenti si avrebbe che $m^{-1} \subseteq (m : m) = A$ che è assurdo perché $m \in S$. Inoltre $m \subsetneq mm^{-1} \subseteq A$ e poiché ogni primo è massimale allora $mm^{-1} = A$. □

Lemma 6.31. *Sempre con A come da ipotesi (2) vale che un ideale è invertibile se e solo se è prodotto finito di ideali primi invertibili.*

Dimostrazione. Se $I = \prod_{i \leq n} m_i$ allora $I^{-1} = \prod_{i \leq n} m_i^{-1}$ e $II^{-1} = A$. Viceversa I è un ideale proprio allora $I^{-1} \supsetneq A$, per il lemma precedente esiste m_1 primo invertibile tale che $I \subsetneq Im_1^{-1} \subseteq A$. Applicando lo stesso ragionamento a Im_1^{-1} si ottiene che o in finiti passi $I \prod_{i \leq n} m_i^{-1} = A$ (che è la tesi) oppure si ottiene una catena strettamente ascendente infinita di ideali contro l'ipotesi A Noetheriano. □

Ci avviciniamo alla fattorizzazione in ideali primi dimostrando che ogni primo è invertibile.

Teorema 6.32. *Sia A che soddisfa l'ipotesi (2) allora ogni primo non nullo è invertibile.*

Dimostrazione. Sia $a \in P \setminus 0$ naturalmente $(a) \subseteq P$ dato che (a) è principale allora è invertibile e quindi per il lemma è prodotto di primi invertibili $P \supseteq \prod_{i \leq n} m_i$ e per il lemma di scansamento esiste j tale che $P \supseteq m_j \neq 0$ ma poichè A è di dimensione uno $P = m_j$. □

Teorema 6.33. *Ogni anello che soddisfa (2) è di Dedekind.*

Dimostrazione. Fissato $I \in A$ dimostriamo induttivamente che è prodotto di primi. Sia $P_1 \supseteq I$ un primo allora $I \supsetneq IP_1^{-1} \supseteq A$, la catena ascendente $I \prod_{i \leq n} P_i^{-1}$ è definitivamente stazionaria quindi si avrà che $I \prod_{i \leq n} P_i^{-1} = A$ cioè $I = \prod_{i \leq n} P_i$. Inoltre la fattorizzazione è unica, infatti supponendo $\prod_{i \leq n} p_i = \prod_{j \leq m} q_j$ con n minimo per cui si la fattorizzazione non è unica, si ha che $p_i \supseteq \prod_{j \leq m} q_j$ e per il lemma di scansamento esiste j tale che $p_i \supseteq q_j$. Avendo A dimensione di Krull uno i due primi coincidono ed essendo invertibili ci riconduciamo a una fattorizzazione non unica più corta che è assurdo. □

Per comodità d'ora in poi A sarà un anello Noetheriano integralmente chiuso, K il campo dei quozienti. Inoltre L sarà un estensione finita di K e B la chiusura integrale di A in L.

Lemma 6.34. *Se L è separabile su K allora B è un A-modulo libero finitamente generato di rango $[L : K]$.*

Dimostrazione. Sia F la chiusura di Galois di L e fissato $x \in B$ sia p il polinomio monico della definizione intero. Vogliamo dimostrare che $\mathrm{tr}_{L/K}(x)$ è in A. Ogni coniugato di x in F è ancora intero su A perché se $p(x) = 0$ per ogni $\sigma \in \mathrm{Gal}_K(F) \quad p(\sigma(x)) = 0$ quindi intero. Per l'osservazione 4.37 $\mathrm{tr}(x) = \sum_{\sigma \in G} \sigma(x)$ ed è intero perché somma di interi. La traccia è quindi intera su A e appartenente al campo dei quozienti K quindi è in A. Sia e_i base di L su K, senza perdita di generalità supponiamo che $e_i \in B$ e chiamiamo $V = \bigoplus_i e_i A$. Definiamo, ricordando l'esistenza della forma traccia 4.38:

$$V^* = \{x \in L \mid \mathrm{tr}(xy) \in A \ \forall y \in V\}$$

e analogamente B^*. Si ha che $V \subset B \subset B^* \subset V^*$ ma V e V^* sono moduli liberi della stessa dimensione e quindi B è modulo finitamente generato con dimensione $[B : A] = [L : K]$. □

Lemma 6.35. *Se B è un A-modulo finitamente generato A anello noetheriano allora B è noetheriano e integralmente chiuso.*

Dimostrazione. La successione

$$0 \longrightarrow \ker \varphi \longrightarrow A^n \longrightarrow B \longrightarrow 0$$

è esatta e sapendo che A^n è noetheriano e che quoziente di noetheriano è noetheriano, si deduce che B è noetheriano.

