Università degli Studi di Pisa
Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea in Matematica

Tesi di Laurea

Basi normali intere: risultati principali nel caso generale e sviluppi recenti nel caso abeliano

Candidata
Valentina Di Proietto

Relatore
Prof. Roberto Dvornicich

Controrelatore
Prof. ssa Ilaria Del Corso

Anno Accademico 2003/2004

Indice

Introduzione

Scopo di questa tesi è studiare il problema della base normale. Data un'estensione di campi L/K finita e di Galois con gruppo di Galois G, una base normale è una base di L come spazio vettoriale su K costituita da elementi coniugati; $\alpha \in L$ è un generatore della base normale se l'insieme $\{\sigma(\alpha)|\sigma \in G\}$ è una base di L/K. Per ogni estensione di campi finita e di Galois esiste sempre una base normale. Una condizione equivalente all'esistenza di una base normale è che L come $K[G]$-modulo sia libero di rango 1.

Sia L/K un'estensione di campi di numeri con gruppo di Galois G e siano $\mathcal{O}_L$ e $\mathcal{O}_K$ i rispettivi anelli degli interi. Il gruppo di Galois G agisce su $\mathcal{O}_L$, per cui ci si può chiedere che struttura abbia $\mathcal{O}_L$ come $\mathcal{O}_K[G]$-modulo. Dire che l'estensione L/K ha una base normale intera significa che $\mathcal{O}_L$ come $\mathcal{O}_K[G]$-modulo è libero di rango 1. Un problema ancora aperto è trovare una condizione necessaria e sufficiente affinché un'estensione di campi di numeri abbia una base normale intera.

Se L/K ha una base normale intera, allora $\mathcal{O}_L$ è libero come modulo su $\mathcal{O}_K$, cioè esiste un base intera relativa di $\mathcal{O}_L$ come $\mathcal{O}_K$-modulo. Se $\mathcal{O}_K$ è un anello a ideali principali, $\mathcal{O}_L$ ha una base intera relativa, mentre in generale non è detto che $\mathcal{O}_L$ sia libero su $\mathcal{O}_K$. Anche nel caso in cui $\mathcal{O}_K$ è PID l'esistenza di una base normale intera non è garantita: per esempio se $K = \mathbb{Q}$ ci sono estensioni senza base normale intera.

L'inizio degli studi sul problema dell' esistenza di una base normale intera risale alla fine del XIX secolo: infatti è presente già in *Zahlbericht* di Hilbert [Hi 1897]. Non si conosce ancora una risposta generale, ma nel corso degli anni sono stati fatti numerosi passi avanti. Una condizione necessaria per l'esistenza di una base normale intera è che l'estensione L/K sia tame [Sp 1916]; purtroppo non è una condizione sufficiente, si possono trovare esempi di estensioni tame senza base normale intera (per esempio si veda [Ka 1984]). Nel caso di estensioni di campi locali si può dire qualcosa in più: vale infatti che tutte le estensioni di Galois finite tame di un campo locale hanno una base normale intera, l'essere tame è in questo caso una condizione necessaria e sufficiente: è il teorema di Noether [No 1931] di cui verrà data, nel secondo capitolo, una dimostrazione di Kawamoto [Ka 1986].

Se $K = \mathbb{Q}$, una condizione necessaria e sufficiente è data, nel caso di estensioni abeliane, dal teorema di Hilbert-Speiser, che afferma che tutte le estensioni abeliane tame di $\mathbb{Q}$ hanno una base normale intera. Recentemente è

stato provato una sorta di viceversa: tra tutti i campi di numeri, $\mathbb{Q}$ è l'unico per cui vale che tutte le estensioni abeliane tame hanno una base normale intera [GrReRuSr 1999].

Né il teorema di Noether né quello di Hilbert-Speiser affrontano il caso di estensioni wild. Un passo avanti in questo senso è stato fatto da Leopoldt [Lo 1959], il quale, nel caso di $K = \mathbb{Q}$ e L abeliana su K, ha trovato un'ordine $\mathcal{A}_{L/K}$ contenuto in $K[G]$ per cui $\mathcal{O}_L$ è libero di rango 1 su $\mathcal{A}_{L/K}$. Lettl e Byott in [ByLe 1996] hanno generalizzato il risultato di Leopoldt al caso in cui K sia un campo ciclotomico e $L \supset K$ un'estensione abeliana di $\mathbb{Q}$. Se L e K soddisfano queste ipotesi si dimostra che l'essere tame per l'estensione L/K è una condizione equivalente all'esistenza di una base normale intera.

Nell'ultimo capitolo vengono analizzate le estensioni L/K che soddisfano le ipotesi del teorema di Byott e Lettl: l'idea è di "misurare" quanto è distante un'estensione di questo tipo dall'avere una base normale intera. Viene definito un indice, che vale 1 nel caso in cui si abbia una base normale intera, che non è altro che il numero di classi laterali di $\mathcal{O}_K[G]$ come sottogruppo di $\mathcal{A}_{L/K}$. Si dimostra che questo indice è finito e che si può calcolare come norma del determinante di un'opportuna matrice quadrata; nelle ultime pagine della tesi vengono fatti alcuni esempi di calcolo. In particolare viene analizzato il caso in cui $K = \mathbb{Q}(\zeta_q)$ e L è un'estensione abeliana di $\mathbb{Q}$, contenente K, con conduttore p^2q, dove p e q sono primi distinti ed entrambi diversi da 2: l'indice, per queste estensioni, coincide con $p^{(p-1)(q-1)}$. Un altro degli esempi che vengono studiati è il caso di $K = \mathbb{Q}(\zeta_q)$ e $L = \mathbb{Q}(\zeta_{q^2})$, dove q è un primo diverso da 2: in questo caso l'indice vale $q^{\frac{q(q-1)}{2}}$.

Desidero ringraziare il prof. Roberto Dvornicich che, oltre ad essere il relatore di questa tesi, mi ha introdotta allo studio della teoria dei numeri. Un ulteriore ringraziamento va al prof. Cornelius Greither dell'Università di Monaco per la gentilezza con cui ha risposto alle mie richieste di chiarimenti.

Capitolo 1

Strumenti

1.1 Anelli di interi

In questo capitolo enunceremo gli strumenti usati nei capitoli successivi, che costituiscono le basi della teoria dei numeri. Ometteremo le dimostrazioni, per le quali si rimanda a [Se 1995], [Na 1990], [Ma 1977] e [La 1970].

Definizione 1.1.1 *Siano A e B due anelli commutativi con identità, A un sottoanello di B, un elemento $\alpha \in B$ è detto intero su A se α è radice di un polinomio monico a coefficienti in A.*

Nel caso di $A = \mathbb{Z}$ e $B = \mathbb{Q}$, si dimostra che tutti e soli gli elementi che annullano polinomi monici a coefficienti in $\mathbb{Z}$ sono elementi di $\mathbb{Z}$. In teoria dei numeri si studia il caso $A = \mathbb{Z}$ e $B = L$, dove L è un campo di numeri, cioè un'estensione finita di $\mathbb{Q}$.
Dato un campo di numeri L, l'insieme degli elementi interi su $\mathbb{Z}$ è un anello che si chiama anello degli interi di L e che viene indicato con $\mathcal{O}_L$. Inoltre, considerando un'estensione di campi di numeri L/K, si verifica che l'anello degli interi di L, $\mathcal{O}_L$, si può definire anche come insieme degli elementi di L che annullano polinomi monici a coefficienti in $\mathcal{O}_K$.
L'anello degli interi di un campo di numeri ha una struttura molto importante, vale infatti:

Proposizione 1.1.2 *L'anello degli interi $\mathcal{O}_L$ di un campo di numeri L è un dominio di Dedekind. In particolare ogni ideale $I \neq 0$ di $\mathcal{O}_L$ si fattorizza in modo unico (a meno dell'ordine) come prodotto di ideali primi:*

$$I = \prod_i P_i^{a_i}$$

dove P_i sono gli ideali primi di $\mathcal{O}_L$ e a_i è diverso da zero al massimo per un numero finito di i.

Gli ideali primi di un anello degli interi, quindi, acquistano un' importanza fondamentale: la proposizione 1.1.2 dice infatti che per descrivere ogni ideale basta descivere gli ideali primi; in un dominio di Dedekind gli ideali primi svolgono la funzione dei primi in un dominio a fattorizazione unica. Se A è un dominio di Dedekind con campo dei quozienti K, si può considerare un altro tipo di ideali, gli ideali frazionari di A.

Definizione 1.1.3 *Un ideale frazionario di un dominio di Dedekind A è un sottoinsieme del campo dei quozienti della forma $I = \frac{1}{\alpha}J$, dove α è un elemento di A diverso da zero e J un ideale di A.*

Sia

$$G(K) = \{I \mid I \text{ è un ideale frazionario di A}\},$$

si può dotare $G(K)$ di un'operazione tale che $G(K)$ sia un gruppo abeliano:

$$\frac{1}{\alpha}I \cdot \frac{1}{\beta}J = \frac{1}{\alpha\beta}(I \cdot J)$$

Il sottoinsieme di $G(K)$

$$H = \{I \mid I \text{ è un ideale frazionario principale}\}$$

è un sottogruppo di $G(K)$; si può così definire il quoziente $G(K)/H(K)$ che è detto gruppo delle classi di ideali. Ovviamente se A è ad ideali principali $G(K)/H(K)$ è costituito dalla sola identità.
Sia $\mathcal{O}_L$ l'anello degli interi di un campo di numeri L, $\mathcal{O}_L$ è uno $\mathbb{Z}$-modulo. La sua struttura come $\mathbb{Z}$-modulo è molto semplice.

Teorema 1.1.4 *Sia L un campo di numeri, $\mathcal{O}_L$ l'anello degli interi, allora $\mathcal{O}_L$ è uno $\mathbb{Z}$-modulo libero di rango $[L : \mathbb{Q}]$.*

In alcuni casi la base di $\mathcal{O}_L$ come $\mathbb{Z}$-modulo è particolarmente intuitiva: è una base i cui elementi sono potenze di un generatore e si chiama base di potenze; è il caso per esempio dell'anello degli interi di $\mathbb{Q}(\zeta_m)$, $\mathbb{Z}[\zeta_m]$, con ζ_m radice m-esima dell'unità.
Anche per le estensioni quadratiche di $\mathbb{Q}$ esiste una base di potenze: infatti una base dell'anello degli interi di $\mathbb{Q}(\sqrt{m})$ è data da $\{1, \sqrt{m}\}$ se $m \equiv 2, 3 \pmod 4$, da $\{1, (1 + \sqrt{m})/2\}$ se $m \equiv 1 \pmod 4$.

Supponiamo che $K \subset L$, entrambi campi di numeri, allora $\mathcal{O}_L$ è un $\mathcal{O}_K$-modulo, in generale non è vero che $\mathcal{O}_L$ è libero di rango $[L : K]$ come $\mathcal{O}_K$-modulo.

1.2 Estensione di primi

Sia L/K un'estensione di campi di numeri (nel corso della tesi chiameremo le estensioni di campi di numeri anche estensioni globali), consideriamo la funzione iniettiva $i_{L/K} : G(K) \to G(L)$ definita da

$$i_{L/K}(I) = I\mathcal{O}_L$$

dove I appartiene a $G(K)$; $i_{L/K}$ manda ideali interi di $\mathcal{O}_K$ in ideali interi di $\mathcal{O}_L$. Se P è un ideale primo di $\mathcal{O}_K$, allora

$$i_{L/K}(P) = P\mathcal{O}_L = Q_1^{e_1}...Q_r^{e_r}, \tag{1.1}$$

dove $Q_1...Q_r$ sono ideali primi di $\mathcal{O}_L$ e $e_i \in \mathbb{N}$. Si dice che gli ideali Q_i stanno sopra a P e l'esponente e_i è chiamato l'indice di ramificazione di Q_i su P ed è indicato con $e_{L/K}(Q_i|P)$.
Ad ogni primo Q_i che sta sopra a P è associato un altro numero naturale $f_{L/K}(Q_i|P) = f_i$, che è la dimensione di $\mathcal{O}_L/Q_i$ come spazio vettoriale su $\mathcal{O}_K/P$. Ricordiamo che $\mathcal{O}_L$ e $\mathcal{O}_K$ sono domini di Dedekind, quindi gli ideali primi sono anche massimali, per cui $\mathcal{O}_L/Q_i$ e $\mathcal{O}_K/P$ sono campi chiamati campi residui. In particolare sono campi finiti, estensioni di $\mathbb{Z}/p\mathbb{Z}$. L'indice di ramificazione e il grado di inerzia sono moltiplicativi in torre.

Proposizione 1.2.1 *Siano $K \subset F \subset L$ campi di numeri, P un primo di $\mathcal{O}_K$, Q un primo di $\mathcal{O}_F$ che sta sopra P, B un primo di $\mathcal{O}_L$ che sta sopra P; allora*

$$e_{L/K}(B|P) = e_{F/K}(Q|P)e_{L/F}(B|Q)$$
$$f_{L/K}(B|P) = f_{F/K}(Q|P)f_{L/F}(B|Q).$$

Si dice che un ideale primo P di $\mathcal{O}_K$ ramifica in L/K se per almeno un i $e_{L/K}(Q_i|P) > 1$, non ramifica altrimenti. Inoltre P è ramificato tamely, o ha una ramificazione moderata, se per ogni Q_i che sta sopra a P vale che $e_{L/K}(Q_i|P)$ è primo con la caratteristica del campo residuo $\mathcal{O}_L/Q_i$. Si dice inoltre che P è ramificato wildly, o ha una ramificazione selvaggia, se non è ramificato tamely. L'estensione L/K è detta tame se tutti i primi di $\mathcal{O}_K$ lo sono.

Teorema 1.2.2 *Sia L/K un' estensione di campi di numeri di grado n, allora i primi Q_i che compaiono in (1.1) sono gli unici ideali di $\mathcal{O}_L$ per cui vale che $Q_i \cap \mathcal{O}_K = P$, inoltre vale che*

$$n = \sum_{i=1}^{r} e_i f_i,$$

dove $e_i = e_{L/K}(Q_i|P)$ e $f_i = f_{L/K}(Q_i|P)$.

A priori non è semplice capire come si fattorizza un primo di $\mathcal{O}_K$ quando viene esteso ad $\mathcal{O}_L$. Uno strumento molto utile è il teorema di Kummer:

Teorema 1.2.3 *Sia $L = K(\alpha)$ con $\alpha \in \mathcal{O}_L$, $m = [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$ e P un ideale primo di $\mathcal{O}_K$ tale che $P \cap \mathbb{Z} = p$, con $p \nmid m$. Se $g(x)$ è il polinomio minimo di α su K e se considero la fattorizzazione di $\overline{g(x)}$ in $\mathcal{O}_K/P[x]$*

$$\overline{g(x)} = \overline{g_1}^{e_1}(x)...\overline{g_r}^{e_r}(x),$$

allora $P\mathcal{O}_K = Q_1^{e_1}...Q_r^{e_r}$, dove $Q_i = (P, g_i(\alpha))$ e g_i è un rappresentante in $\mathcal{O}_K[x]$ di $\overline{g_i(x)}$. Inoltre il grado di inerzia $f_{L/K}(Q_i|P)$ per ogni primo Q_i coincide col grado del polinomio $g_i(x)$.

Se L/K è un'estensione di Galois con $G = Gal(L/K)$ la situazione descritta sopra si può percisare meglio. In questo caso, infatti, G agisce transitivamente sui primi sopra P, lo stabilizzatore del primo Q sopra P secondo l'azione di G si chiama gruppo di decomposizione e si indica con $D(Q|P) = \{\sigma \in G \mid \sigma(Q) = Q\}$; il teorema 1.2.2 diventa:

Teorema 1.2.4 *Sia L/K un' estensione di campi di numeri di grado n, con gruppo di Galois $G = Gal(L/K)$, P un primo di K, allora i primi Q_i che compaiono in (1.1) sono gli unici ideali di $\mathcal{O}_L$ per cui vale che $Q_i \cap \mathcal{O}_K = P$, inoltre l'indice di ramificazione e il grado di inerzia di Q_i su P non dipendono da i, ma solo da P, per cui, se $e = e_{L/K}(P)$ e $f = f_{L/K}(P)$, vale che*

$$n = efr.$$

La proposizione seguente è un esempio di applicazione del teorema 1.2.3 al caso di un'estensione di Galois.