Ogni elemento $x \in L$ intero su B è anche intero su A quindi appartiene alla chiusura integrale di A in L che è B. □

Lemma 6.36. *Dati due primi in B contenuti uno dentro l'altro ($P \subset Q$) tali che $P \cap A = Q \cap B$ allora i dui primi coincidono.*

Dimostrazione. Quozientando B per P si ottiene che la stessa proprietà nel caso $P = 0$ quindi senza perdita di generalità dimostriamo il lemma in questo caso. Sia $x \in Q \setminus 0$ e p il polinomio monico della definizione di intero, il termine noto a che lo possiamo supporre diverso da zero è in $xB \subset Q$ quindi $a \in Q \cap A = P \cap A = 0$. In conclusione ogni elemento di Q deve stare anche in P. □

Teorema 6.37. *Sa A è un dominio di Dedekind e B un A-modulo finitamente generato allora B è un dominio di Dedekind.*

Dimostrazione. Per il lemma 6.35 B è un anello Noetheriano e integralmente chiuso. Inoltre per la proposizione 6.22 la tesi è equivalente a dimostrare che ogni primo non nullo è massimale. Siano $P_1 \subset P_2$ primi di B non nulli allora $P_1 \cap A \subset P_2 \cap A$ ma poichè A è Dominio di Dedekind allora $P_1 \cap A = 0$ o $P_1 \cap A = P_2 \cap A$. Nel primo caso per il lemma 6.36 $P_1 = 0$ contro le nostre ipotesi, mentre nel secondo caso sempre per il lemma 6.36 $P_1 = P_2$ quindi ogni primo coincide col massimale che lo contiene. □

Definizione 6.38. Se Q ideale di B e P ideale di A si dice che $Q|P$ se $P = Q \cap A$ (equivalentemente se $PB \subset Q$).

Sia P un ideale di A e PB la sua estensione a B, per il teorema 6.37 PB si fattorizza in prodotto di ideali primi. Cioè

$$PB = \prod_{Q|P} Q^{e_Q}$$

con $e_Q = v_Q(PB)$.

Definizione 6.39 (indice di ramificazione)**.** Definiamo l'indice di ramificazione di Q nell'estensione L su K (campi delle frazioni di B e A) l'intero positivo e_Q.

Definizione 6.40 (grado residuo)**.** Si definisce grado residuo di Q nell'estensione L su K l'intero positivo $f_Q = \left[{}^{B}\!/_{Q} : {}^{A}\!/_{P} \right]$.

Definizione 6.41. Un'estensione di campi L su K si dice non ramificata in $Q \subset B$ se $e_Q = 1$ e ${}^{B}\!/_{Q}$ è estensione separabile di ${}^{A}\!/_{P}$.

Un'estensione di campi L su K si dice non ramificata in $P \subset A$ se per ogni $Q|P$ è non ramificata in Q.

Definizione 6.42. Un'estensione di campi si dice totalmente ramificata in P se esiste un unico ideale primo Q che divide P e il grado residuo è uno ($f_Q = 1$).

6.3 Anelli locali

Sia A un anello di valutazione, P il suo ideale massimale K il campo dei quozienti e k il campo dei residui. Per ogni polinomio monico $f \in A[x]$ definiamo $B = {}^{A[x]}\!/_{(f)}$ una A-algebra con base $\{x^i\}_{i<n}$ e campo dei quozienti L. Infine sia $l = {}^{B}\!/_{PB}$ e $\bar{f} \in k[x]$ la proiezione di f. Per il terzo teorema di omomorfismo si ha che $l = {}^{k[x]}\!/_{(\bar{f})}$. Supponiamo $\bar{f}$ irriducibile e andiamo a dimostrare proposizioni utili in seguito.

Proposizione 6.43. *Nelle ipotesi sopra B è un anello di valutazione discreta con ideale massimale PB e campo dei residui l.*

Dimostrazione. Se $\bar{f}$ è irriducibile allora $(\bar{f})$ è massimale quindi l è un campo e PB è ideale massimale. Dobbiamo dimostrare che B è locale. Se esistesse un altro ideale massimale M in B si avrebbe $M + PB = B$ e sappiamo per il lemma 6.35 che B è noetheriano, quindi usando il lemma di Nakayama (per l'enunciato si veda Lang [4, p 424]) si ottiene che $M = B$ contro l'ipotesi che M sia proprio. Sia π il generatore di $P = \pi A$ allora $\pi B = \pi AB = PB$ quindi PB è principale e non nilpotente perché non lo era in A. Abbiamo tutte le ipotesi per usare su B la proposizione 6.5 quindi B è anello di valutazione. □

Corollario 6.44. *Il polinomio f è irriducibile in $K[x]$ e B è la chiusura integrale di A in L.*

Dimostrazione. B è un dominio quindi $B \otimes_A K \simeq {}^{A[x] \otimes_A K}\!/_{(f)} \simeq {}^{K[x]}\!/_{(f)}$ è dominio e quindi (f) è primo in PID quindi massimale e f irriducibile. Abbiamo già dimostrato che B è integralmente chiuso per il lemma 6.35 e ogni elemento intero su A è anche intero su B quindi in B, da cui la tesi. □

Corollario 6.45. *Se il polinomio $\bar{f}$ è separabile allora L su K è non ramificata in P.*

Dimostrazione. La proposizione 6.43 afferma che $PB = Q$ è primo, cioè $e_Q = 1$ perciò l'estensione è non ramificata in Q e quindi in P perché Q è l'unico primo che divide P. Infine $l = {}^{k[x]}\!/_{(\bar{f})}$ è separabile su k perché $\bar{f}$ è separabile. □

6.4 Campi completi

Supponiamo in questa sezione che K sia completo rispetto la topologia indotta dalla valutazione v.