Proposizione 1.2.5 *Sia $L = \mathbb{Q}(\zeta_m)$ un campo ciclotomico, ζ_m una radice m-esima dell'unità, cosideriamo l'estensione di Galois $L/\mathbb{Q}$, supponiamo che $m = p^k n$, $p \nmid n$, allora $e_{L/K}(p) = \varphi(p^k)$ ed $f_{L/K}(p)$ è l'ordine moltiplicativo di $p \pmod m$. Invece se q è un primo che non divide m, $e_{L/K}(q) = 1$ ed $f_{L/K}(q)$ è l'ordine moltiplicativo di $q \pmod m$.*

1.3 Traccia e norma

Deinizione 1.3.1 *Se L/K è un'estensione di campi di numeri di grado n, con $\sigma_1, ..., \sigma_n$ gli omomorfismi distinti che vanno da L nella chiusura algebrica di K, che sono l'identità ristretti a K, allora si definiscono*

$$\begin{array}{ll} \mathrm{Tr}_{L/K} : L \to K & \mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x) \\ \mathrm{N}_{L/K} : L \to K & \mathrm{N}_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x). \end{array}$$

Nel caso in cui l'estensione L/K sia di Galois è facile vedere che $\mathrm{Tr}_{L/K}$ e $\mathrm{N}_{L/K}$ hanno immagine effettivamente in K, nel caso di estensione non di Galois basta prendere la chiusura normale. Traccia e norma sono due strumenti fondamentali in teoria dei numeri, vediamone le proprietà.

Proposizione 1.3.2 *Con le stesse ipotesi della definizione 1.3.1 si ha*

$$\begin{array}{l} \mathrm{Tr}_{L/K} \text{ è un omomorfismo di } (L,+) \text{ in } (K,+) \\ \mathrm{N}_{\mathrm{L/K}} \text{ è un omomorfismo di } (L^*,\cdot) \text{ in } (K^*,\cdot). \end{array}$$

Proposizione 1.3.3 *Siano $K \subset F \subset L$ campi di numeri, allora*

$$\begin{array}{l} \mathrm{Tr}_{L/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{L/F} \\ \mathrm{N}_{L/K} = \mathrm{N}_{L/K} \circ \mathrm{Tr}_{L/F}. \end{array}$$

Si può definire la norma anche di un ideale a partire dagli ideali primi ed estenderla, grazie alla fattorizzazione unica, a tutti gli ideali. Sia Q un ideale primo di $\mathcal{O}_L$ che sta sopra P, ideale primo di $\mathcal{O}_K$, e $f = [\mathcal{O}_L/Q : \mathcal{O}_K/P]$, allora

$$\mathrm{N}_{L/K}(Q) = P^f.$$

Nel caso in cui $K = \mathbb{Q}$ la norma di un ideale I di $\mathcal{O}_L$ coincide con il numero di elementi del quoziente $\mathcal{O}_L/I$. Basta vederlo nel caso degli ideali primi. Si considera p un ideale primo di $\mathbb{Z}$ e un ideale primo P di $\mathcal{O}_L$ che sta sopra p, allora

$$\mathrm{N}_{L/K}(P) = p^f$$

con $f = [\mathcal{O}_L/P : \mathbb{Z}/p\mathbb{Z}]$ e p^f il numero di elementi di $\mathcal{O}_L/P$.

1.4 Discriminante e differente

Definizione 1.4.1 *Sia L/K un'estensione di campi di numeri di grado n, si dice differente di L/K l'ideale intero $D_{L/K} = (\mathcal{O}_L^{'})^{-1}$, dove*

$$\mathcal{O}_L^{'} = \{x \in L \,|\, \mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K\}.$$

Le proprierà importanti del differente sono moltissime, sono qui citate solo quelle che verranno usate.

Proposizione 1.4.2 *(i) Se I è un ideale (possibilmente anche frazionario) di $\mathcal{O}_K$, allora*

$$\mathrm{Tr}_{L/K}(J) \subset I \quad \Leftrightarrow \quad J \subset I{D_{L/K}}^{-1},$$

per ogni ideale J, eventualmente anche frazionario, di $\mathcal{O}_L$.

(ii) Se $K \subset F \subset L$ sono campi di numeri, allora $D_{L/K} = D_{L/F}D_{F/K}$.

(iii) Se Q è un ideale primo di $\mathcal{O}_L$ che sta sopra P, ideale primo di $\mathcal{O}_K$, e $P\mathcal{O}_L = Q^eA$ con $Q \nmid A$, allora Q^{e-1} divide il differente $D_{L/K}$. Inoltre se l'indice di ramificazione di Q su P è primo con la norma da K in $\mathbb{Q}$ di P, allora Q^e non divide il differente $D_{L/K}$. Se Q è ramificato wildly, invece, Q^e divide il differente.

(iv) Se K_1 e K_2 sono due estensioni linarmente disgiunte di K ($K_1 \cap K_2 = K$), e se $(D_{K_1/K}, D_{K_2/K}) = 1$, allora $\mathcal{O}_{K_1K_2} = \mathcal{O}_{K_1} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_2}$.

Sia L/K un'estensione di campi di grado n e separabile, sia $\{\alpha_1, ..., \alpha_n\}$ una n-upla di elementi di L, definiamo il discriminante

$$\mathrm{disc_{L/K}}(\alpha_1, ..., \alpha_n) = \det(\sigma_i\alpha_j)^2, \tag{1.2}$$

con σ_i immersioni distinte di L nella chiusura algebrica di K. La prima proprietà che useremo del discriminante può già essere enunciata.

Proposizione 1.4.3 *$disc_{L/K}(\alpha_1, ..., \alpha_n) = 0$ se e solo se $\alpha_1, ..., \alpha_n$ sono linearmente dipendenti su K.*

Se prendiamo un'altra n-upla di elementi di L si vede che i discriminanti differiscono per il quardato del determinante della matrice dell'applicazione che manda una n-upla nell'altra. Torniamo ora a considerare L/K un'estensione di campi di numeri di grado n e, come sempre, $\mathcal{O}_L$ ed $\mathcal{O}_K$ gli anelli degli interi. Se $\mathcal{O}_L$ è un $\mathcal{O}_K$-modulo libero di rango n si può definire il discriminante di $\mathcal{O}_L$ scegliendo come n-upla una base di $\mathcal{O}_L$ su $\mathcal{O}_K$; vale che due n-uple di elementi generano lo stesso modulo se i discriminanti differiscono per un'unità di $\mathcal{O}_K$. Nel caso di $K = \mathbb{Q}$, siccome gli invertibili di $\mathcal{O}_K$ sono ± 1, il discriminante non dipende dalla scelta della base di $\mathcal{O}_L$. Consideriamo ora $K = \mathbb{Q}$ e $L = \mathbb{Q}(\zeta_q)$ con $q \in \mathbb{Z}$ primo e diverso da 2; una base di $\mathcal{O}_L$ su $\mathbb{Z}$ è data da $\{1, \zeta_q, ..., \zeta_q^{q-2}\}$, e $\mathrm{disc}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(1, \zeta_q, ..., \zeta_q^{q-2}) = \pm q^{q-2}$ e vale il $+$ se e solo se $q \equiv 1 \pmod 4$. Sempre nel caso di $K = \mathbb{Q}$, ma $L = \mathbb{Q}(\sqrt{m})$ se $m \equiv 2, 3 \pmod 4$, allora $\mathrm{disc}_{\mathbb{Q}(\sqrt{m}/\mathbb{Q})} = 4m$; invece se $m \equiv 1 \pmod 4$, allora $\mathrm{disc}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}} = m$.
Nel caso generale si definisce il discriminante di $\mathcal{O}_L$ come l'$\mathcal{O}_K$-modulo generato dai discriminanti $\mathrm{disc}_{L/K}(u_1, ..., u_n)$, dove gli u_i variano fra gli elementi di $\mathcal{O}_L$ linearmente indipendenti su K.

A questo punto possiamo enunciare la relazione che c'è tra discriminante e differente.

Proposizione 1.4.4 *Discriminante e differente sono collegati dalla formula seguente:*

$$\mathrm{disc}_{L/K} = \mathrm{N}_{L/K}(D_{L/K}),$$

dove $\mathrm{N}_{L/K}$ è la norma di ideali.

1.5 Valori assoluti su un campo

Definizione 1.5.1 *Un valore assoluto su un campo K è una funzione*

$$|\ |_v : K \to \mathbb{R}_+$$

tale che soddisfi:

(i) $|x|_v \geq 0$ *e* $|x|_v = 0 \Leftrightarrow x = 0$,

(ii) $|xy|_v = |x|_v |y|_v\ \forall x, y \in K$,

(iii a) $|x + y|_v \leq |x|_v + |y|_v\ \forall x, y \in K$,

(iii b) $|x + y|_v \leq \max(|x|_v, |y|_v)$.

Il valore assoluto si dice non archimedeo o valutazione se soddisfa (iii b).

Un valore assoluto definisce una topologia sul campo; la distanza è data da

$$d(x, y) = |x - y|_v.$$

Due valori assoluti si dicono equivalenti se inducono la stessa topologia.
Su $\mathbb{Q}$ si possono definire valori assoluti in almeno due modi:

(i) $x \in \mathbb{Q}$, $|x|_\infty = |x|$ è il valore assoluto ordinario che è archimedeo;

(ii) $x \in \mathbb{Q}$, $x = p^k \frac{m}{n}$, $k \in \mathbb{Z}$ e $(mn, p) = 1$, $|x|_p = e^{-k}$, è il valore assoluto p-adico, non archimedeo.

In realtà per $\mathbb{Q}$ non ci sono altre possibilità, vale infatti:

Teorema di Ostrowsky 1.5.2 *A meno di equivalenza gli unici valori assoluti non banali su* $\mathbb{Q}$ *sono* $|\ |_\infty$ *e* $|\ |_p$.

Quindi i valori assoluti non archimedei sono in corrispondenza biunivoca con i primi di $\mathbb{Z}$. Nel caso di valore assoluto non archimedeo è più comodo adottare la notazione additiva, cioè definire

$$v(x) := -\log |x|_v.$$

Gli assiomi della def 1.5.1 diventano

(i) $v(x) \in \mathbb{R}$, $v(x) = \infty \Leftrightarrow x = 0$,

(ii) $v(x + y) = v(x) + v(y)$,

(iii b) $v(x + y) \geq \min\{v(x), v(y)\}$.

Assumiamo che v sia non archimedeo, allora l'insieme

$$\mathcal{O}_v := \{x \in K |\, v(x) \geq 0\}$$

è un sottoanello di K, in particolare è un anello di valutazione di K. Inoltre

$$\mathcal{M}_v := \{x |\, v(x) > 0\}$$

è un ideale di $\mathcal{O}_v$ costituito dagli elementi di $\mathcal{O}_v$ che non sono unità ed è l'unico ideale massimale di $\mathcal{O}_v$, che quindi è un anello locale.
Nel caso di $K = \mathbb{Q}$ e v il valore assoluto p-adico, $\mathcal{O}_v$ viene indicato con $\mathbb{Z}_{(p)}$ e coincide con $\mathbb{Z}$ localizzato al primo p.

Avendo messo una topologia su un campo, ha senso la definizione seguente.

Definizione 1.5.3 *Un campo* K *è completo rispetto ad un valore assoluto se ogni successione di Cauchy ha limite in* K.

Dato un campo K e un valore assoluto $|\ |_v$, in generale K non sarà completo; si può però completare e il completamento è unico a meno di isometria.

Teorema 1.5.4 *Sia* K *un campo e* $|\ |$ *un valore assoluto su* K*, allora esiste un unico (a meno di isometria) campo* $\widehat{K}$ *chiamato il completamento di* K *rispetto a* $|\ |$*, tale che* $\widehat{K}$ *è completo rispetto a un valore assoluto che estende* $|\ |$ *e* K *è denso in* $\widehat{K}$.

Per il valore assoluto p-adico, il completamento di $\mathbb{Q}$ è il campo $\mathbb{Q}_p$. L'anello di valutazione di $\mathbb{Q}_p$ si indica con $\mathbb{Z}_p$ che è detto l'anello degli interi p-adici e coincide con la chiusura topologica di $\mathbb{Z}$ in $\mathbb{Q}_p$.

1.6 Valori assoluti su campi di numeri

Come per $\mathbb{Q}$ i valori assoluti non archimedei corrispondono ai primi di $\mathbb{Z}$, così vale per un campo di numeri e il suo anello degli interi, si ha infatti:

Teorema 1.6.1 *Sia L un campo di numeri di grado n su $\mathbb{Q}$, sia v una valutazione discreta (cioè tale che il suo gruppo dei valori sia discreto), allora esiste un primo P dell'anello degli interi $\mathcal{O}_L$ tale che $v(x) = n(x)$, dove $n(x)$ è l'esponente a cui compare il primo P nella fattorizzazione dell'ideale generato da x. Viceversa ogni primo P dell'anello degli interi $\mathcal{O}_L$ definisce in questo modo una valutazione su K che è discreta.*

Quindi ogni primo di un campo di numeri induce una valutazione discreta sul campo, nel caso di valutazione discreta l'anello $\mathcal{O}_v$ è un anello ad ideali principali e $\mathcal{M}_v$ l'unico ideale primo di $\mathcal{O}_v$. Il completamento di un campo di numeri L rispetto alla valutazione indotta da un primo Q dell'anello degli interi $\mathcal{O}_L$ è un campo ed è indicato in genere con L_Q; inoltre l'anello $\mathcal{O}_{L_Q} = \{x \in L_Q | \, v(x) \geq 0\}$, che è la chiusura di $\mathcal{O}_L$ in L_Q, è un anello ad ideali principali con un unico ideale primo, la chiusura di $\mathcal{M}_v$. L'anello $\mathcal{O}_{L_Q}$ è chiamato anello degli interi di L_Q; nel caso di $L = \mathbb{Q}$, l'anello degli interi di $\mathbb{Q}_p$ è $\mathbb{Z}_p$, definito alla fine del paragrafo precedente.

Se L è un campo di numeri contenente K e P un ideale primo di $\mathcal{O}_K$, indicheremo

$$L \otimes_K K_P \cong \prod_{Q_i | P} L_{Q_i}$$

con L_P che non è un campo, ma un prodotto di campi.

Per l'anello degli interi vale una formula analoga:

$$\mathcal{O}_{L_P} = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K_P} \cong \prod_{Q_i | P} \mathcal{O}_{L_{Q_i}}. \tag{1.3}$$

Per le dimostrazioni si veda [FrTa 1991].

1.7 Estensioni di p-adici

Le estensioni finite di campi di $\mathbb{Q}_p$ si chiamano campi p-adici e sono un esempio di campi locali; per gli argomenti trattati in questa tesi campi locali e campi p-adici saranno sinonimi. Siano K e L campi p-adici, tali che $K \subset L$, e $\mathcal{O}_K$ e $\mathcal{O}_L$ i rispettivi anelli degli interi e P e Q gli ideali primi (che sappiamo essere unici perché le valutazioni sono discrete). Gli anelli degli interi di campi p-adici sono domini di Dedekind, per cui la fattorizzazione unica degli ideali; sono anche anelli con un solo ideale primo, per cui ogni ideale di un anello degli interi di un campo p-adico è potenza opportuna di questo primo.
I campi $\mathcal{O}_L/Q$ e $\mathcal{O}_K/P$ si chiamano campi residui e sono campi finiti come nel caso di estensioni di campi di numeri.

Nel caso di campi p-adici la struttura di $\mathcal{O}_L$ come $\mathcal{O}_K$-modulo è molto più semplice che nel caso di campi di numeri: si dimostra infatti che esiste sempre un elemento $\alpha \in \mathcal{O}_L$ che genera $\mathcal{O}_L$ come $\mathcal{O}_K$-modulo.

Definizione 1.7.1 *Se P è l'ideale primo di $\mathcal{O}_K$ e Q l'ideale primo di $\mathcal{O}_L$, allora $P\mathcal{O}_L = Q^e$ ed $e_{L/K}$ è detto l'indice di ramificazione di L su K. Si dice grado di inerzia di L su K il numero $f_{L/K} = [\mathcal{O}_L/Q : \mathcal{O}_K/P]$, cioè il grado dell'estensione dei campi residui.*

Sono le stesse definizioni del caso di campi di numeri, solo che nel caso dei p-adici l'anello degli interi ha un solo ideale primo, per cui l'indice di ramificazione e il grado di inerzia non dipendono dalla scelta del primo. Anche nel caso locale il grado dell'estensione si può esprimere in termini dell'indice di ramificazione e del grado di inerzia.

Proposizione 1.7.2 *Sia L/K un'estensione di campi p-adici di grado n, siano e ed f rispettivamente l'indice di ramificazione ed il grado di inerzia, allora*

$$n = ef.$$

Come nel caso di campi di numeri l'indice di ramificazione e il grado di inerzia sono moltiplicativi nelle torri di estensioni .