Teorema 6.46. *Nelle solite ipotesi vale che B è anello di valutazione discreta e A modulo libero di rango $[L : K]$, inoltre L è completo rispetto la topologia indotta da B.*

Dimostrazione. Iniziamo supponendo che L sia separabile su K. Per il lemma 6.34 B è A-modulo libero finitamente generato di rango $n = [L : K]$ e per il lemma 6.35 è un dominio di Dedekind. L è un K-spazio vettoriale e ogni primo di B induce una valutazione w_i su L e una topologia vettoriale τ_i su L. Però poiché L è di dimensione finita esiste unica topologia su L (che è completa) e per il teorema 6.9 esiste unica valutazione $w = w_i$ quindi tutte le valutazioni sono indotte da un solo primo. Perciò B è locale e anello di valutazione discreta.

Trattiamo ora il caso non separabile, senza perdita di generalità possiamo spezzare l'estensione in una separabile e una puramente inseparabile e spezzando a sua volta quella puramente inseparabile ci riconduciamo al caso di un estensione radicale non separabile. Sia $L = K(x)$ con $x^q \in K$ per qualche $q = p^k$ definiamo la valutazione $w(y) = \frac{v(y^q)}{m}$ dove m è l'intero positivo che rende suriettiva la valutazione w. L'anello degli interi di w contiene $A[x] = B$ ma ogni elemento con valutazione non negativa è intero su A quindi è in B perciò B è l'anello degli interi di L. B è quindi dominio di Dedekind locale e analogamente al caso precedente si dimostra che L è completo. Rimane da dimostrare che B è A-modulo finitamente generato. Siano $b_i \in B$ elementi tali che le loro immagini $\bar{b_i}$ in $B/\pi B$ siano base di $B/\pi B$ su k, vogliamo dimostrare che b_i siano linearmente indipendenti su A. Se esistesse una combinazione lineare tale che $\sum_{i\leq n} a_i b_i = 0$ possiamo supporre (a meno di dividere tutti gli a_i per un opportuna potenza di π) che un a_j non sia divisibile per π. Quindi riducendo modulo πB avremmo una combinazione lineare $\sum_{i\leq n} \bar{a_i}\bar{b_i} = 0$ con un coefficiente non nullo e ciò è assurdo. Infine, chiamando $M = span_B \{b_i\}_{i\leq n}$, per ogni $b \in B$ possiamo trovare $m \in M$ e $b' \in B$ tali che $b = m + \pi b'$. Per induzione si può scrivere ogni elemento $b = \sum_{i\in\mathbb{N}} m_i \pi^i$ ma M è completo perché A modulo finitamente generato quindi $b \in M$ e $B = M$. Abbiamo dimostrato che B è A-modulo finitamente generato di rango minore o uguale a $\left[B/\pi B : k\right] = \left[B/\pi B : A/\pi A\right] = n$. Infine $\{x_i\}_{i<q}$ sono elementi di B linearmente indipendenti su A quindi il rango è esattamente $[L : K]$. □

Corollario 6.47. *Esiste un unica valutazione su L che prolunga la valutazione di K e inoltre due elementi coniugati hanno la stessa valutazione.*

Dimostrazione. Dalla dimostrazione del teorema si è dimostrato in due modi diversi a seconda dei casi che l'estensione è unica. Nel caso dell'estensione

radicale e puramente inseparabile i coniugati di un elemento coincide sempre con l'elemento stesso, quindi la tesi segue banalmente. Nell'altro caso l'estensione di campi è separabile e quindi possiamo prenderne la chiusura di Galois L. Per ogni $\sigma \in \mathrm{Gal}_K(L)$ si ha che la valutazione $v_L \circ \sigma$ è una valutazione su L quindi deve coincidere con v_L e quindi elementi coniugati hanno la stessa valutazione. □

Corollario 6.48. *Data L estensione di grado n di K allora $n = ef$ con e indice di ramificazione e f grado residuo.*

Dimostrazione. E' ovvio che $[L : K] = [B : A] = n$ perchè B è A-modulo libero. Anche ${}^{B}\!/_{PB}$ è ${}^{A}\!/_{PA}$ modulo libero di rango n. L'ideale PB si spezza come prodotto finito dell'unico ideale primo Q di B ($PB = Q^e$) vogliamo calcolare la dimensione di $\left[{}^{B}\!/_{PB} : {}^{A}\!/_{PA}\right] = n$ in un altro modo. Prendendo la catane di ideali

$$ {}^{B}\!/_{Q^e} \supset {}^{Q}\!/_{Q^e} \supset \cdots \supset {}^{Q^{e-1}}\!/_{Q^e} \supset 0 $$

Inoltre vale che ${}^{{}^{Q^i}\!/_{Q^e}}\!/_{{}^{Q^{i+1}}\!/_{Q^e}} \simeq {}^{Q^i}\!/_{Q^{i+1}} \simeq {}^{B}\!/_{Q}$ quindi

$$ n = \left[{}^{B}\!/_{PB} : {}^{A}\!/_{PA}\right] = e\left[{}^{B}\!/_{Q} : {}^{A}\!/_{PA}\right] = ef $$