Proposizione 1.7.3 *Siano $K \subset F \subset L$ campi p-adici, allora*

$$\begin{aligned} e_{L/K} &= e_{F/K} e_{L/F} \\ f_{L/K} &= f_{F/K} f_{L/F}. \end{aligned}$$

1.8 Estensioni non ramificate

Definizione 1.8.1 *Un' estensione di campi p-adici L/K si dice non ramificata se $e_{L/K} = 1$.*

Le estensioni non ramificate si riescono a caratterizzare nel modo seguente

Teorema 1.8.2 *(i) Se $K \subset L$ è non ramificata, con P e Q rispettivamente gli ideali primi e $\mathcal{O}_L/Q = \mathcal{O}_K/P(\overline{\alpha})$, dove $\alpha \in \mathcal{O}_L$, allora $L = K(\alpha)$ e il polinomio minimo f di α su K è tale che $\overline{f(x)} \in \mathcal{O}_K/P[x]$ è irriducibile.*

(ii) Se $L = K(\alpha)$, con α intero, e $g(x)$ è il polinomio minimo di α su K tale che $\overline{g(x)} \in \mathcal{O}_K/P[x]$ non ha radici multiple, allora L/K è non ramificata e $\mathcal{O}_L/Q = \mathcal{O}_K/P(\overline{\alpha})$.

Si dimostra che le estensioni non ramificate di un campo p-adico K sono in corrispondenza biunivoca con le estensioni del campo residuo $\mathcal{O}_K/P$ e grazie a questa corrispondenza si ha che sono estensioni di Galois, con gruppo di Galois isomorfo al gruppo di Galois dell'estensione di campi residui corrispondente, e che in particolare sono estensioni cicliche.

Teorema 1.8.3 *Esiste esattamente un' estensione non ramificata di grado n di un campo p-adico K.*

1.9 Estensioni totalmente ramificate

Definizione 1.9.1 *Siano $K \subset L$ campi p-adici, si dice che L/K è totalmente ramificata se $[L : K] = e_{L/K}$, cioè $f_{L/K} = 1$.*

Anche le estensioni totalmente ramificate si riescono a caratterizzare.

Teorema 1.9.2 *Sia L/K un'estensione di campi p-adici, siano P e Q, come sempre gli ideali primi, con $(\pi) = P$ e $(\Pi) = Q$, $P\mathcal{O}_L = Q^e$, allora*

(i) se $K \subset L$ è totalmente ramificata, Π soddisfa un'equazione di "Eisenstein" $x^e + a_{e-1}x^{e-1} + ... + a_0 = 0$, dove $a_i \equiv 0 \pmod{P}$ e $a_0 \not\equiv 0 \pmod{P^2}$;

(ii) l'equazione precedente è irriducibile e, se α è una radice, allora $K(\alpha)/K$ è totalmente ramificata di grado e.

In realtà ci servirà la caratterizzazione delle estensioni totalmente ramificate tame.

Definizione 1.9.3 *Siano $K \subset L$ campi p-adici, P e Q gli ideali primi ed $e_{L/K}$ l'indice di ramificazione, allora si dice che L/K è tame o moderata se $e_{L/K}$ è primo con la caratteristica del campo residuo $\mathcal{O}_K/P$. Se $e_{L/K}$ non è primo con la caratteristica del campo residuo, l'estensione si dice wild o selvaggia.*

Per le estensioni tame il teorema 1.9.2 diventa:

Teorema 1.9.4 *(i) Se $K \subset L$ è totalmente ramificata e tame, esiste Π in L che soddisfa $x^e - a\pi = 0$, con $a \in \mathcal{O}_K^*$, $(\pi) = P$, $(\Pi) = Q$.*

(ii) Se $a \in \mathcal{O}_K$, $p \nmid e$, allora ogni radice dell'equazione $x^e - a$ genera un'estensione tame, che è totalmente ramificata se $(a) = P^b$, con $(b, p) = 1$.

Sappiamo descrivere alcuni tipi di estensioni di p-adici; in realtà sappiamo molto di più, poiché componendo le estensioni che abbiamo descritto troviamo tutte le estensioni possibili.

Teorema 1.9.5 *Sia L/K un'estensione di campi p-adici di grado $n = ef$, sia $e = p^a e_1$ con $(p, e_1) = 1$, allora esistono N e T estensioni di K tali che*

$$K \subset N \subset T \subset L,$$

con N/K non ramificata di grado f, T/N tame totalmente ramificata di grado e_1, L/T wild totalmente ramificata di grado p^a.

1.10 Locale-globale

I campi p-adici sono uno strumento utilissimo per risolvere problemi nelle estensioni di campi di numeri. Data un'estensione di campi di numeri L/K, dato un primo P di $\mathcal{O}_K$ e primi di $Q_1...Q_r$ di $\mathcal{O}_L$ sopra P, si considerino i campi p-adici $L_{Q_1}, ..., L_{Q_r}, K_P$.

Teorema 1.10.1 *Con le ipotesi suddette vale che*

(i) $[L_{Q_i} : K_P] = e_{L/K}(Q_i|P) f_{L/K}(Q_i|P)$

(ii) Se $\overline{P}$ *e* $\overline{Q_i}$ *sono rispettivamente gli ideali primi di* $\mathcal{O}_{K_P}$ *e* $\mathcal{O}_{L_{Q_i}}$*, allora* $e_{L_{Q_i}/K_P}(\overline{Q_i}|\overline{P}) = e_{L/K}(Q_i/P)$*,* $f_{L_{Q_i}/K_P}(\overline{Q_i}|\overline{P}) = f_{L/K}(Q_i/P)$*.*

Vari strumenti che si usano in teoria dei numeri sono definiti sia nel caso di estensioni di campi di numeri sia nel caso di estensioni di campi p-adici e ci sono relazioni esplicite tra le due definizioni, come abbiamo visto per l'indice di ramificazione ed il grado di inerzia. Per esempio la definizione di norma, sia di un elemento che di un ideale, di traccia e di differente nel caso di estensioni di campi p-adici sono le stesse che nel caso di estensioni di campi di numeri e valgono le relazioni seguenti:

Proposizione 1.10.2 *(i) Se* $\alpha \in L$

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{r} \mathrm{N}_{L_{Q_i}/K_P}(\alpha),$$

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{r} \mathrm{Tr}_{L_{Q_i}/K_P}(\alpha).$$

(ii) Siano $D_{L/K}$ *e* $D_{L_{Q_i}/K_P}$ *rispettivamente il differente dell'estensione di campi di numeri* L/K *e quello dell'estensione p-adica* L_{Q_i}/K_P*, allora*

$$D_{L/K}\mathcal{O}_{L_{Q_i}} = D_{L_{Q_i}/K_P}.$$

Inoltre

$$D_{L/K} = \prod_{Q} (D_{L_Q/K_P} \cap \mathcal{O}_L),$$

dove il prodotto è fatto su tutti i primi Q *di* $\mathcal{O}_L$ *e, per ogni* Q*,* P *è l'ideale primo di* $\mathcal{O}_K$ *che sta sotto* Q*.*

Anche nel caso locale il differente serve a capire come ramifica il primo e la relazione fra differente e ramificazione è la stessa del caso globale.
Un'altra relazione locale-globale che useremo è la seguente proposizione:

Proposizione 1.10.3 *Un ideale primo di* Q *di* $\mathcal{O}_L$ *che sta sopra ad un primo* P *è ramificato tamely in un'estensione di campi di numeri* L/K *se e solo se la corrispondente estensione* L_Q/K_P *è tame.*

Se l'estensione di campi di numeri è di Galois, si riesce a descrivere il gruppo di Galois delle estensioni L_{Q_i}/K_P.

Teorema 1.10.4 *Se l'estensione di campi di numeri* L/K *è di Galois, con gruppo di Galois* G*, allora la corrispondente estensione di campi locali* L_{Q_i}/K_P *è di Galois e il gruppo di Galois di* L_{Q_i}/K_P *è un sottogruppo di* G *e in particolare è isomorfo al gruppo di decomposizione di* Q_i *su* P*.*

1.11 Anelli di gruppo

Sia G un gruppo finito e K un campo, chiamiamo $K[G]$ l'insieme delle combinazioni lineari formali $\alpha = \sum_{g\in G} a_g g$, con $g \in G$ e $a_g \in K$. $K[G]$ è un anello in cui le operazioni sono definite da

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g,$$

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h (gh).$$

Se R è un anello contenuto in K (nei casi trattati in questa tesi R sarà sempre un dominio di Dedekind) si definisce

$$R[G] = \left\{ \sum_{g\in G} a_g g \,:\, a_g \,\in\, R \right\}.$$

$R[G]$ è un R-ordine in $K[G]$, cioè un sottoanello di $K[G]$ che ha lo stesso elemento unità di $K[G]$, è un R-modulo finitamente generato e tale che

$$KR[G] = K[G].$$

1.12 Moduli su anelli PID

Per le dimostrazioni dei risultati seguenti si veda [La 2002].

Sia V uno spazio vettoriale di dimensione finita su un campo K, A un'applicazione lineare da V in sé e $K[X]$ l'anello (PID) di polinomi a coefficienti in K.
Considero l'omomorfismo

$$\Phi : K[X] \longrightarrow K[A] \subset End_K(V)$$

che ad X associa A, esteso per lineanità a tutti i polinomi di $K[X]$. L'anello $K[A]$, come sottoanello di $K[X]$, è commutativo.
V diventa così un $K[X]$-modulo con la moltiplicazione

$$(f(X))v = \Phi(f(X))v$$

per ogni $f(X) \in K[X]$ e $v \in V$.
Il nucleo di Φ è un ideale principale di $K[X]$, generato da un polinomio monico, il polinomio minimo di A, che chiameremo $m_A(X)$.

Definizione 1.12.1 *V si dice un $K[A]$-modulo ciclico se esiste un vettore $v \in V$ tale che $K[A]v = K[X]v = V$, cioè se V è generato su K dagli elementi $v, A(v), A^2(V), \ldots$.*

Se V è un $K[A]$-modulo ciclico, allora V è isomorfo a $K[X]/(m_A(X))$, tramite la mappa che ad $f(X)$ associa $f(A)v$; inoltre la dimensione di V come spazio vettoriale su K coincide con il grado di $m_A(X)$.
Si può dimostrare anche che $m_A(X)$ è univocamente determinato da A e non dipende dalla scelta del generatore v di V.

Teorema 1.12.2 *Sia V uno spazio vettoriale di dimensione finita sul campo K e A un'applicazione lineare da V in V, allora V si decompone nel modo seguente:*

$$V = V_1 \oplus ... \oplus V_r,$$

dove ogni V_i è un $K[A]$-sottomodulo modulo ciclico, con polinomio minimo m_i tale che

$$m_1 \mid m_2 \mid ... \mid m_r.$$

La sequenza $(m_1, m_2, ..., m_r)$ è univocamente determinata da V ed A e m_r è il polinomio minimo di A.

Il seguente corollario servirà per la dimostrazione del teorema 2.1.2

Corollario 1.12.3 *Con le stesse ipotesi del teorema sono equivalenti:*

(i) V è un $K[A]$-modulo ciclico,

(ii) $deg(m_A(X)) = dim_K(V)$.

Il teorema 1.12.2 è un caso particolare del teorema seguente, la cui dimostrazione si trova in [Sa 1967].

Teorema 1.12.4 *Sia A un anello ad ideali principali, M un A-modulo libero di rango finito n e M' un sottomodulo di M, allora*

(i) M' è libero di rango $\leq n$;

(ii) esiste una base $(e_1, ..., e_n)$ di M, un intero $q \leq n$ e elementi non nulli $a_1, ..., a_q$ di A tali che $(a_1e_1, ..., a_qe_q)$ sia una base di M' e tali che a_i divide a_{i+1} per $1 \leq i \leq q-1$.

1.13 Caratteri di Dirichlet

Per le dimostrazioni dei risultati in questo paragrafo si veda [Wa 1982].

Definizione 1.13.1 *Un carattere di Dirichlet è un omomorfismo moltiplicativo*

$$\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*.$$

χ si dice pari se $\chi(-1) = 1$, dispari se $\chi(-1) = -1$.

Se $n \mid m$ allora χ induce un omomorfismo da $(\mathbb{Z}/m\mathbb{Z})^*$ in $(\mathbb{C})^*$, componendo con la mappa naturale $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.
χ, quindi, modulo n o modulo m, definisce sostanzialmente la stessa funzione.

Definizione 1.13.2 *Sia χ un carattere di Dirichlet, si sice conduttore di χ e si indica con f_χ o f il minimo intero n per cui χ è definito modulo n. I caratteri definiti modulo il proprio conduttore sono detti primitivi.*

Definizione 1.13.3 *Se G è un gruppo abeliano si definisce gruppo duale di G e si indica con $\widehat{G}$ il gruppo $Hom(G, \mathbb{C}^*)$. Se G ha esponente n, allora $\widehat{G} = Hom(G, \mathbb{Z}/n\mathbb{Z})$.*

Sia ζ_n una radice n-esima primitiva dell'unità, identificando $G = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ con $(\mathbb{Z}/n\mathbb{Z})^*$, un carattere di Dirichlet definito modulo n diventa un elemento di $\widehat{G}$, viceversa un elemento di $\widehat{G}$ è un carattere di Dirichlet definito modulo n. Vediamo che relazione c'è tra i gruppi di Galois di estensioni abeliane di $\mathbb{Q}$ contenute in $\mathbb{Q}(\zeta_n)$ e caratteri di Dirichlet definiti modulo n.
Valgono i seguenti risultati.

Lemma 1.13.4 *Se G è un gruppo abeliano finito, allora $G \cong \widehat{G}$.*

Lemma 1.13.5 *Se G è un gruppo abeliano finito, allora $G \cong \widehat{\widehat{G}}$ con un isomorfismo canonico.*

Consideriamo ora la mappa

$$\begin{array}{ccc} G \times \widehat{G} & \to & \mathbb{C}^* \\ (g, \chi) & \mapsto & \chi(g). \end{array}$$

È non degenere in entrambi gli argomenti. Sia H un sottogruppo di G, definendo

$$H^\perp = \{\chi \in \widehat{G} |\, \chi(h) = 1, \forall h \in H\}$$

troviamo gli isomorfismi seguenti:

(i) $H^\perp \cong (\widehat{G/H})$,

(ii) $\widehat{H} \cong \widehat{G}/H^\perp$,

(iii) $(H^\perp)^\perp \cong H$.

Sia χ un carattere modulo n, cioè un carattere di $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, e L il campo fissato dal nucleo di χ. Allora $L \subseteq \mathbb{Q}(\zeta_n)$ e, se n è minimale, $n = f_\chi$. Il campo L dipende solo da χ ed è detto il campo corrispondente a χ. Più in generale, sia X un gruppo finito di caratteri di Dirichlet e n il minimo comune multiplo dei conduttori dei caratteri in X, X è un sottogruppo del gruppo duale di $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Sia H l'intersezione dei nuclei di questi caratteri e L il campo fissato da H, L è detto il campo corrispondente a X.
Sia X il gruppo di caratteri di Dirichlet associato ad un campo L, allora abbiamo una mappa

$$Gal(L/\mathbb{Q}) \times X \to \mathbb{C}^*.$$

Sia K un campo contenuto in L e

$$Y = \{\chi \in X | \chi(g) = 1, \forall g \in Gal(L/K)\}.$$

Allora

$$Y = Gal(L/K)^{\perp} = (\widehat{Gal(L/\mathbb{Q})/Gal(L/K)}) = \widehat{Gal(K/\mathbb{Q})}.$$

Viceversa, se consideriamo un sottogruppo $Y \subseteq X$ e K il campo fissato da

$$Y^{\perp} = \{g \in Gal(L/\mathbb{Q}) | \chi(g) = 1, \forall \chi \in Y\},$$

allora $Y^{\perp} = Gal(L/K)$ (per la corrispondenza di Galois).
Quindi $Y = (Y^{\perp})^{\perp} = Gal(L/K)^{\perp} = \widehat{Gal(K/\mathbb{Q})}$. Segue che c'è una corrispondenza biunivoca tra i sottogruppi di X e i sottocampi di L data da

$$\begin{array}{rcl} Gal(L/K)^{\perp} & \leftrightarrow & K \\ Y & \leftrightarrow & \text{campo fissato da } Y^{\perp}. \end{array}$$

Questa crea una corrispondenza biunivoca tra tutti i gruppi dei caratteri di Dirichlet e i sottocampi di campi ciclotomici.

Capitolo 2

Primi risultati

2.1 Base normale per un' estensione di campi

Definizione 2.1.1 *Sia L/K un'estensione di Galois di grado n, con gruppo di Galois $G = Gal(L/K) = \{\sigma_1, ..., \sigma_n\}$. Si dice che L/K ha una base normale se esiste un elemento $\alpha \in L$ tale che $\{\sigma_1(\alpha), ..., \sigma_n(\alpha)\}$ sia una base di L/K.*

L'estensione L/K deve essere necessariamente di Galois, in questo modo l'azione di G su L è ben definita: se $\alpha \in L$, $\sigma(\alpha) \in L$ per ogni $\sigma \in G$.
Quindi, considerando L come modulo su $K[G]$, l'azione dell'anello di gruppo è definita da

$$(\sum_{\sigma \in G} a_\sigma \sigma)(x) = \sum_{\sigma \in G} a_\sigma \sigma(x)$$

per $a_\sigma \in K$, $\sigma \in G$ e $x \in L$.
Dimostrare l'esistenza della base normale per L/K è chiaramente equivalente a verificare che L è libero di rango 1 come modulo su $K[G]$.
Le basi normali di campi esistono sempre: è la tesi del teorema seguente.

Teorema (della base normale) 2.1.2 *Sia L/K un'estensione di Galois di grado n, con gruppo di Galois $G = Gal(L/K) = \{\sigma_1, ..., \sigma_n\}$, allora esiste una base normale per L/K.*

Dimostrazione

Supponiamo prima che K sia infinito.
Sia

$$\varphi(i, j) : \{1, ..., n\} \times \{1, ..., n\} \longrightarrow \{1, ..., n\}$$

tale che $\sigma_i \circ \sigma_j = \sigma_{\varphi(i,j)}$.
Siano $X_1, ..., X_n$ indeterminate, consideriamo la matrice

$$M = (X_{\varphi(i,j)})_{i,j}.$$

Se indichiamo con $d(X_1, ..., X_n)$ il $\det M$, allora $d(X_1, ..., X_n) \neq 0$ come polinomio in $K[X_1, ..., X_n]$, infatti $d(1, 0, ..., 0) = \pm 1$ perché le righe e le colonne sono permutazioni delle X_i.
Dimostriamo ora che $\exists\, \alpha \in L$ tale che $d(\sigma_1(\alpha), ..., \sigma_n(\alpha)) \neq 0$.
Sia $a_1, ..., a_n$ una base di L/K, allora $\det[\sigma_i(a_j)]_{i,j}^2 = \text{disc}(a_1, ..., a_n) \neq 0$; possiamo quindi considerare il seguente cambiamento di variabili:

$$X_i \longmapsto \sum_{j=1}^{n} \sigma_i(a_j) Y_j.$$

Otteniamo allora

$$d(X_1, ..., X_n) = g(Y_1, ..., Y_n) \neq 0.$$

Poiché K é un campo infinito esistono $s_1, ..., s_n$ appartenenti a K tali che $g(s_1, ..., s_n) \neq 0$. Ma

$$g(s_1, ..., s_n) = d(\sum_{j=1}^{n} \sigma_1(a_j) s_j, ..., \sum_{j=1}^{n} \sigma_n(a_j) s_j).$$

Gli s_j appartengono a K, per cui sono lasciati fissi dal gruppo di Galois, quindi

$$d(\sum_{j=1}^{n} \sigma_1(a_j) s_j, ..., \sum_{j=1}^{n} \sigma_n(a_j) s_j) = d(\sigma_1(\sum_{j=1}^{n} a_j s_j), ..., \sigma_n(\sum_{j=1}^{n} a_j s_j)).$$

Se $\alpha = \sum_{j=1}^{n} a_j s_j$ troviamo che $d(\sigma_1(\alpha), ..., \sigma_n(\alpha)) \neq 0$.
Per concludere basta osservare che $d(\sigma_1(\alpha), ..., \sigma_n(\alpha))$ è la radice quadrata del dicriminante di $(\sigma_1(\alpha), ..., \sigma_n(\alpha))$, dimostrando quindi che $\sigma_1(\alpha), ..., \sigma_n(\alpha)$ è una base. Vediamo questa ultima verifica:

$$\begin{aligned}(\text{disc}(\sigma_1(\alpha), ..., \sigma_n(\alpha)))^{\frac{1}{2}} &= \det[\sigma_i \sigma_j(\alpha)]_{i,j} = \\ &= \det[\sigma_{\varphi(i,j)}(\alpha)]_{i,j} = d(\sigma_1(\alpha), ..., \sigma_n(\alpha)).\end{aligned}$$

Supponiamo ora che K sia un campo finito, allora $G = Gal(L/K) =< \sigma >$, con $\sigma^n = \text{id}$ se $n = |G|$. Possiamo considerare σ come applicazione lineare da L in L: supponiamo infatti che $K = \mathbb{F}_{p^a}$ e $L = \mathbb{F}_{p^{an}}$, allora $\sigma(x) = x^{p^a}$ per ogni x che appartiene ad L; vale allora

$$\sigma(ax + by) = (ax + by)^{p^a} = a^{p^a} x^{p^a} + b^{p^a} y^{p^a} = ax^{p^a} + by^{p^a} = a\sigma(x) + b\sigma(y)$$

per $a, b \in L$ e $x, y \in K$. Il polinomio minimo di σ è $m(X) = X^n - 1$: infatti $m(\sigma) = 0$ e non può esistere un polinomio di grado minore che si annulli calcolato in σ; se esistesse avremmo un' equazione di questo tipo:

$$a_0 \text{id} + a_1\sigma + a_2\sigma^2 + ... + a_{n-1}\sigma^{n-1} = 0 \tag{2.1}$$

con gli $a_i \in K$ non tutti nulli.
Dato che $\text{id}, \sigma^1, ..., \sigma^{n-1}$ sono caratteri distinti che vanno da L^* in L^*, l'equazione (2.1), contradirebbe il teorema di Artin sull'indipendenza lineare dei

caratteri. Poiché inoltre il grado di $m(X)$ coincide con la dimensione di L come spazio vettoriale su K, dal corollario 1.12.3 segue che L è un $K[\sigma]$-modulo ciclico, cioè esiste un elemento $\alpha \in L$ tale che

$$\alpha, \sigma(\alpha), \sigma^2(\alpha), ..., \sigma^{n-1}(\alpha) \tag{2.2}$$

sia una base di L come spazio vettoriale su K. La base in (2.2) è chiaramente normale.

□

2.2 Base normale per l'anello degli interi

Il problema analogo per l'anello degli interi non è così semplice ed è infatti ancora aperto. Sia L/K un'estensione di Galois di campi con $G = Gal(L/K)$, allora L ha una base normale intera se e solo se $\mathcal{O}_L$ è isomorfo ad $\mathcal{O}_K[G]$ come $\mathcal{O}_K[G]$-modulo. Se esistesse sempre una base normale intera avremmo che $\mathcal{O}_L$ sarebbe sempre un $\mathcal{O}_K$-modulo libero, cioè dovrebbe esistere sempre una base intera relativa e questo in generale è falso. Ci sono numerosi controesempi: MacKenzie e Scheuneman in [MKSc 1971] dimostrano che se $K = \mathbb{Q}(\sqrt{-14})$ e $L = \mathbb{Q}(\sqrt{-7}, \sqrt{-14})$ non esiste una base intera (di $\mathcal{O}_L$ come $\mathcal{O}_K$-modulo). Anche nel caso in cui $\mathcal{O}_K$ sia ad ideali principali, caso in cui $\mathcal{O}_L$ è libero su $\mathcal{O}_K$, non sempre esiste una base normale intera, cioè non sempre vale che $\mathcal{O}_L$ è un $\mathcal{O}_K[G]$-modulo libero, questo si vede già nel caso di $K = \mathbb{Q}$.

Vediamo infatti cosa succede se $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{-1})$, in questo caso $G = Gal(L/K) = \{\mathrm{id}, \sigma\}$, dove σ è il coniugio. Allora $\mathcal{O}_K[G] = \mathbb{Z} \oplus \mathbb{Z}\sigma = \{a + b\sigma \mid a, b \in \mathbb{Z}\}$ e $\mathcal{O}_L = \mathbb{Z}[i]$. Se esistesse una base normale intera avremmo che $\mathbb{Z}[i] \cong \mathbb{Z}[G]$ come $\mathbb{Z}[G]$-modulo, cioè dovrebbe esistere un elemento $\alpha = x + iy$ con x, $y \in \mathbb{Z}$ tale che $\mathbb{Z}[i] = \mathbb{Z}[G](x + iy)$. Vediamo che questo non è possibile: se esistesse α, allora $(a+b\sigma)(x+iy)$, al variare di a e b in $\mathbb{Z}$, dovrebbe descrivere tutti gli elementi di $\mathbb{Z}[i]$, ma

$$(a + b\sigma)(x + iy) = a(x + iy) + b(x - iy) = (a + b)x + (a - b)iy.$$

Ovviamente $a + b$ e $a - b$ hanno la stessa parità, per cui

(i) se x o y è pari, $(a + b)x$ o $(a - b)y$ è sempre pari,

(ii) se x e y sono dispari, allora $(a + b)x$ o $(a - b)y$ hanno la stessa parità.

Per cui qualunque siano i valori di x e y, $(a + b\sigma)(x + iy)$, al variare di a e b in $\mathbb{Z}$, non può descrivere tutti gli elementi di $\mathbb{Z}[i]$, cioè non può esistere una base normale intera.

Una conizione necessaria per l'esistenza di una base normale è che la traccia

$$\mathrm{T}_{L/K} : \mathcal{O}_L \to \mathcal{O}_K$$

sia surgettiva, cioè L/K sia tame. La dimostrazione di questo è presente già in [Sp 1916].

Lemma 2.2.1 *Sia L/K un' estensione di Galois con $G = Gal(L/K)$ tale che $\mathcal{O}_L \cong \mathcal{O}_K[G]$, come $\mathcal{O}_K[G]$-modulo, allora la traccia $T_{L/K} : \mathcal{O}_L \to \mathcal{O}_K$ è surgettiva.*

Dimostrazione

Sia f l'isomorfismo di $\mathcal{O}_K[G]$-moduli tra $\mathcal{O}_L$ e $\mathcal{O}_K[G]$ e, se id è l'identità di G, $a = f(\mathrm{id})$. Siccome f è un isomorfismo, allora per ogni x appartenente ad $\mathcal{O}_K$ esistono elementi $\{a_g\}_{g\in G}$ di $\mathcal{O}_K$ tali che

$$x = f\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g g(a);$$

così per ogni $h \in G$ si ha

$$x = h(x) = \sum_{g\in G} a_g hg(a) = \sum_{g\in G} a_{h^{-1}g} g(a).$$

Cioè per ogni $h \in G$

$$a_g = a_{h^{-1}g},$$

ovvero gli a_g sono indipendenti da g. Allora possiamo scrivere x in modo più chiaro

$$x = a_{\mathrm{id}} \sum_{g\in G} g(a) = a_{\mathrm{id}} \mathrm{Tr}_{L/K}(a) = \mathrm{Tr}_{L/K}(a_{\mathrm{id}} a).$$

Quindi abbiamo la tesi: ogni elemento di $\mathcal{O}_K$ appartiene all'immagine della traccia.

□

Lemma 2.2.2 *Sia L/K una estensione di Galois di campi di numeri, allora L/K è tame se e solo se la traccia è surgettiva.*

Dimostrazione

Cominciamo coll'osservare che $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ coincide col minimo comune multiplo degli ideali interi di $\mathcal{O}_K$ tali che estesi ad $\mathcal{O}_L$ dividono il differente. Questo si vede applicando una proprietà del differente: sia I un ideale intero di $\mathcal{O}_K$, allora

$$I \mid \mathrm{Tr}_{L/K}(\mathcal{O}_L) \quad \Leftrightarrow \quad \mathcal{O}_L \subset I {D_{L/K}}^{-1}.$$

Cioè $I \mid \mathrm{Tr}_{L/K}(\mathcal{O}_L)$ se e solo se $I\mathcal{O}_L \mid D_{L/K}$, così il massimo divisore di $D_{L/K}$ che è estensione di un ideale di $\mathcal{O}_K$ è uguale a $\mathrm{Tr}_{L/K}(\mathcal{O}_L)\mathcal{O}_L$, quindi $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ è il minimo comune multiplo, come volevamo dimostrare. Verificare la surgettività della traccia equivale a dimostrare che il differente non ha divisori diversi da $\mathcal{O}_L$ che siano estensioni di ideali di $\mathcal{O}_K$. Se L/K è normale allora $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \neq \mathcal{O}_K$ se e solo se esiste un ideale primo di Q di $\mathcal{O}_L$ tale che $Q^e \mid D_{L/K}$, con $e = e_{L/K}(Q)$. L'ultima condizione è equivalente per il primo Q

ad avere ramificazione selvaggia. Se avesse ramificazione moderata, allora Q^e non potrebbe dividere $D_{L/K}$ e viceversa, se Q ha ramificazione selvaggia allora la corrispondente estensione di campi locali L_Q/K_P, con P il primo che sta sotto Q è un'estensione wild. Quindi Q^e divide il differente locale e di conseguenza anche anche il differente globale.

□

Lo stesso risultato vale nel caso locale.

Corollario 2.2.3 *Sia L/K una estensione di Galois di campi p-adici, allora L/K è tame se e solo se la traccia è surgettiva.*

Dimostrazione

La dimostrazione è molto simile a quella del lemma 2.2.2. Si dimostra, allo stesso modo di prima, che $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ coincide col minimo comune multiplo degli ideali interi di $\mathcal{O}_K$ tali che estesi ad $\mathcal{O}_L$ dividono il differente. La traccia è surgettiva, quindi, se e solo il differente non ha divisori del tipo $I\mathcal{O}_L$, dove $I \subsetneq \mathcal{O}_K$. Ma $D_{L/K} = Q^m$ (Q l'ideale primo di $\mathcal{O}_L$), con $m \leq e-1$ se L/K è tame, e $m \geq e$ altrimenti, cioè Q^e è la minima potenza di Q della forma $I\mathcal{O}_L$, con $I \subsetneq \mathcal{O}_K$.

□

Quindi se un'estensione, di campi di numeri o di campi p-adici, ha una base normale intera è tame. Ci si può chiedere se è vero il viceversa. In effetti l'estensione $\mathbb{Q}(i)/\mathbb{Q}$ per cui abbiamo visto che non esiste una base normale intera non è tame, il primo 2 è ramificato wildly. Purtroppo la ramificazione moderata non garantisce l'esistenza di una base normale intera. Il seguente esempio si trova in [Ka 1984].

Teorema 2.2.4 *Siano m ed n interi di $\mathbb{Z}$ liberi da quadrati. Supponiamo che $m, n \equiv 3 \pmod 4$, $m < -1$, $n < 0$ e che $(m,n) = 1$. Allora l'estensione quadratica $\mathbb{Q}(\sqrt{m}, \sqrt{n})/\mathbb{Q}(\sqrt{m})$ è tame senza base normale intera.*

Dimostrazione

Poniamo $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ e $K = \mathbb{Q}(\sqrt{m})$. Sia $G = Gal(L/K) = \{1, \tau\}$, dove τ è il coniugio. Allora una base di $\mathcal{O}_L$ su $\mathcal{O}_K$ come $\mathcal{O}_K$-modulo è data da $\{1, \frac{\sqrt{n}+\sqrt{m}}{2}\}$: si vede applicando un risultato di Bird e Parry i quali in [BiPa 1976] danno una condizione necessaria e sufficiente affinché le estensioni $\mathbb{Q}(\sqrt{m}, \sqrt{n})/\mathbb{Q}(\sqrt{m})$ abbiano una base intera. Inoltre $\{1, \sqrt{m}, \frac{\sqrt{n}+\sqrt{m}}{2}, \frac{1+\sqrt{nm}}{2}\}$ è una $\mathbb{Z}$-base di $\mathcal{O}_L$. Si vede facilmente: infatti ogni elemento di $\mathcal{O}_L$ si scrive

$$\frac{e + f\sqrt{m} + g\sqrt{n} + h\sqrt{mn}}{2}$$

con $e,\ f,\ g,\ h,\ \in \mathbb{Z}$ e $e \equiv h \pmod 2$, $f \equiv g \pmod 2$. Sia α un elemento di $\mathcal{O}_L$, allora $\alpha = a + b\sqrt{m} + c\frac{\sqrt{n}+\sqrt{m}}{2} + d\frac{1+\sqrt{nm}}{2}$, con $a, b, c, d \in \mathbb{Z}$. Allora $\tau(\alpha) = a + b\sqrt{m} + c\frac{-\sqrt{n}+\sqrt{m}}{2} + d\frac{1-\sqrt{nm}}{2}$, per cui

$$\begin{pmatrix} \alpha \\ \tau(\alpha) \end{pmatrix} = A \begin{pmatrix} 1 \\ (\sqrt{m}+\sqrt{n})/2 \end{pmatrix}$$

dove

$$A = \begin{pmatrix} a + b\sqrt{m} + d(1+m)/2 & c - d\sqrt{m} \\ a + (b+c)\sqrt{m} + d(1+m)/2 & -(c + d\sqrt{m}) \end{pmatrix}.$$

Allora abbiamo che $\det(A) = -(c - d\sqrt{m})((2a + d) + (2b + c)\sqrt{m})$ e α è un generatore di una base normale intera di L/K se e solo se il determinante di A appartiene agli invertibili di $\mathbb{Z}[\sqrt{m}]$. Cioè $\det(A)$ deve avere norma uguale a più o meno uno:

$$(2a + d)^2 - m(2b + c)^2 = \pm 1$$
$$c^2 - md^2 = \pm 1.$$

Siccome $-m > 1$, abbiamo che $2a + d = \pm 1$, $2b + c = 0$, $c = \pm 1$ e $d = 0$, cioè $2a = \pm 1$, che è un assurdo perché $a \in \mathbb{Z}$. Non esiste quindi una base normale intera per L/K. L'estensione è tame perché la traccia $\mathrm{Tr}_{L/K}$ è chiaramente surgettiva, infatti

$$\mathrm{Tr}_{L/K}(a + b\sqrt{m} + c\frac{\sqrt{n}+\sqrt{m}}{2} + d\frac{1+\sqrt{nm}}{2}) = 2a + d + (2b + c)\sqrt{m}$$

ed ogni elemento di $\mathbb{Z} + \mathbb{Z}(\sqrt{m})$ può essere scritto come $2a + d + (2b + c)\sqrt{m}$.