□

Corollario 6.49. *Per ogni $x \in L$ si ha che $v_L(x) = \frac{1}{f} v_K\left(\mathrm{N}_{{}^{L}\!/_{K}}(x)\right)$ dove f è il grado residuo dell'estensione.*

Dimostrazione. Sempre distinguendo i casi se l'estensione è radicale e puramente inseparabile vale che se il polinomio minimo di x è $x^n - a$ allora $N(x) = a$. Si dimostra prendendo la base $\{x^i\}_{i<n}$ e scrivendo x_L nella base ottenendo la matrice compagna del polinomio minimo di x che ha determinante a. Vale quindi $v_L = \frac{1}{m} v_K(x^q) = \frac{1}{m} v_K(a) = \frac{1}{m} v_K(\mathrm{N}(x))$. Sia $w' = mw = v_K \circ \mathrm{N}_{{}^{L}\!/_{K}}$ vogliamo dimostrare che l'immagine di w' è $f\mathbb{Z}$ (cioè $m = f$). Per fare ciò si q il generatore dell'ideale massimale di B e per la definizione di indice di ramificazione e vale che $(\pi) = (q)^e$ quindi il minimo della valutazione w' è $w'(q) = \frac{1}{e} v_K(\mathrm{N}(\pi)) = \frac{n}{e} v_K(\pi) = \frac{n}{e} = f$.

Passiamo ora al caso in cui l'estensione sia di separabile. Prendiamo L la chiusura di Galois e vale che

$$ v_K\left(\mathrm{N}_{{}^{L}\!/_{K}}(x)\right) = \sum_{\sigma \in \mathrm{Gal}(L)} v_K(\sigma(x)) = |\mathrm{Gal}_K(L)|\, v_K(x) $$

dove abbiamo usato l'osservazione 4.37 per la norma e il corollario 6.47 per l'invarianza per coniugio. Dobbiamo dimostrare che $|\mathrm{Gal}_K(L)| = f$, si

osserva che per il teorema dell'elemento primitivo $L = K[\alpha]$ con α intero e con polinomio minimo monico $f \in A[x]$ quindi $|\mathrm{Gal}_K(L)| = [L : K] = \deg(f) = \deg(\bar{f}) = [l : k] = f$. □

6.5 Gruppo di Galois

Dimostreremo che il gruppo di Galois dell'estensione non ramificata di un campo locale corrisponde al gruppo di Galois di una corrispondente estensione del campo residuo e vicevera. Per fare ciò è necessario qualche lemma sulle radici dei polinomi, dunque enunciamo il lemma di Hensel.

Lemma 6.50 (di Hensel)**.** *Sia A anello di valutazione discreta completo, e $f \in A[x]$. Ogni radice semplice λ di $\bar{f} \in k[x]$ si solleva in modo unico a x radice di f in A.*

Dimostrazione. Dimostriamo innanzitutto l'unicità del sollevamento. Sia x radice allora $f(X) = (X - x)g(X)$ con $\bar{g}(\lambda) \neq 0$ (la radice λ è semplice). Se x' fosse un altra radice allora $0 = f(x') = (x' - x)g(x')$ ma poichè $g(\lambda) \neq 0$ allora $v(g(x')) = 0$ quindi $g(x')$ è invertibile e $x = x'$. Passiamo ora all'esistenza, vogliamo trovare una successione convergente x_n e $\overline{x_n} = \lambda$ tale che $f(x_n) \equiv 0 \mod \pi^n$ e il limite della successione è la radice cercata. Sia x_1 un qualsiasi elemento con proiezione λ allora $f(x_1) \equiv 0 \mod \pi$ e costruiamo per induzione la successione. Dato x_n come richiesto poniamo $x_{n+1} = x_n + h\pi^n$ e vale per la formula di Taylor $f(x_{n+1}) = f(x_n) + h\pi^n f'(x_n) + h^2\pi^{2n} f'(y)$. Riducendo modulo π^{n+1} si ottiene che

$$f(x_{n+1}) \equiv f(x_n) + h\pi^n f'(x_n) \mod \pi^{n+1}$$

Poiché per passo induttivo si ha che $f(x_n) \equiv 0 \mod \pi^n$ e che $f'(x_n) \in A^*$ allora basta scegliere

$$h = -\frac{f(x_n)}{\pi^n f'(x_n)}$$

La successione così creata è di Cauchy quindi converge a x radice cercata. □

Teorema 6.51. *Sia L un estensione non ramificata di un campo locale K, F un estensione di K, l'insieme degli K-omomorfismi di L in F è in corrispondenza biunivoca e canonica con l'insieme degli k-omomorfismi di l in f.*

Dimostrazione. Indichiamo con B e con C le chiusure integrali di A in L e in F, ovviamente si ha che $\mathrm{Hom}_K(L, F) = \mathrm{Hom}_A(B, C)$. Ci basta dimostrare che l'omomorfismo canonico di proiezione $\varphi : \mathrm{Hom}_A(B, C) \longrightarrow \mathrm{Hom}_k(l, f)$ è biunivoco. Esiste x in B tale che $B = A[x]$ con polinomio minimo p di x di grado $n = [L : K]$, quindi $\{x^i\}_{i<n}$ è base di B come A-modulo libero. Gli omomorfismi di B in C (e di l in f) corrispondono in modo biunivoco alle

radici di p in C (in f). Naturalmente ogni radice in C si proietta a radice in f, viceversa per il lemma di Hensel 6.50 ogni radice di $\bar{p}$ si solleva in modo unico a radice di f, quindi la corrispondenza è biunivoca. □

Corollario 6.52. *Sia l estensione separabile e finita di k allora esiste unica, a meno di isomorfismo, estensione non ramificata L di K corrispondente all'estensione l su k. Inoltre L su K è di Galois se e solo se lo è l su k e in questo caso vale* $\mathrm{Gal}_K(L) = \mathrm{Gal}_k(l)$

Dimostrazione. Per il teorema dell'elemento primitivo $l = k[\alpha]$ con polinomio minimo $\bar{p} \in k[x]$, sia p un qualunque sollevamento di $\bar{p}$ in $A[x]$, $B = {}^{A[x]}\!/_{(p)}$ anello di valutazione discreta e L il campo dei residui di B. Per il corollario 6.45, sapendo che $\bar{p}$ è separabile perché l è separabile, L è non ramificata su K. L'ultima informazione discende dal teorema precedente applicato nel caso $L = F$. □

Corollario 6.53. *Data F estensione di K, le estensioni L non ramificate $K \subset L \subset F$ sono in corrispondenza biunivoca con le sottoestensioni separabili l contenute in f e contenenti k. Inoltre esiste unica estensione massimale non ramificata contenuta in F.*

Dimostrazione. La mappa dalle estensioni non ramificate L in quelle separabili l è data dalla definizione di estensione non ramificata 6.41. La surietività e l'inettività sono conseguenza del corollario 6.52. L'esistenza e l'inicità dell'estensione massimale non ramificata è data dal teorema analogo valido per le estensioni separabili più la corrispondenza appena dimostrata. □

Teorema 6.54. *K campo locale, per ogni $n \in \mathbb{N}$ esiste unica estensione non ramificata di grado n generata da ω radice $q^n - 1$ primitiva dell'unità dove $q = |k|$ e si ha che $B = A[\omega]$. L'estensione è di Galois con gruppo ciclico generato da $x \mapsto x^q$.*

Dimostrazione. Poiché k ha unica estensione l di grado n ed l è separabile quindi per il corollario 6.52 esiste L estensione di K di grado n non ramificata. Dimostriamo che $K[\omega]$ è estensione separabile di grado n e quindi coincide con L. ω è radice del polinomio $g(x) = x^{q^n-1} - 1 \in A[x]$ e sia $\bar{g}$ la proiezione in $k[x]$ che è non ramificata perché k campo finito. Per il corollario 6.45 $K[\omega]$ è non ramificata inoltre poiché anche $\bar{\omega}$ è radice $q^n - 1$ dell'unità vale che:

$$[K[\omega] : K] = [k[\omega] : k] = n$$

Per il corollario 6.52 $\mathrm{Gal}_K(L) = \mathrm{Gal}_k(L) = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ generato da $\bar{\omega} \mapsto \bar{\omega}^q$ che corrisponde all'automorfismo di L su K (di Frobenius) che mappa $\omega \mapsto \omega^q$. □

Lemma 6.55. *Sia L estensione non ramificata di K allora la norma e la traccia di l in k sono suriettive.*

Dimostrazione. Dimostriamo che la norma è suriettiva, usando le convensioni che $|k| = q$ e ω radice $q^n - 1$ dell'unità in B e $\mathrm{Gal}_k(l) = \langle\sigma\rangle$ con $\sigma(\bar{\omega}^i) = \bar{\omega}^{qi}$. Calcoliamo la norma di un qualsiasi elemento in l che è della forma $\bar{\omega}^k$.

$$\mathrm{N}_{l/k}(\bar{\omega}^k) = \prod_{i=0}^{n-1} \bar{\omega}^{kq^i} = \bar{\omega}^{k\frac{q^n-1}{q-1}}$$

Quindi poichè $k \leq q^n - 1$ e $\mathrm{N}(\bar{\omega}^k) = 1$ se e solo se $q - 1|k$ si deduce che ci sono esattamente $\frac{q^n-1}{q-1}$ elementi con la stessa norma, quindi l'immagine di N ha esattamente $q - 1$ elementi ed è suriettiva su k.