□

2.3 Caso locale

Nel caso locale ogni estensione tame ha una base normale intera: la dimostrazione seguente è di Kawamoto [Ka 1986].

Teorema 2.3.1 *Sia L/K un'estensione di campi locali tame e di Galois; allora L/K ha una base normale intera.*

Dimostrazione

La dimostrazione è un po' tecnica, lo schema dimostrativo però è abbastanza semplice. Prima si prende un'estensione L'/K tale che $L \subset L'$ e L'/L sia non ramificata e si descrive il gruppo di Galois di L'/K. In seguito si considerano le due sottoestensioni L'/K_0' e K_0'/K, dove K_0' è la massima sottoestensione non ramificata di L'/K, si trova una base normale intera per ciascuna di esse e succesivamente per l'estensione composta. Infine si applica la traccia ($\mathrm{Tr}_{L'/L}$) a questa base, la cui immagine è una base normale intera di L/K.

Siano e ed f rispettivamente l'indice di ramificazione ed il grado di inerzia di L/K, q il numero di elementi nel campo residuo di K e L' l'estensione non

ramificata di L di grado e. Allora L'/K è un'estensione tame: infatti l'indice di ramificazione è moltiplicativo nelle torri di estensioni; siccome L/K è tame con indice di ramificazione e e L'/L è non ramificata, allora $e_{L'/K} = e_{L/K} = e$. Inoltre L'/K è ancora di Galois: infatti l'immagine di L' tramite un omomorfismo iniettivo che lascia fisso K deve essere contenuta in un'estensione non ramificata di grado e di L, che è unica, cioè coincide con L'.
Sia π un primo di K, Π un primo di L e ξ una radice (q^f-1)-esima dell'unità tale che $\Pi^e = \pi\xi$. Siccome L/K è tame, $L = K(\Pi, \xi)$, ma è anche di Galois: $\xi^{\frac{q^f-1}{e}}$ deve appartenere ad L, cioè $e \mid q^f - 1$. Allora $(q^f-1)e$ divide $q^{ef}-1$. Perciò $\xi = \eta^e$, dove η è una radice $(q^{ef}-1)$-esima contenuta in L'. Ponendo $\pi' = \Pi\eta^{-1}$, troviamo che $\pi'^e = (\Pi)^e\eta^{-e} = \pi$ e π' è un primo di L'.
Chiamiamo $F = K(\pi')$, allora F è un'estensione totalmente ramificata di grado e di K. Sia K_0' la massima sottoestensione non ramificata di L'/K e ζ una radice $(q^{ef}-1)$-esima dell'unità. Allora

$$K_0' = K(\zeta),\ L' = K(\zeta, \pi').$$

Siano G e H rispettivamente i gruppi di Galois di L'/K e L'/K_0'. Allora H è un sottogruppo normale di G, poiché l'estensione K_0'/K è non ramificata, quindi normale. Inoltre H è ciclico perché l'estensione L'/K_0' è radicale, ma anche G/H è ciclico perché è il gruppo di Galois di un'estensione non ramificata. Sia ϕ il generatore del gruppo di Galois dell'estensione non ramificata L'/F e τ il generatore di H, allora il gruppo G è generato da ϕ e τ. Vediamo cosa succede ai generatori:

$$\begin{array}{ll} \phi(\zeta) = \zeta^{\,q}, & \phi(\pi) = \pi \\ \tau(\zeta) = \zeta, & \tau(\pi') = \omega\pi', \end{array}$$

dove ω è una radice e-esima dell'unità. Abbiamo descritto il gruppo di Galois di L'/K, consideriamo ora l'estensione L'/K_0'.

(i) Una base normale intera di L'/K_0'.
Una base intera di L'/K_0' è data da $\{\pi'^{\,m}\}_{m=0,1,\dots,e-1}$. Se $\alpha \in \mathcal{O}_{L'}$ allora $\alpha = \sum_{m=0}^{e-1} u_m \pi'^m$, per certi $u_m \in \mathcal{O}_{K_0'}$. Allora abbiamo che

$$\begin{pmatrix} \alpha \\ \tau(\alpha) \\ \vdots \\ \tau^{e-1}(\alpha) \end{pmatrix} = A \begin{pmatrix} 1 \\ \pi' \\ \vdots \\ \pi'^{e-1} \end{pmatrix},$$

dove

$$A = (u_m\omega^{im})_{0\le i,\, m\le e-1}$$

Il determinante di (ω^{im}) è un deteminante di Vandermonde, cioè il prodotto di tutte le differenze delle entrate della matrice A.
I fattori saranno del tipo $(\omega^k - \omega^n) = \omega^k(1-\omega^{n-k})$; dimostriamo che ogni fattore è invertibile in $\mathcal{O}_{K_0'}$, cosicché il determinante sarà invertibile in

$\mathcal{O}_{K_0'}$. ω^{n-k} è ancora una radice e-esima dell'unità ed è quindi invertibile. Per vedere che $1-\omega^{n-k}$ è invertibile consideriamo il polinomio $f(x) = 1+x+...+x^{e-1}$. Allora ω^{n-k} è una radice di $f(x)$, cioè $x-\omega^{n-k} \mid f(x)$, in particolare $1-\omega^{n-k} \mid e$, è quindi invertibile perché L'/K_0' è tame. Allora, poiché

$$\det(\mathrm{A}) = \left(\prod_{m=0}^{e-1} u_m\right) \det(\omega^{im}),$$

α genera una base normale intera se e solo se tutti gli u_m $(m = 0, ..., e-1)$ sono unità di $\mathcal{O}_{K_0'}$. In particolare $\alpha = \sum_{m=0}^{e-1} \pi'^m$ genera una base normale intera di L'/K_0'.

(ii) Una base normale intera di K_0'/K.
Una base intera di K_0'/K è data da $\{\zeta^m\}_{m=0,1,...,ef-1}$, poiché K_0'/K è non ramificata. Consideriamo le estensioni di campi residui: $\mathcal{O}_{K_0'}/Q$, dove Q è l' ideale primo di $\mathcal{O}_{K_0'}$, e $\mathcal{O}_K/P$, dove P è l' ideale primo di $\mathcal{O}_K$. Il gruppo di Galois dell'estensione di campi residui è isomorfo a quello dell'estensione K_0'/K. Per il teorema della base normale (Teorema 2.1.2) si ha che l'estensione di campi residui ha una base normale, con $\overline{\beta}$ il generatore. Sia $\beta \in \mathcal{O}_{K_0'}$ un rappresentante di $\overline{\beta}$, allora β genera una base normale intera di K_0'/K. β in termini della base scelta all'inizio si scrive come $\beta = \sum_{m=0}^{ef-1} b_m \zeta^m$, con $b_m \in \mathcal{O}_K$.

(iii) Una base normale intera di L'/K.
Da (i) e (ii) segue che $\mathcal{O}_{L'} = \oplus_{i=0}^{e-1} \oplus_{j=0}^{ef-1} \mathcal{O}_K \tau^i \alpha \sigma^j \beta$. Dalle forme di α e β precisate in (i) e (ii) si vede che vale che

$$\tau^i \alpha \sigma^j \beta = \tau^i \sigma^j (\alpha\beta).$$

Perciò $\alpha\beta$ genera una base normale intera di L'/K.

(iv) Una base normale intera di L/K.
Una base normale di intera di L/K è a questo punto semplice da trovare: $\mathrm{Tr}_{L'/L}(\alpha\beta)$ genera una base normale intera di L/K, per vederlo basta ripetere lo stesso ragionamento fatto nel lemma 3.2.3, sostituendo K a $\mathbb{Q}$.

□

In realtà vale un risultato più forte. Sia L/K un'estensione di campi di numeri di Galois tame, sia P un primo di $\mathcal{O}_K$ tale che $P\mathcal{O}_L = (Q_1...Q_r)^e$, allora L_{Q_i}/K_P è un'estensione di campi locali di Galois tame con gruppo di Galois $G_i \cong D(Qi|P)$ dove $D(Q_i|P)$ è il gruppo di decomposizione di Q_i su P. Applicando il teorema appena dimostrato si ha, per ogni i, $\mathcal{O}_{L_{Q_i}} \cong \mathcal{O}_{K_P}[G_i]$ come $\mathcal{O}_{K_P}[G_i]$-modulo, cioè tutte le estensioni locali tame hanno una base normale intera. Vale il seguente teorema:

Teorema 2.3.2 *Con le ipotesi suddette*

$$\mathcal{O}_{L_P} \cong \mathcal{O}_{K_P}[G].$$

Per la dimostrazione serve un lemma

Lemma 2.3.3 *Sia $\mathcal{O}_{L_P}$ un $\mathcal{O}_{K_P}[G]$-modulo e G_1 il gruppo di decomposizione di Q_1 su p, quindi $G_1 = \{g \in G : g(\mathcal{O}_{L_{Q_1}}) = \mathcal{O}_{L_{Q_1}}\}$. Siano $\{\mathcal{O}_{L_{Q_i}}\}_{i=1}^r$ tali che*

(i) $\mathcal{O}_{L_P} = \oplus_{i=1}^r \mathcal{O}_{L_{Q_i}}$,

(ii) *l'azione di G su $\mathcal{O}_{L_P}$ permuta gli $\mathcal{O}_{L_{Q_i}}$, cioè per ogni $g \in G$, per ogni $i \in I$, $g(\mathcal{O}_{L_{Q_i}}) = \mathcal{O}_{L_{Q_j}}$ per qualche j in I,*

(iii) *l'azione è transitiva, cioè per ogni i e j esiste $g \in G$ tale che $g(\mathcal{O}_{L_{Q_i}}) = \mathcal{O}_{L_{Q_j}}$,*

allora

$$\mathcal{O}_{L_P} \cong \mathcal{O}_{L_{Q_1}} \otimes_{\mathcal{O}_{K_P}[G_1]} \mathcal{O}_{K_P}[G].$$

Dimostrazione

C'è una corrispondenza biunivoca tra

$$\{\mathcal{O}_{L_{Q_i}}\} \quad \leftrightarrow \quad \{\text{classi laterali di } G_1\}$$

data da

$$\left(\mathcal{O}_{L_{Q_i}}\right) \quad \leftrightarrow \quad \{g \in G : g(\mathcal{O}_{L_{Q_1}}) = \mathcal{O}_{L_{Q_i}}\}.$$

Prendiamo un insieme di rappresentanti delle classi laterali di G_1 in G, $\{g_1\}_{i\in I}$ con $g_1 =$id. Definiamo una funzione

$$\alpha : G \times \mathcal{O}_{L_{Q_1}} \quad \to \quad \mathcal{O}_{L_P}$$

data da $\alpha(g,\, w) = g(w)$. Questa si estende chiaramente:

$$\begin{array}{ccc} \alpha : \mathcal{O}_{K_P}[G] \times \mathcal{O}_{L_{Q_1}} & \to & \mathcal{O}_{L_P} \\ \alpha\left(\sum a_j g_j,\, w\right) & \mapsto & \sum a_j g_j(w). \end{array}$$

Siccome per $h \in G_1$ vale che

$$\alpha(gh,\, w) = gh(w) = g(hw) = \alpha(g,\, hw),$$

α si estende a

$$\widetilde{\alpha} : \mathcal{O}_{K_P}[G] \otimes_{\mathcal{O}_{K_P}[G_1]} \mathcal{O}_{L_{Q_1}} \quad \to \quad \mathcal{O}_{L_P}.$$

Definiamo $\beta : \mathcal{O}_{L_P} \to \mathcal{O}_{K_P}[G] \otimes_{\mathcal{O}_{K_P}[G_1]} \mathcal{O}_{L_{Q_1}}$. Poichè $\mathcal{O}_{L_P} = \oplus_{i=1}^r \mathcal{O}_{L_{Q_i}}$ è sufficiente definire $\beta : \mathcal{O}_{L_{Q_i}} \to \mathcal{O}_{K_P}[G] \otimes_{\mathcal{O}_{K_P}[G_1]} \mathcal{O}_{L_{Q_1}}$ per ogni i. Sia $w_i \in \mathcal{O}_{L_{Q_i}}$, definiamo $\beta(w_i) = g_i \otimes g_i^{-1}(w_i)$. Verifichiamo ora che $\widetilde{\alpha}$ e β sono una l'inversa dell'altra. Per prima cosa vale che

$$\widetilde{\alpha}\beta(w_i) = \widetilde{\alpha}(g_i \otimes g_i^{-1}(w_i)) = g_i g_i^{-1}(w_i) = w_i.$$

Per ogni $g \in G$, g si può scivere come $g = g_i h$ per un unico $i \in I$ e $h \in G_1$. Così per $w \in \mathcal{O}_{L_{Q_1}}$ si ha

$$\beta\widetilde{\alpha}(g \otimes w) = \beta(g(w)) = \beta(g_i(h(w))) = g_i \otimes hw = g_i h \otimes w = g \otimes w.$$

□

Se L/K è un'estensione di campi di numeri di Galois, $L_P = L \otimes_K K_P$ e L_{Q_i} come sempre i campi costruiti completando L a primi Q_i di $\mathcal{O}_L$, le ipotesi del lemma 2.3.3 sono soddisfatte. Infatti l'ipotesi (i) è la formula (1.3); per vedere che le altre due ipotesi sono verificate basta ricordarsi che il gruppo di Galois G agisce sui primi sopra P e che l'azione è transitiva. In termini delle valutazioni indotte da i primi Q_i dire che G agisce e che l'azione è transitiva si traduce esattamente con le ipotesi (ii) e (iii).

Dimostrazione di 2.3.2

Applicando il lemma si ha che $\mathcal{O}_{L_P} \cong \mathcal{O}_{L_{Q_1}} \otimes_{\mathcal{O}_{K_P}[G_1]} \mathcal{O}_{K_P}[G]$. Poiché l'estensione L_{Q_i}/K_P è tame, $\mathcal{O}_{L_{Q_1}} \cong \mathcal{O}_{K_P}[G_1]$ come $\mathcal{O}_{K_P}[G_1]$-modulo, per cui si ha che $\mathcal{O}_{L_P} \cong \mathcal{O}_{K_P}[G]$ come $\mathcal{O}_{K_P}[G_1]$-modulo. Rimane da vedere che $\mathcal{O}_{L_P} \cong \mathcal{O}_{K_P}[G]$ come $\mathcal{O}_{K_P}[G]$-modulo. Scritto in altri termini dobbiamo dimostrare che se N è un A-modulo, l'isomorfismo di A-moduli $A \otimes_A N \cong N$ è in realta un isomorfismo di N-moduli. Ma $A \otimes_A N$ è un N-modulo con la sruttura seguente:

$$m(a \otimes n) = a \otimes mn;$$

quindi si vede che come N-modulo è isomorfo ad N.

□

Il fatto che ogni estensione tame locale abbia una base normale si chiama in genere teorema di Noether, riferendosi all'articolo [No 1931]. L'articolo in questione, putroppo, è un po' oscuro; infatti Noether nella prima pagina afferma che dimosterà che data un'estensione di campi di numeri L/K di grado n, per ogni primo P di $\mathcal{O}_K$ che non divide n, cioè tale che non sia un primo che sta sopra ai primi che compaiono nella fattorizzazione di n, esiste una base normale intera di L_P/K_P. E questo risultato si trova effettivamente nell'articolo; una riga più sotto aggiunge però:

> *Insbesondere also: Besitzt L/K keine höhere Verzweigung, so existier an jeder Verzweigungsstelle eine Normalbasis;*

che vuol dire

> In particolare anche: Se L/K non ha nessuna ramificazione superiore, allora esiste una base normale per ogni primo ramificato.

Non è affatto chiaro come si passi dal caso in cui $P \nmid n$ a tutte le estensioni senza ramificazione superiore (tame). Infatti dire che $P \nmid n$ è un ipotesi più forte del supporre che l'estensione L/K sia tame: suppurre che $P \nmid n$ vuol dire che $P \nmid e\, f\, r$, mentre tame significa che $(e,\, P) = 1$. In sostanza il teorema di Noether, così come lei lo enuncia, vale solo per estensioni tame totalmente ramificate. Per estensioni non ramificate esiste una base normale intera: è la parte (ii) della dimostrazione del teorema 2.3.1. Il problema nasce quando si ha a che fare con estensioni miste, in cui cioè sia presente sia inerzia che ramificazione. Questo caso non è affatto semplice da risolvere. L'articolo di Noether viene citato in quasi tutti gli articoli che ho letto, una dimostrazione alternativa, a parte quella

di Kawamoto esposta, si trova in [Fr 1983]; è una dimostrazione che non usa le tecniche di Noether, ma un risultato di Swan sui moduli proiettivi [Sw 1960]. Che l'articolo di Noether abbia qualche problema è sottolineato anche da Childs, che, in [Ch 2000], afferma che una dimostrazione soddisfacente del teorema di Noether viene data solo nel 1960 da Swan nell'articolo appena citato. Usando il risultato di Swan la dimostrazione è la seguente:

Dimostrazione di 2.3.1

Sia L/K un'estensione tame e sia $G = Gal(L/K)$. L'azione di $\mathcal{O}_K[G]$ su $\mathcal{O}_L$ rende $\mathcal{O}_L$ un $\mathcal{O}_K[G]$-modulo proiettivo. Per vederlo basta dimosrtare che $\mathcal{O}_L$ è proiettivo come $\mathcal{O}_K$-modulo e che esiste

$$f: \quad \mathcal{O}_L \quad \rightarrow \quad \mathcal{O}_L$$

omomorfismo di $\mathcal{O}_K$-moduli tale che $\sum_{\sigma\in G} \sigma f(\sigma^{-1}\alpha) = \alpha$, per ogni α in $\mathcal{O}_L$ [Ri 1959]. Ricordando che un modulo $\mathcal{O}_L$ è proiettivo se è un addendo diretto di un modulo libero, si vede che $\mathcal{O}_L$ è proiettivo come $\mathcal{O}_K$-modulo, perché è libero come modulo su $\mathcal{O}_K$. Sicome L/K è tame, la traccia è surgettiva, per cui $\exists\ \beta \in \mathcal{O}_L$ tale che $\mathrm{Tr}_{L/K}\beta = 1$. Prendendo come f la moltiplicazione per β si ha che

$$\sum_{\sigma\in G} \sigma(\beta\sigma^{-1}\alpha) = \alpha,$$

per ogni $\alpha \in \mathcal{O}_L$. Per cui $\mathcal{O}_L$ è proiettivo come $\mathcal{O}_K[G]$-modulo. Per dimostrare la tesi ci serve però che $\mathcal{O}_L$ sia un $\mathcal{O}_K[G]$-modulo libero. Per il teorema della base normale 2.1.2

$$L \cong K[G]$$

come $K[G]$-modulo, ma $L \cong K \otimes_{\mathcal{O}_K} \mathcal{O}_L$ e $K[G] \cong K \otimes_{\mathcal{O}_K} \mathcal{O}_K[G]$, per cui

$$K \otimes_{\mathcal{O}_K} \mathcal{O}_L \cong K \otimes_{\mathcal{O}_K} \mathcal{O}_K[G].$$

A questo punto si applica il risultato di Swan [Sw 1960]: se G è un gruppo finito e P e P' sono moduli finitamente generati, poiettivi su $R[G]$, dove R è un dominio completo, se $K \otimes P \cong K \otimes P'$, come $K[G]$ moduli, dove K è il campo quoziente di R, allora $P \cong P'$. Applicandolo al nostro caso con $\mathcal{O}_L = P$, $\mathcal{O}_K[G] = P'$, $R[G] = \mathcal{O}_K[G]$, si ha che

$$\mathcal{O}_L \cong \mathcal{O}_K[G],$$

come $\mathcal{O}_K[G]$ moduli, cioè $\mathcal{O}_L$ ha una base normale intera su $\mathcal{O}_K$.

□

Nel caso delle estensioni tame di campi locali, vale un risultato più forte, cioè che esiste una base normale intera per ogni ideale ambiguo di L. I seguenti risultati si trovano in [Ul 1970].

Definizione 2.3.4 *Un ideale I di $\mathcal{O}_L$, eventualmente anche frazionario, si dice ambiguo se è un G-modulo, cioè se è invariante per l'azione di G.*

Teorema 2.3.5 *Un' estensione di campi locali di Galois è tame se e solo se ogni ideale ambiguo ha una base normale intera.*

Dimostrazione

Se L/K è tame ogni ideale ambiguo di L è proiettivo come modulo su $\mathcal{O}_K[G]$. La dimostrazione è molto simile al caso di $\mathcal{O}_K$, anche in questo caso usiamo il risultato di Rim [Ri 1959]. Dimostriamo quindi che se I è un ideale ambiguo è proiettivo come $\mathcal{O}_K$-modulo e che esiste

$$f: \quad I \quad \rightarrow \quad I$$

omomorfismo di $\mathcal{O}_K$-moduli, tale che $\sum_{\sigma \in G} \sigma f(\sigma^{-1}\alpha) = \alpha$, per ogni α in I. L'ideale I è principale su $\mathcal{O}_L$, che è libero su $\mathcal{O}_K$, quindi è proiettivo come $\mathcal{O}_K$-modulo. La f è esattemente quella della proposizione precedente. I è quindi proiettivo come $\mathcal{O}_K[G]$-modulo. Anche i passaggi successivi ricalcano quelli svolti nel teorema precedente. Per ogni ideale frazionario si ha che $IK = L$ e

$$IK \cong I \otimes_{\mathcal{O}_K} K.$$

Applicando sempre il teorema della base normale abbiamo

$$L \cong K[G] \cong \mathcal{O}_K[G] \otimes_{\mathcal{O}_K} K.$$

Anche in questo caso le ipotesi del teorema di Swan sono soddisfatte, quindi

$$I \cong \mathcal{O}_K[G].$$

Viceversa se ogni ideale ambiguo di L ha una base normale intera, allora in particolare $\mathcal{O}_L$ ha una base normale intera, quindi l'estensione è tame.

□

Capitolo 3

Estensioni abeliane

3.1 Teorema di Kronecker-Weber e definizione di conduttore

Definizione 3.1.1 *Un'estensione abeliana globale assoluta è una estensione finita di $\mathbb{Q}$ che sia normale e abbia gruppo di Galois abeliano.*

Per le estensioni abeliane globali assolute vale il teorema di Kronecker-Weber, per la cui dimostrazione si veda [Na 1990].

Teorema 3.1.2 *Sia $L/\mathbb{Q}$ un'estensione abeliana globale assoluta con gruppo di Galios $G = Gal(L/\mathbb{Q})$, allora $L \subset \mathbb{Q}(\zeta_m)$, per qualche m.*

Vediamo che esiste un m minimo per cui $L \subset \mathbb{Q}(\zeta_m)$: supponiamo che $L \subset \mathbb{Q}(\zeta_{m_1})$ e $L \subset \mathbb{Q}(\zeta_{m_2})$, allora $L \subset \mathbb{Q}(\zeta_{m_1}) \cap \mathbb{Q}(\zeta_{m_2})$, ovvero $L \subset \mathbb{Q}(\zeta_d)$, dove $d = (m_1, m_2)$.
Ha senso, a questo punto, definire il conduttore.

Definizione 3.1.3 *Sia $L/\mathbb{Q}$ un'estensione abeliana globale assoluta, diciamo che d è il conduttore di L se d è il minimo intero per cui $L \subset \mathbb{Q}(\zeta_d)$. Indicheremo il conduttore di L con $f(L)$.*

3.2 Teorema di Hilbert-Speiser

Il problema della base normale intera per estensioni abeliane globali assolute è risolto, infatti sappiamo dare una condizione necessaria e sufficiente per l'esistenza; il risulato seguente è noto come Teorema di Hilbert-Speiser.

Teorema 3.2.1 *Sia $L/\mathbb{Q}$ un'estensione abeliana globale assoluta con gruppo di Galois $G = Gal(L/\mathbb{Q})$, sia n il conduttore di L. Sono equivalenti:*

(i) L ha una base normale intera su $\mathbb{Q}$;

(ii) $L/\mathbb{Q}$ *è un'estensione tame;*

(iii) n *è libero da quadrati.*

Prima della dimostrazione premettiamo qualche lemma.

Lemma 3.2.2 *Sia* $L/\mathbb{Q}$ *un'estensione abeliana globale assoluta con gruppo di Galois* $G = Gal(L/\mathbb{Q})$*, sia* n *il conduttore di* L*. Un primo* p *è ramificato tamely in* $L/\mathbb{Q}$ *se e solo se* $p \mid n$ *e* $p^2 \nmid n$*.*

Dimostrazione

Sia $n = p^a m$ con $a \geq 0$ e $p \nmid m$ e sia P un ideale primo di $\mathbb{Q}(\zeta_n)$ che sta sopra p. Se $p \mid n$ e $p^2 \nmid n$, dalla proposizione 1.2.5 segue che $p \nmid e_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(p)$. Così p è ramificato tamely in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ e quindi anche in $L/\mathbb{Q}$. Viceversa se p è ramificato tamely in $L/\mathbb{Q}$, allora $p \mid n$ (infatti se $p \nmid n$, sempre dalla proposizione 1.2.5 segue che p non ramifica in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ quindi neanche in $L/\mathbb{Q}$). Allora $a \geq 1$ e p è ramificato tamely anche in $L\mathbb{Q}(\zeta_{pm})/\mathbb{Q}$ perché l'indice di ramificazione è moltiplicativo in torre. Inoltre, poiché $e_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(p) = \varphi(p^a) = p^{a-1}(p-1)$, abbiamo che $p^{a-1} \mid e_{\mathbb{Q}(\zeta_n)/L\mathbb{Q}(\zeta_{pm})}(p) \mid [\mathbb{Q}(\zeta_n) : L\mathbb{Q}(\zeta_{pm})]$. Sia $M = [L\mathbb{Q}(\zeta_{pm}) : \mathbb{Q}(\zeta_{pm})]$, otteniamo che

$$[\mathbb{Q}(\zeta_n) : L\mathbb{Q}(\zeta_{pm})] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{pm})]/M = \varphi(n)/M\varphi(pm) = p^{a-1}/M.$$

Quindi $p^{a-1} \mid p^{a-1}/M$, cioè $M = 1$ ovvero $L\mathbb{Q}(\zeta_{pm}) = \mathbb{Q}(\zeta_{pm})$. Arriviamo allora all'inclusione $L \subset \mathbb{Q}(\zeta_{pm})$, che implica $n \mid pm$ e $p^2 \nmid n$.

□

Lemma 3.2.3 *(i) Se* $F/\mathbb{Q}$ *è normale e ha una base normale intera e* $L/\mathbb{Q}$ *è normale con* $L \subset F$*, allora anche* $L/\mathbb{Q}$ *ha una base normale intera. Difatti, se i coniugati di* α *formano una base normale di* $F/\mathbb{Q}$*, allora i coniugati di* $Tr_{F/L}(\alpha)$ *formano una base normale intera di* $L/\mathbb{Q}$*.*
(ii) Se $K_i/\mathbb{Q}$ $(i = 1, ..., s)$ *sono linearmente disgiunte ed hanno discriminanti a due a due primi tra loro, sono tutte normali e hanno basi normali intere, allora il loro composto* $K = K_1...K_s$ *ha una base normale intera.*

Dimostrazione

(i) Sia $G = Gal(F/\mathbb{Q})$ e $\{\sigma(\alpha) : \sigma \in G\}$ una base normale intera di F. Sia H il sottogruppo di G che fissa L. Un intero $x = \sum_{\sigma \in G} a_\sigma \sigma(\alpha)$ $(a_\sigma \in \mathbb{Z})$ sta in $\mathcal{O}_L$ se e solo se per ogni $h \in H$ si ha $h(x) = x$, e poiché

$$h(x) = \sum_{\sigma \in G} a_{h^{-1}\sigma}\sigma(\alpha)$$

questo avviene quando $a_{h\sigma} = a_\sigma$ per ogni $h \in H$. Segue che, se $X_1 = H, X_2, ..., X_t$ sono le classi laterali di H in G ($H \triangleleft G$, poiché $L/\mathbb{Q}$ é normale), allora ogni $x \in \mathcal{O}_L$ si puó scrivere come

$$x = a_1 w_1 + ... + a_t w_t$$

con $w_j = \sum_{\sigma \in X_j} \sigma(\alpha)$ e $a_j \in \mathbb{Z}$: cosí $\{w_1, ...w_t\}$ é una base intera di L. Siccome i w_j sono tutti coniugati, essi formano una base normale intera. Inoltre $w_1 = Tr_{F/L}(\alpha)$: abbiamo dunque la tesi.
(ii) Se $w_j^{(i)} (j = 1, ..., [K_i : \mathbb{Q}])$ è una base normale intera di $K_i (i = 1, ..., s)$, allora, per la proposizione 1.4.2, parte (iv), si ha che l'insieme di tutti i prodotti $w_{i_1}^{(1)} ... w_{i_s}^{(s)}$ forma una base intera del composto K. Per vedere che detta base è normale è sufficiente osservare che quest'insieme è invariante per l'azione del gruppo di Galois.

□

Dimostrazione di 3.2.1

(i)⇒(ii) Già visto nel caso generale (Lemma 2.2.1).
(ii)⇒(iii) Ogni primo p di $\mathbb{Q}$ è ramificato tamely, quindi, per il lemma 3.2.2, m è libero da quadrati.
(iii)⇒(i) Verifichiamo per prima cosa che esiste una base normale intera per $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, con m libero da quadrati. Se $n = p$, primo, l'insieme $\zeta_p, \zeta_p^2, ..., \zeta_p^{p-1}$ è una base normale intera di $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. L'esistenza della base normale intera segue dal lemma 3.2.3 parte *(ii)* per $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, con n libero da quadrati, e dalla parte *(i)* dello stesso lemma per $L/\mathbb{Q}$.

□

Dal teorema 3.2.1 segue, ovviamente, che i campi ciclotomici con base normale intera sono $\mathbb{Q}(\zeta_n)$, con n libero da quadrati. Supponiamo che $n = p_1 p_2 ... p_r$, allora una base normale intera di $\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$ è data da $\zeta_{p_i}, ..., \zeta_{p_i}^{p_i - 1}$ e una base normale intera di $\mathbb{Q}(\zeta_n)$, come risulta dalla dimostrazione del lemma 3.2.3 parte *(ii)*, è data da tutti i prodotti $\zeta_{p_1}^{j_1} \zeta_{p_2}^{j_2} ... \zeta_{p_r}^{j_r}$.

Vediamo un altro esempio del teorema appena dimostrato: consideriamo le estensioni quadratiche di $\mathbb{Q}$, cioè le estensioni $L/\mathbb{Q}$ tali che $[L : \mathbb{Q}] = 2$. Esse sono ovviamente estensioni di Galois di $\mathbb{Q}$, con gruppo di Galois abeliano. Inoltre, se $[L : \mathbb{Q}] = 2$, allora $L = \mathbb{Q}(\sqrt{n})$, con $n \in \mathbb{Z}$ e libero da quadrati. Per trovare tra queste le estensioni con base normale intera, basta vedere quali sono quelle tame, considerando la fattorizzazione dei primi esposta nella prossima proposizione, che è un corollario del teorema di Kummer (Teorema 1.2.3).