Per dimostrare che la traccia è suriettiva dimostriamo una cosa più forte cioè se l estensione finita di k la traccia è suriettiva se e solo se l è separabile su k (che è nelle ipotesi del lemma). Se l non fosse separabile allora $[l : k]_i = p^m$ con m positivo e quindi per le proprietà della traccia si ha che $\mathrm{tr}(x) = p^m \sum_\sigma \sigma(x) = 0 \in k$. Viceversa se l è separabile su k esiste x tale che $0 \neq \sum_\sigma \sigma(x) = \mathrm{tr}(x)$ ma poiché la traccia è un applicazione da l in k k-lineare non nulla allora è suriettiva. □

Teorema 6.56. *Data estensione L di K non ramificata per ogni $\alpha \in K$ sono equivalenti:*

- *esiste $x \in L$ tale che $\mathrm{N}_{L/K}(x) = \alpha$.*
- $n = [L : K]|v_K(\alpha)$

Dimostrazione. Ricordando che il corollario 6.47 sia v_L l'estensione della valutazione v_K, per il corollario 6.49 vale che

$$v_K(\alpha) = v_K\left(N_{L/K}(x)\right) = nv_L(x) \equiv 0 \mod n$$

Viceversa, se $\alpha = 0$ è banalmente vero altrimenti per $\alpha \neq 0$ sia $v_K(\alpha) = nq$ e sia $x \in L$ tale che $v_L(x) = q$ allora $v(\alpha) = fq = fv_L(x) = v_K\left(\mathrm{N}_{L/K}(x)\right)$ da cui $\alpha = a\,\mathrm{N}_{L/K}(x)$ con a invertibile in A. Ci siamo ricondotti al caso $\alpha \in A^*$ per la corrispondenza tra i gruppi di Galois di L e di l (corollario 6.52) la traccia e la norma in L corrispondono a quelle in l cioè:

$$\overline{\mathrm{tr}_{L/K}(x)} = \mathrm{tr}_{l/k}(x) \quad e \quad \overline{\mathrm{N}_{L/K}(x)} = \mathrm{N}_{l/k}(x)$$

Sia la norma che la traccia sono suriettive in k per il lemma 6.55, cerchiamo x che soddisfi le ipotesi come limite di una successione. Costruiamo per induzione la successione x_n avente la proprietà $\mathrm{N}(x_n) \equiv \alpha \mod \pi^n$con x_1 tale che $\mathrm{N}(x_1) = \alpha \mod \pi$ che è possibile perché la norma è suriettiva. Dato x_n costruiamo $x_{n+1} = x_n + h\pi^n$ allora ponendo $y = \prod_{i\neq 0} \sigma^i(\alpha)$ si ottiene

$$\begin{aligned}(x_{n+1}) &= \prod_{i<n} \varphi(x_n + h\pi^n) \equiv \prod_{i<n} \varphi(x_n) + \pi \sum_{i<n} \sigma^i(y)\sigma(h) \equiv \\ &\equiv \mathrm{N}(x_n) + \pi\,\mathrm{tr}(yh) \mod \pi^{n+1}\end{aligned}$$

Per la suriettività della traccia si può scegliere h tale che $\mathrm{N}(x_{n+1}) \equiv \alpha \mod \pi^{n+1}$. La successione x_n è di Cauchy e converge a x con $\mathrm{N}(x) = \alpha$. $\square$

Capitolo 7

Il gruppo di Brauer di un campo locale

Consideriamo ora il caso di algebre su campi locali con valutazione $v : K^* \longrightarrow \mathbb{Z} \cup \{+\infty\}$. Se consideriamo un'algebra di divisione D si può estendere la valutazione sul campo a tutta l'algebra definendo la valutazione w nel seguente modo.

$$w(x) = \frac{1}{d} v\left(\mathrm{Nrd}_{D/K}(x)\right)$$

Dove d è l'unico intero positivo che rende suriettiva sugli interi la valutazione, inoltre ricordiamo la convenzione che $w(0) = +\infty$.

Osservazione 7.1. *La valutazione w gode delle seguenti proprietà:*

1. *E' un omomorfismo di gruppi.*
2. *Chiamando n la dimensione di D su K, la restrizione di w al campo K è un multiplo di v ($w = \frac{n}{d} v$).*
3. *Ha la proprietà che per ogni coppia di elementi x e y vale*

$$w(x + y) \geq \min\{w(x), w(y)\} \tag{7.1}$$

4. *La topologia indotta da w è la stessa di quella di D come spazio vettoriale di dimensione n^2 su K.*
5. *L'anello B degli interi di D è l'insieme degli elementi in D interi su A (con A l'anello degli interi in K).*

Dimostrazione. 1. Ricordando che la norma ridotta è un omomorfismo di gruppi $\mathrm{Nrd} : D^* \longrightarrow K^*$ e anche la valutazione $v : K^* \longrightarrow Z$ è un omomorfismo, la loro composizione è ancora un omomorfismo. Di conseguenza w è un omomorfismo.

2. Per le proprietà della norma vale che $\mathrm{Nrd}(k) = k^n$ quindi $w(k) = \frac{n}{d}v(k)$ per ogni $k \in K$.

3. Per ogni elemento $x \in D$ sia L un sottocampo massimale contenente x. Ricordando che D è un L spazio vettoriale di dimensione $n = [L : K]$, per le proprietà della norma vale che:

$$\mathrm{N}_{L/K}(x)^n = \mathrm{N}_{D/K}(x) = \mathrm{Nrd}_{D/K}(x)^n$$

Segue che la norma w ristretta a L è un multiplo scalare della norma v_L indotta dalla valutazione v. Per dimostrare la disuguaglianza 7.1 usiamo il fatto che w è un omomorfismo di gruppi e senza perdita di generalità possiamo supporre $y = 1$. Abbiamo quindi che

$$w(x+1) = cv_L(x+1) \geq c\min\{v_L(x), v_L(1)\} = \min\{w(x), w(1)\}$$

4. Abbiamo dimostrato che w è una valutazione quindi induce una norma su D che diventa K-spazio vettoriale normato. Per la completezza di K si ha che anche D è spazio vettoriale completo e, dato che D è algebra finita, la topologia prodotto coincide con la topologia indotta da w.