Proposizione 3.2.4 *Sia $L = \mathbb{Q}(\sqrt{n})$, n libero da quadrati, e $\alpha = \sqrt{n}$.*

(i) Caso $n \equiv 2 \pmod 4$.
Se $p \mid n$, $p\mathcal{O}_L = (p, \alpha)^2$,
se $p \nmid n$,
se $n = c^2$, per un certo $c \in \mathbb{Z}$, $p\mathcal{O}_L = (p, (\alpha - c))(p, (\alpha + c))$,
se $n \neq c^2$ $\forall c \in \mathbb{Z}$, $p\mathcal{O}_L = (p)$.

(ii) Caso $n \equiv 3 \pmod 4$.
Se $p \mid n$, $p\mathcal{O}_L = (p, \alpha)^2$,
se $p \nmid n$, $p \neq 2$,

se $n = c^2$, *per un certo* $c \in \mathbb{Z}$, $p\mathcal{O}_L = (p, (\alpha - c))(p, (\alpha + c))$,
se $n \neq c^2$ $\forall c \in \mathbb{Z}$, $p\mathcal{O}_L = (p)$,
$p = 2$,
$2\mathcal{O}_L = (2, \alpha + 1)^2$.

(iii) Caso $n \equiv 1 \pmod 4$.
Se $p \mid n$, $p\mathcal{O}_L = (p, (\alpha - p)/2)^2$,
se $p \nmid n$, $p \neq 2$,
se $n = c^2$, *per un certo* $c \in \mathbb{Z}$, $p\mathcal{O}_L = P_1P_2$, P_1, P_2, *primi di* $\mathcal{O}_L$,
se $n \neq c^2$ $\forall c \in \mathbb{Z}$, $p\mathcal{O}_L = P$, P *primo di* $\mathcal{O}_L$,
$p = 2$,
se $n \equiv 1 \pmod 8$, $p\mathcal{O}_L = Q_1Q_2$, *con* Q_1, Q_2, *primi di* $\mathcal{O}_L$,
se $n \equiv 5 \pmod 8$, $p\mathcal{O}_L = Q$, Q *primo di* $\mathcal{O}_L$.

In queste estensioni l'unico primo che può essere ramificato wildly è 2, poiché se p è ramificato wildly $(e_{L/\mathbb{Q}}(p), p) \neq 1$. Nel caso di $[L : \mathbb{Q}] = 2$, affinché un primo sia ramificato wildly, $e_{L/\mathbb{Q}}(p) = 2$ e $char(\mathcal{O}_L/P) = 2$, per ogni P primo di $\mathcal{O}_L$ che sta sopra p. L'unica possibilità è quindi $p = 2$. Nel caso di $n \equiv 1 \pmod 4$, il primo 2 è non ramificato, l'estensione è quindi tame.
In entrambi gli altri due casi 2 ha indice di ramificazione uguale a 2, per ogni primo che sta sopra di lui ed è quindi ramificato wildly, sia quando $n \equiv 2 \pmod 4$, sia quando $n \equiv 3 \pmod 4$. Concludendo, gli unici casi di estensioni quadratiche di $\mathbb{Q}$ tame sono per $n \equiv 1 \pmod 4$.

Nel caso delle estensioni quadratiche di $\mathbb{Q}$, è facile calcolare il conduttore: basta usare la formula del conduttore-discriminante, che, per estensioni quadratiche di $\mathbb{Q}$, assume una forma molto semplice. Per la dimostrazione della formula del conduttore-discriminante si veda [Wa 1982].

Teorema(formula del conduttore-discriminante) 3.2.5 *Sia* L *una estensione abeliana di* $\mathbb{Q}$, *con* $X(L)$ *il gruppo di caratteri di Dirichlet associato, allora il discriminante di* L, $disc_{L/\mathbb{Q}}$, *è dato da*

$$\mathrm{disc}_{L/\mathbb{Q}} = (-1)^u \prod_{\chi \in X(L)} f(\chi),$$

dove u *denota il numero di caratteri dispari in* $X(L)$.

Se chiamo $f(L)$ il conduttore di L, vale che

$$f(L) = m.c.m.\{f(\chi) : \chi \in X(L)\}.$$

Infatti $L \subseteq \mathbb{Q}(\zeta_f)$ con $f = f(L)$ (Teorema 3.1.2) e per ogni χ in $X(L)$ vale che $f(\chi) \mid f$. Così $M = m.c.m.\{f(\chi) : \chi \in X(L)\}$ divide f. Siccome tutti i caratteri di $X(L)$ possono essere considerati come caratteri modulo M, allora $L \subseteq Q(\zeta_M)$, cioè $f \mid M$. Segue che $f = M$.
Nel caso di estensioni quadratiche, il gruppo dei caratteri è isomorfo a $\mathbb{Z}/2\mathbb{Z}$, un carattere è l'identità, il suo conduttore è ovviamente 1, il conduttore del campo

coincide, quindi, a meno del segno, col discriminante.
Il discriminante di un'estensione quadratica $L/\mathbb{Q}$, con $L = \mathbb{Q}(\sqrt{n})$, è uguale ad n o $4n$, a seconda che si abbia, rispettivamente, $n \equiv 1 \pmod 4$ oppure no. Ricordando che n è libero da quadrati per ipotesi, si conclude che tutte e sole le estensioni quadratiche di $\mathbb{Q}$ con base normale intera sono del tipo $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$, con $n \equiv 1 \pmod 4$.

3.3 Risultato di Leopoldt

Considerando sempre il caso di estensioni abeliane globali assolute $L/\mathbb{Q}$ con $G = Gal(L/\mathbb{Q})$, n conduttore di L e $\mathcal{O}_L$ l'anello degli interi di L, si ha che L ha una base normale intera su $\mathbb{Q}$ se e solo se $\mathcal{O}_L$ è isomorfo a $\mathbb{Z}[G]$ come $\mathbb{Z}[G]$-modulo. $\mathbb{Z}[G]$ è un ordine di $\mathbb{Q}[G]$. Leopoldt in [Lo 1959] descrive la struttura di $\mathcal{O}_L$ come $\mathbb{Z}[G]$-modulo, determinando un ordine $\mathfrak{A}_{L/\mathbb{Q}}$ dell'anello di gruppo $\mathbb{Q}[G]$ e un elemento T_L tale che $\mathcal{O}_L = \mathfrak{A}_{L/\mathbb{Q}}T_L$. Lettl in [Le 1990] dà una dimostrazione elementare del risultato di Leopoldt. Seguiremo la notazione di Lettl.
Sia X il gruppo dei caratteri di Dirichlet corrispondente a L, che identifichiamo con il gruppo duale di G. Sia $\chi \in \widehat{G}$, definiamo

$$\varepsilon_{\chi,G} = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma \ \in \bar{\mathbb{Q}}[G] \tag{3.1}$$

dove $\overline{\mathbb{Q}}$ è la chiusura algebrica di $\mathbb{Q}$. Valgono le seguenti proprietà:

(i) $\varepsilon_{\chi,G}^2 = \varepsilon_{\chi,G}$,
(ii) $\varepsilon_{\chi,G}\varepsilon_{\psi,G} = 0$ se $\chi \neq \psi$,
(iii) $\varepsilon_{\chi,G}\sigma = \chi(\sigma)\varepsilon_{\chi,G}$,
(iv) $1 = \sum_{\chi\in G^*}\varepsilon_{\chi,G}$.

Gli $\varepsilon_{\chi,G}$ sono chiamati idempotenti ortogonali dell' anello di gruppo $\overline{\mathbb{Q}}[G]$.

Definizione 3.3.1 *Per ogni $n \in \mathbb{N}$, indicando con $\mathbb{P}$ l'insieme dei primi di $\mathbb{Z}$, poniamo*

$$\mathfrak{D}(n) := \left\{ d \in \mathbb{N} \;\middle|\; \left(\prod_{p\in\mathbb{P}\setminus\{2\},p|n} p\right) \middle| d,\ \ d \mid n,\ \ d \not\equiv 2\ (4) \right\}$$

e, se $\nu_p : \mathbb{N} \to \mathbb{N}_0$ denota l'esponente p-adico ($\forall n \in \mathbb{N}\ p^{\nu_p(n)} \mid n$ e $p^{\nu_{p(n)}+1} \nmid n$),

$$q(n) := \prod_{p\in\mathbb{P},\ \nu_p(n)\geq 2} p^{\,\nu_p(n)}.$$

Definizione 3.3.2 *Sia X un gruppo finito di caratteri di Dirichlet, chiamamo $n = m.c.m.\{f_\chi | \chi \in X\}$ e d in $\mathfrak{D}(n)$. Allora*

$$\Phi_d := \{\chi \in X |\, q(f_\chi) = q(d)\}.$$

Sia $d \in \mathfrak{D} = \mathfrak{D}(n)$, dove n è il conduttore di L. Poniamo

$$K_d := K \cap \mathbb{Q}(\zeta_d) \text{ e } \eta_d := \mathrm{Tr}_{\mathbb{Q}(\zeta_d)/K_d}\zeta_d.$$

Se definiamo

$$T_L := \sum_{d\in\mathfrak{D}} \eta_d = \sum_{d\in\mathfrak{D}} \mathrm{Tr}_{\mathbb{Q}(\zeta_d)/K_d}\zeta_d$$

e

$$\varepsilon_d := \sum_{\chi\in\Phi_d} \varepsilon_\chi$$

possiamo enunciare il teorema di Leopoldt.

Teorema 3.3.3 *Sia L un campo di numeri abeliano. Allora*

$$\mathcal{O}_L = \mathfrak{A}_{L/\mathbb{Q}} T_L$$

per $\mathfrak{A}_{L/\mathbb{Q}} = \mathbb{Z}[G][\{\varepsilon_d | d \in \mathfrak{D}\}]$.

3.4 Struttura di modulo di Galois per estensioni relative

In [ByLe 1996] Byott e Lettl generalizzano il risultato di Leopoldt considerando le estensioni di campi di numeri L/K, dove L è abeliano su $\mathbb{Q}$ e K è un campo ciclotomico. Se G è il gruppo di Galois di L/K, l'ordine definito da Leopoldt in questo caso si chiama ordine associato all'estensione L/K ed è dato da

$$\mathcal{A}_{L/K} = \{\alpha \in K[G] | \alpha\mathcal{O}_L \subset \mathcal{O}_L\} \tag{3.2}$$

dove $K[G]$, come sempre, opera sulla struttura additiva di L.
Byott e Lettl dimostrano che, con le ipotesi suddette, $\mathcal{O}_L$ è isomorfo a $\mathcal{A}_{L/K}$ come $\mathcal{A}_{L/K}$-modulo.
Sia L un campo di numeri assoluto abeliano con conduttore n ($L \subset \mathbb{Q}(\zeta_n)$) e K un sottocampo di L con conduttore $m' \mid n$. Per ogni intero $t \in \mathbb{N}$ e M campo di numeri sia $M_t = M \cap \mathbb{Q}(\zeta_t)$. Poniamo

$$m = m' \prod_{p\in\mathbb{P},\ p|n \text{ e } p\nmid m'} p.$$

Se $m \equiv 2 \pmod 4$, $\mathbb{Q}(\zeta_m)$ ha come conduttore $\frac{m}{2}$. L'estensione $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m)$ ha sempre grado $\frac{m}{n}$: infatti $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, per cui $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] = \frac{\varphi(n)}{\varphi(m)}$ e se $n = m' p_1^{e_1} ... p_r^{e_r} p_{r+1}^{e_{r+1}} ... p_s^{e_s}$ e $m = m' p_1 ... p_r$, con $p_i \mid m'$ $\forall i = r+1...n$,

$$\frac{\varphi(n)}{\varphi(m)} = \frac{n}{m};$$

si vede semplicemente sfruttando la definizione della funzione di Eulero.
Sia $\Gamma = Gal(L/L_m) \leq Gal(L/K) = G$.

Sia $\psi \in \Gamma^*$ un carattere di Γ di ordine l, $\mathfrak{G} = Gal(\mathbb{Q}(\zeta_l)/K_l)$, allora, per $\gamma \in \Gamma$, $\psi(\gamma) \in \mathbb{Q}(\zeta_l)$, poiché vale che $(\psi(\gamma))^l = \psi^l(\gamma) = 1$.
Definiamo i caratteri coniugati a ψ, ψ^σ, per $\sigma \in \mathfrak{G}$, con

$$\psi^\sigma(\gamma) := \sigma(\chi(\gamma)).$$

ψ^σ è un carattere, infatti abbiamo che

$$\psi^\sigma(\gamma\eta) = \sigma(\psi(\gamma\eta)) = \sigma(\psi(\gamma))\sigma(\psi(\eta)) = \psi^\sigma(\gamma)\psi^\sigma(\eta).$$

Gli idempotenti di (3.1) diventano

$$\varepsilon_{\psi^\sigma,\Gamma} = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\sigma(\psi(\gamma^{-1}))\gamma \ \in \mathbb{Q}(\zeta_l)[\Gamma].$$

Sia

$$\mathcal{E}_\psi = \sum_{\sigma\in\mathfrak{G}}\varepsilon_{\psi^\sigma,\Gamma} = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\left(\sum_{\sigma\in\mathfrak{G}}\sigma(\psi(\gamma^{-1}))\right)\gamma = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\left(\mathrm{Tr}_{\mathbb{Q}(\zeta_l)/K_l}\psi(\gamma^{-1})\right)\gamma.$$

Poiché $\mathrm{Tr}_{\mathbb{Q}(\zeta_l)/K_l}\psi(\gamma^{-1})$ appartiene a K_l, $\mathcal{E}_\psi \in K_l[\Gamma]$.

Definizione 3.4.1 *Siano ψ e $\chi \in \Gamma^*$, diremo che*

$$\psi \equiv \chi \Leftrightarrow \mathcal{E}_\psi = \mathcal{E}_\chi. \tag{3.3}$$

Si vede che la relazione definita in (3.3) è una relazione di equivalenza, per cui chiameremo $\overline{\Gamma^*} \subset \Gamma^*$ l'insieme dei rappresentanti per le classi in cui Γ^* è diviso dalla relazione (3.3).

Proposizione 3.4.2 *Γ non è ciclico se e solo se $m \equiv 2 \pmod 4$, $8 \mid n$ e $L\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$.*

Dimostrazione

Sia $n = m'p_1^{e_1}...p_r^{e_r}p_{r+1}^{e_{r+1}}...p_s^{e_s}$ e $m = m'p_1...p_r$, con $p_i \mid m' \ \forall i = r+1...n$.
Se $L\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$, si ha che

$$\Gamma = Gal(L/L_m) = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$$

e $|\Gamma| = n/m = p_1^{e_1-1}...p_r^{e_r-1}p_{r+1}^{e_{r+1}}...p_s^{e_s}$.
Se $m \equiv 2 \pmod 4$ e $8 \mid n$, allora Γ è isomorfo ad un sottogruppo H del gruppo $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$ tale che

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^*/H.$$

Poichè nella fattorizzazione di m c'è solo un 2 e $8 \mid n$, sia che $2 \mid m'$, sia che $2 \nmid m'$, H contiene $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, per cui H non può essere ciclico.
Viceversa, se Γ non è ciclico, poiché $\Gamma \cong Gal(L\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m))$ è un quoziente di

$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$, allora $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$ non deve essere ciclico. Affinché non lo sia nella fattorizzazione di n deve comparire almeno una terza potenza di 2, cioè $8 \mid n$ e $m \equiv 2 \pmod 4$. Queste due condizioni non bastano ancora a garantire che Γ non sia ciclico, infatti se la 2-parte di $\frac{n}{m}$ è uguale a 4 e $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m)) \cong \mathbb{Z}/2\mathbb{Z}$, Γ è ciclico. Per evitarlo dobbiamo imporre che $L\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$.