5. Come nella dimostrazione del punto 3 sia x in D e L campo massimale contenente x. Vale che $w(x) \geq 0$ se e solo se $v_L(x) \geq 0$ se e solo se x è intero su A .

□

Lemma 7.2. *Sia D un corpo centrale su un campo locale K (diverso da K) allora esiste un campo L contenuto in D che sia un'estensione propria e non ramificata di K.*

Dimostrazione. Ragioniamo per assurdo supponendo che ogni estensione di K contenuta in D sia ramificata. Per ogni estensione L si ha che il campo residuo l coincide col campo residuo k di K, altrimenti si avrebbe un estensione separabile propria di k che per il corollario 6.53 corrisponde a una sottoestensione propria e non ramificata di K. Sia π un elemento di D con valutazione pari a uno e b un intero in D. Chiamando L il campo generato su K da b e l il campo residuo. Per quanto detto sopra il campo l coincide con il campo k, quindi esiste un elemento a_0 in A tale che $\overline{b} = \overline{a_0}$. Leggendo l'uguaglianza in B si ottiene che $b = a_0 + \pi b_1$ per qualche altro intero b_1. Iterando il ragionamento si ottiene che

$$b = \sum_{n\in\mathbb{N}} a_n\pi^n$$

con gli a_n in $A \subset K(\pi)$, essendo $K(\pi)$ un sottospazio vettoriale di D è chiuso quindi ogni elemento b del corpo D è contenuto in $K(\pi)$ quindi il corpo è commutativo e in particolare coincide col suo centtro K. Ciò è assurdo. □

Teorema 7.3. *Per ogni corpo D centrale su un campo locale K esiste un sottocampo massimale non ramificato.*

Dimostrazione. Sia L un campo massimale tra quelli non ramificati, vogliamo far vedere che $C_D(L) = L$ che per il corollario 4.30 è equivalente alla tesi. Per il teorema del centralizzatore (4.29) $C_D(L)$ è un corpo con centro L; inoltre ogni estensione di L in $C_D(L)$ è ramificata perché L è massimale tra i campi non ramificati. Per il lemma 7.2 il corpo $C_D(L)$ deve coincidere col suo centro L, abbiamo ottenuto l'uguaglianza e quindi la tesi. □

Abbiamo ora tutti gli strumenti per costruire l'invariante di Hasse e calcolare esplicitamente il gruppo di Brauer di un campo locale.

Data una qualsiasi algebra semplice centrale su un campo locale K per il teorema di Wedderburn (3.36) è un algebra di matrici su un corpo D. Per il teorema appena dimostrato (7.3), il corpo D contiene un sottocampo massimale non ramificato L. L'algebra A sarà equivalente a una della forma (L, K, f) (per il teorema 5.5) con f un opportuno factor set. Inoltre ad ogni estensione non ramificata L di K corrisponde un estensione separabile l del campo residuo k e poiché k è finito l'estensione l è di Galois con gruppo ciclico. Per il teorema di corrispondenza (6.52) anche l'estensione L è di Galois con gruppo ciclico $\mathbb{Z}/n\mathbb{Z}$. E' importante notare che per i campi finiti esiste l'automorfismo di Frobenius che è un generatore canonico del gruppo di Galois e per il teorema 6.51 possiamo individuare un generatore canonico φ del gruppo $\mathrm{Gal}_K(L)$ corrispondente all'automorfismo di Frobenius. Per quanto detto nella sezione sulle algebre cicliche (5.15) ogni algebra su un campo locale è della forma (K_n, K, σ, a) con K_n sottocampo massimale non ramificato di D e unica estensione non ramificata di K di grado $n = \mathrm{ind}_K A$. Possiamo scegliere come generatore del gruppo ciclico l'automorfismo canonico φ grazie al corollario 5.16, infatti esiste un naturale s coprimo con n tale che $\sigma^s = \varphi$ e quindi $[(K_n, K, \sigma, a)] = [(K_n, K, \varphi, a^s)]$. Infine il corollario 5.19 caratterizza i valori di a per cui le algebre generate sono isomorfe. Nel nostro caso le due algebre (K_n, K, φ, a) e (K_n, K, φ, b) sono isomorfe se e solo se esiste un elemento c in K_n tale che $\mathrm{N}_{K_n/K}(c) = \frac{b}{a}$. Questa uguaglianza è equivalente (per il teorema 6.56) a $n \mid v(\frac{b}{a})$ cioè che le valutazioni di a e di b sono congrue modulo n. Questa ultima condizione ci permette di scegliere come rappresentante un'opportuna potenza del generatore π. Abbiamo dimostrato che ogni algebra su un campo locale è equivalente a una della forma

$$(K_n, K, \varphi, \pi^i)$$

per opportuni interi n e i con $0 \leq i < n$.

Possiamo definire l'invariante di Hasse di un algebra A nel seguente modo.

Definizione 7.4. Sia A un algebra su un campo locale K, abbiamo dimostrato che è equivalente a una della forma (K_n, K, φ, π^i). L'invariante di

Hasse della classe di A è l'elemento del gruppo $\mathbb{Q}/\mathbb{Z}$ dato da $\frac{i}{n}$ e denoteremo con

$$\operatorname{Inv} A = \frac{i}{n}$$

L'invariante è ben definito perché la costruzione descritta è unica, inoltre non dipende dalla classe di equivalenza dell'algebra perché dipende solo dal corpo relativo. Rimane da verificare che la funzione Inv è un isomorfismo di gruppi.

Teorema 7.5. *La funzione inversa dell'invariante di Hasse che manda la frazione $\frac{b}{a}$ in $[(K_a, K, \varphi, \pi^b)]$ è ben definita.*

Dimostrazione. Dato un elemento di $\mathbb{Q}/\mathbb{Z}$ e una sua scrittura $\frac{b}{a}$ vogliamo dimostrare che genera un algebra equivalente a quella generata da $\frac{s}{n}$ con $0 \leq s < n$, $(s, n) = 1$ e $\frac{b}{a} = \frac{s}{n}$. La tesi è equivalente a mostrare che

$$[(K_a, K, \varphi_a, \pi^b)] = [(K_n, K, \varphi_n, \pi^s)]$$

Sia l'intero d il massimo divisore di a e b, si ha che $a = dn$ e $b = d(s + kn)$ pe qualche intero k. Prendiamo in K_a il sottocampo K_n fissato dal sottogruppo $\langle \varphi_a^n \rangle$ di cardinalità d, il campo K_n è estensione non ramificata di K. L'omomorfismo suriettivo di proiezione manda il gruppo $\operatorname{Gal}_K K_a$ nel gruppo $\operatorname{Gal}_K K_n$ e il generatore canonico φ_a nel generatore canonico φ_n relativo alla sottoestensione. Per il teorema 5.20 l'algebra $[(K_a, K, \varphi_a, \pi^{d(s+kn)}]$ è equivalente all'algebra $[(K_n, K, \varphi_n, \pi^{s+nk})]$ che a sua volta è equivalente a $[(K_n, K, \varphi_n, \pi^s)]$ perché $n \mid (s + nk) - s$. □

Immediata conseguenza del teorema è che l'invariante è una funzione biunivoca. Dimostriamo ora che l'invariante di Hasse è un isomorfismo di gruppi.

Teorema 7.6. *Per un campo locale K l'invariante di Hasse è un isomorfismo di gruppi.*

Dimostrazione. Verifichiamo che l'unico elemento mandato nell'elemento neutro di $\mathbb{Q}/\mathbb{Z}$ è la classe di K. Si ha che $[K] = [(L, K, \varphi, 1)]$ quindi $\operatorname{Inv} K = \frac{0}{[L:K]} = 0$ ed è l'inico elemento nel nucleo dell'invariante perché la funzione è biunivoca. Verifichiamo ora che sia un omomorfismo di gruppi. Date due algebre della forma $(K_a, K, \varphi_a, \pi^b)$ e $(K_c, K, \varphi_c, \pi^d)$ sono equivalenti rispettivamente a $(K_{ac}, K, \varphi_{ac}, \pi^{bc})$ e a $(K_{ac}, K, \varphi_{ac}, \pi^{da})$. Quindi per il corollario 5.18 vale che

$$[(K_{ac}, K, \varphi_{ac}, \pi^{bc})][(K_{ac}, K, \varphi_{ac}, \pi^{da})] = [(K_{ac}, K, \varphi_{ac}, \pi^{bc+da})]$$

Da cui si ottiene che

$$\operatorname{Inv}([(K_a, K, \varphi_a, \pi^b)][(K_c, K, \varphi_c, \pi^d)]) = \operatorname{Inv}(K_{ac}, K, \varphi_{ac}, \pi^{bc+da}) =$$
$$= \frac{bc + ad}{ac} = \frac{b}{a} + \frac{d}{c} = \operatorname{Inv}[(K_a, K, \varphi_a, \pi^b)] + \operatorname{Inv}[(K_c, K, \varphi_c, \pi^d)]$$

Di conseguenza l'invariante di Hasse è un isomorfismo di gruppi. □

Abbiamo dimostrato che il gruppo di Brauer di un campo locale è il gruppo delle radici dell'unità.

$$\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$$

Bibliografia

[1] S. Bosch, *Algebra*, Heiderberg, Springer, 1992.

[2] I. B. Fesenko e S. V. Vostokov, *Local Fields and Their Extensions*, Providence, American Mathematical Society, 2002.

[3] I. N. Herstein, *Non Commutative Rings*, Menasha, The Mathematical Association of America, 1968.

[4] S. Lang, *Algebra*, New York, Springer, 2002.

[5] A. Frölich e M. J. Taylor, *Algebraic Number Theory*, Cambridge, Cambridge University Press, 1991.

[6] J. P. Serre, *Local Fields*, Paris, Springer, 1979.

[7] D. Rosso, *Il gruppo di Brauer di un campo locale*, 2007.

[8] I. Reiner, *Maximal Orders*, New York, Academic press, 1975.