□

Lemma 3.4.3 *Siano L, m, m', n come sopra, se $p_i \neq 2$ per ogni i, allora $L\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$.*

Dimostrazione

Possiamo supporre che $m = p_1...p_k$ e $n = p_1^{a_1}...p_k^{a_k}$, poiché la presenza del fattore m' in m e n o di eventuali fattori di m' in n non cambiano la dimostrazione. Allova vale che

$$\mathbb{Q}(\zeta_n) = \prod_{i=1}^{k} \mathbb{Q}(\zeta_{mp_i^{a_i-1}})$$

e

$$Gal(\mathbb{Q}(\zeta_{mp_i^{a_i-1}})/\mathbb{Q}(\zeta_m)) = \mathbb{Z}/(p_i^{a_i-1})\mathbb{Z}. \tag{3.4}$$

Per $p \neq 2$ il gruppo di Galios in 3.4 è ciclico. Chiaramente si ha che $L \subset \mathbb{Q}(\zeta_n)$, $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$, perciò $L\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$.
Supponiamo, per assurdo, che $L\mathbb{Q}(\zeta_m) \subsetneq \mathbb{Q}(\zeta_n)$, allora per qualche i

$$L(\zeta_{p_i}) \subsetneq \mathbb{Q}(\zeta_{mp_i^{a_i-1}}).$$

Guardando i rispettivi gruppi di Galois si ha

$$Gal(\mathbb{Q}(\zeta_n)/L(\zeta_{p_i})) \supsetneq Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{mp_i^{a_i-1}})).$$

Da questa equazione e da (3.4) segue che $Gal(\mathbb{Q}(\zeta_n)/L(\zeta_{p_i}))$ ha ordine divisibile per p_i, cioè $p_i \mid [\mathbb{Q}(\zeta_{p_1^{a_1}...p_k^{a_k}}) : L\mathbb{Q}(\zeta_{p_i})]$. In più il gruppo di Galois in (3.4) è ciclico; scelgo l'unico sottosruppo di ordine p, allora

$$L(\zeta_{p_i}) \subset \mathbb{Q}(\zeta_{mp_i^{a_i-2}}),$$

cioè

$$L \subset \mathbb{Q}(\zeta_{\frac{n}{p_i}}),$$

che contraddice l'ipotesi che n sia il conduttore di L.

□

Nel caso in cui $m \equiv 2 \pmod 4$ e $8 \mid n$, L_{2m} è un'estensione quadratica di L_m e L/L_{2m} è ciclica. Così, sia $\omega_2 \in \Gamma^*$ l'unico carattere non banale che è banale su $Gal(L/L_{2m})$, gli $\mathcal{E}_\psi$ di prima cambiano in questo modo:

$$E_\psi = \begin{cases} \mathcal{E}_\psi + \mathcal{E}_{\psi\omega_2} & \text{se } \Gamma \text{ non è ciclico e } \psi\omega_2 \text{ hanno ordine pari} \\ \mathcal{E}_\psi & \text{in tutti gli altri casi.} \end{cases}$$

Poniamo inoltre

$$\mathcal{B}_{L/K} = \mathcal{O}_K[G][E_\psi | \psi \in \overline{\Gamma^*}] = \bigoplus_{\psi \in \overline{\Gamma^*}} \mathcal{O}_K[G]E_\psi.$$

Sia $\mathcal{D}(m,n) = \{d \in \mathbb{N} |\ m \mid d \text{ e } d \mid n\}$. Per $t \in \mathcal{D}(m,n)$ sia $\mathcal{R}_t \in (\mathbb{Z}/n\mathbb{Z})^*$ un insieme di rappresentanti per $Gal(K_{\frac{t}{m}}/\mathbb{Q})$, che è un quoziente di $(\mathbb{Z}/n\mathbb{Z})^*$. Definiamo

$$T_{L/K} = \sum_{t \in \mathcal{D}(m,n)} \sum_{\sigma \in \mathcal{R}_t} \mathrm{Tr}_{\mathbb{Q}(\zeta_t)/\mathrm{L_t}} \sigma(\zeta_t).$$

Teorema 3.4.4 *Sia L un campo di numeri abeliano contenente $K = \mathbb{Q}(\zeta_{m'})$. Allora l'ordine associato di $\mathbb{Q}(\zeta_{m'})$ è dato da*

$$\mathcal{A}_{L/\mathbb{Q}(\zeta_{m'})} = \mathcal{B}_{L/\mathbb{Q}(\zeta_{m'})} = \bigoplus_{\psi \in \overline{\Gamma^*}} \mathcal{O}_{\mathbb{Q}(\zeta_{m'})}[G]E_\psi,$$

e $T_{L/\mathbb{Q}(\zeta_{m'})}$ genera $\mathcal{O}_L$ come modulo libero di rango 1 su $\mathcal{A}_{L/\mathbb{Q}(\zeta_{m'})}$. Più esplicitamente abbiamo

$$\mathcal{O}_L = \mathcal{B}_{L/\mathbb{Q}(\zeta_{m'})} T_{L/\mathbb{Q}(\zeta_{m'})} = \bigoplus_{t \in \mathcal{D}(m,n)} \bigoplus_{\sigma \in \mathcal{R}_t} \mathcal{O}_{\mathbb{Q}(\zeta_{m'})}[G]\mathrm{Tr}_{\mathbb{Q}(\zeta_t)/L_t} \sigma(\zeta_t).$$

Il risultato di Leopoldt è un corollario del teorema precedente; basta applicarlo al caso di $K = \mathbb{Q}$, cioè ad $m' = 1$, e la dimostrazione del teorema 3.4.4 è indipendente da quella di Leopoldt. Prima di arrivare al teorema 3.4.4 un passo intermedio è stato fatto da Chan e Lim [ChLi 1993], che hanno dimostrato il seguente teorema:

Teorema 3.4.5 *Siano L e K estensioni ciclotomiche di $\mathbb{Q}$, con $K \subset L$. Allora $\mathcal{O}_L$ è un modulo libero di rango uno sull'ordine associato $\mathcal{A}_{L/K}$.*

Capitolo 4

Applicazioni

4.1 Introduzione

In questa parte definiremo un oggetto che misura, detto in termini non matematici, quanto è distante un'estensione dall'avere una base normale. Le estensioni che cosidereremo sono tra quelle per cui vale il teorema 3.4.4.
Sia quindi L un'estensione abeliana di $\mathbb{Q}$, con conduttore n, $K = \mathbb{Q}(\zeta_{m'})$ e $G = Gal(L/K)$; supporremo inoltre che $\Gamma = Gal(L/L_m)$ sia ciclico, per cui $\mathcal{A}_{L/K} = \bigoplus_{\psi \in \overline{\Gamma^*}} \mathcal{O}_K[G]\mathcal{E}_\psi$. Consideriamo $\mathcal{O}_K[G] \subset \mathcal{A}_{L/K}$; vogliamo calcolare il numero di classi laterali di $\mathcal{O}_K[G]$ in $\mathcal{A}_{L/K}$, cioè

$$[\mathcal{A}_{L/K} : \mathcal{O}_K[G]].$$

Questo indice è finito: infatti $\mathcal{O}_K[G]$ e $\mathcal{A}_{L/K}$ sono due $\mathcal{O}_K$-moduli liberi di rango uguale a $|G|$. Che $\mathcal{O}_K[G]$ sia libero di rango $|G|$ è ovvio; invece per $\mathcal{A}_{L/K}$ c'è qualche precisazione da fare. Dalla struttura di $\mathcal{A}_{L/K}$ data nel teorema 3.4.4 si deduce che è un $\mathcal{O}_K$- modulo libero: infatti $\mathcal{A}_{L/K}$ è una somma diretta di $\mathcal{O}_K[G]$ moltiplicato per degli idempotenti. Per vedere che $\mathcal{A}_{L/K}$ ha rango $|G|$, basta notare che $\mathcal{A}_{L/K}$ è un $\mathcal{O}_K$-ordine di $K[G]$, in altre parole che

$$\mathcal{A}_{L/K}K = K[G],$$

e questo segue dalla definizione di $\mathcal{A}_{L/K}$ in (3.2).

Lemma 4.1.1 *Sia $\{a_1, ..., a_n\}$ una base di $\mathcal{A}_{L/K}$ come $\mathcal{O}_K$-modulo e $\{b_1, ..., b_n\}$ una base $\mathcal{O}_K[G]$, sia inoltre D la matrice che esprime la base $\{b_1, ..., b_n\}$ in termini della base $\{a_1, ..., a_n\}$, allora*

$$[\mathcal{A}_{L/K} : \mathcal{O}_K[G]] = |N_{K/\mathbb{Q}}(\det(D))|.$$

Dimostrazione

Per calcolare l'indice ricordiamo che $\mathcal{A}_{L/K}$ e $\mathcal{O}_K[G]$ sono gruppi abeliani rispetto alla somma, in particolare, quindi, $\mathbb{Z}$-moduli liberi: infatti sono $\mathcal{O}_K$-moduli liberi e $\mathcal{O}_K$ è un modulo libero su $\mathbb{Z}$. Se localizziamo rispetto ad un primo P di $\mathcal{O}_K$ che sta sopra ad un primo p di $\mathbb{Z}$, allora $(\mathcal{O}_K[G])_P = (\mathcal{O}_K)_P[G]$ diventa un modulo libero su un anello ad ideali principali; lo stesso vale per $\mathcal{A}_{L/K}$. Basta dimostrare la formula della tesi nel caso locale poiché

$$[(\mathcal{A}_{L/K})_P : (\mathcal{O}_K[G])_P] = p - \text{parte di } [\mathcal{A}_{L/K} : \mathcal{O}_K[G]].$$

Per verificarlo, consideriamo il quoziente $\mathcal{A}_{L/K}/\mathcal{O}_K[G]$; come gruppo abeliano è una somma diretta di gruppi ciclici e possiamo supporre che ogni addendo sia potenza di un primo, $\mathcal{A}_{L/K}/\mathcal{O}_K[G] = \bigoplus_i \mathbb{Z}/p_i^{c_i}\mathbb{Z}$.
Localizzando si ha che se $p_i \neq p$, allora $(\mathbb{Z}/p_i^{c_i}\mathbb{Z})_p = 0$, altrimenti se $p_i = p$, $(\mathbb{Z}/p^{c_i}\mathbb{Z}) = p^{c_i}$. Dimostriamo ora che nel caso locale la formula è corretta. Supponiamo che $\mathcal{O}_K$ sia ad ideali principali e usiamo il teorema di struttura per moduli su anelli a ideali principali (Teorema 1.12.4). Usando le notazioni del teorema, chiamiamo $A = \mathcal{O}_K$, $M = \mathcal{A}_{L/K}$ e $M' = \mathcal{O}_K[G]$, allora esiste una base di $\mathcal{A}_{L/K}$, $\{e_1, ..., e_n\}$ ed elementi $k_1, ..., k_n$ di $\mathcal{O}_K$ tale che $\{k_1e_1, ..., k_ne_n\}$ è una base di $\mathcal{O}_K[G]$. Allora

$$\mathcal{A}_{L/K}/\mathcal{O}_K[G] \cong \mathcal{O}_K/k_1\mathcal{O}_K \times ... \times \mathcal{O}_K/k_n\mathcal{O}_K.$$

Dalla definizione di norma segue che $|\mathcal{O}_K/k_i\mathcal{O}_K| = N_{K/\mathbb{Q}}(k_i)$. Siccome la norma è moltiplicativa, si ha che $|\mathcal{A}_{L/K}/\mathcal{O}_K[G]| = \prod_{i=1}^n N_{K/\mathbb{Q}}(k_i) = N_{K/\mathbb{Q}}(k_1 \dots k_n)$. In questo caso la matrice D della tesi è un matrice diagonale che ha sulla diagonale gli elementi $k_1, ..., k_n$, per cui $N_{K/\mathbb{Q}}(k_1 \dots k_n) = N_{K/\mathbb{Q}}(\det(D))$.
Inoltre si può notare che il discorso precedente non dipende dalla scelta delle basi di $\mathcal{O}_K[G]$ e $\mathcal{A}_{L/K}$, in quanto se cambio base il determinante cambia per la moltiplicazione di un elemento invertibile, cioè l'indice è lo stesso.

□

Se consideriamo $T_{L/K}$ del teorema 3.4.4 abbiamo che

$$[\mathcal{A}_{L/K} : \mathcal{O}_K[G]] = [\mathcal{A}_{L/K}T_{L/K} : \mathcal{O}_K[G]T_{L/K}] = [\mathcal{O}_L : \mathcal{O}_K[G]T_{L/K}].$$

Ecco che l'ultimo indice misura quanto manca ad $\mathcal{O}_L$ dall'essere isomorfo ad $\mathcal{O}_K[G]T_{L/K}$. Siccome, come vedremo in seguito, se esiste una base normale intera deve essere generata da $T_{L/K}$, l'indice definito sopra dà la stima migliore per misurare la "distanza" da una base normale intera.

Proposizione 4.1.2 *Se L/K è un'estensione tame, allora $\mathcal{A}_{L/K} = \mathcal{O}_K[G]$.*

Dimostrazione

Vale sempre che $\mathcal{O}_K[G] \subset \mathcal{A}_{L/K}$; va dimostrata quindi l'altra inclusione.
Sia P un primo di $\mathcal{O}_K$, tale che $P\mathcal{O}_L = (Q_1...Q_r)^e$, consideriamo

$$\mathcal{O}_{L_P} = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K_P} \cong \prod_{i=1}^{r} \mathcal{O}_{L_{Q_i}}$$

.
Sia $\alpha \in \mathcal{A}_{L/K}$, allora $\alpha\mathcal{O}_L \subset \mathcal{O}_L$, ma vale anche che $\alpha\mathcal{O}_{L_P} \subset \mathcal{O}_{L_P}$. Se L/K è tame, per il teorema 2.3.2 vale che $\mathcal{O}_{L_P}$ è un modulo libero di rango 1 su $\mathcal{O}_{K_P}[G]$, cioè esiste $z \in \mathcal{O}_{L_P}$ tale che $\mathcal{O}_{L_P} \cong \mathcal{O}_{K_P}[G]z$. Quindi $\alpha z \in \mathcal{O}_{K_P}[G]z$ e, poiché z non può essere un divisore di zero in quanto genera $\mathcal{O}_{L_P}$ come $\mathcal{O}_{K_P}[G]$-modulo, $\alpha \in \mathcal{O}_{K_P}[G]$. Ma $\alpha \in K[G]$, quindi $\alpha \in K[G] \cap \mathcal{O}_{K_P}[G] = (K \cap \mathcal{O}_{K_P})[G]$. Gli elementi di $(K \cap \mathcal{O}_{K_P})[G]$ sono gli elementi di K con valutazione P-adica maggiore o uguale a zero, cioè gli elementi dell'anello di valutazione di K con la valutazione P-adica. Lo stesso ragionamento si può fare per ogni primo $P \in \mathcal{O}_K$, per cui si ottiene che $\alpha \in R[G]$, dove R è l'intersezione di tutti gli anelli di valutazione di K, ma per un teorema di algebra commutativa ([AtMD 1969]) $R = \mathcal{O}_K$. Segue che $\alpha \in \mathcal{O}_K[G]$, cioè la tesi.

□

Dimostreremo ora che l'essere tame per le estensioni considerate nel teorema 3.4.4 è una condizione necessaria e sufficiente per l'esistenza di una base normale intera.

Teorema 4.1.3 *Sia L un'estensione abeliana di $\mathbb{Q}$ con $G = Gal(L/K)$ e $K = \mathbb{Q}(\zeta_{m'})$, $K \subset L$, allora L/K ha una base normale intera se e solo se L/K è tame.*

Dimostrazione

Se L/K ha una base normale intera, L/K è tame (Lemma 2.2.1).
Viceversa supponiamo che L/K sia tame, allora, per la proposizione 4.1.2 vale che $\mathcal{A}_{L/K} = \mathcal{O}_K[G]$. Il teorema 3.4.4 mi dice che esiste $T_{L/K} \in \mathcal{O}_L$ tale che $\mathcal{O}_L = \mathcal{A}_{L/K}T_{L/K}$ come $\mathcal{A}_{L/K}$-modulo, per cui, nel caso tame

$$\mathcal{O}_L = \mathcal{A}_{L/K}T_{L/K} = \mathcal{O}_K[G]T_{L/K},$$

come $\mathcal{A}_{L/K}$-modulo, cioè come $\mathcal{O}_K[G]$-modulo: quindi $T_{L/K}$ genera una base normale intera di L/K.

□

Abbiamo quindi trovato un insieme di estensioni per cui la ramificazione moderata è sufficiente per l'esistenza di una base normale intera, le estensioni L/K con L abeliana su $\mathbb{Q}$ e $K = \mathbb{Q}(\zeta_{m'})$. Si vede che l'indice definito sopra è la scelta migliore: infatti se esiste una base normale intera, l'estensione deve essere

tame e $\mathcal{A}_{L/K} = \mathcal{O}_K[G]$, quindi il generatore della base normale intera coincide col generatore di $\mathcal{O}_L$ come $\mathcal{A}_{L/K}$-modulo, cioè è $T_{L/K}$ del teorema 3.4.4.

Se riuscissimo a togliere l'ipotesi che L sia abeliana su $\mathbb{Q}$ avremmo trovato un analogo del teorema di Hilbert-Speiser, cioè avremmo trovato che tutte le estensioni tame abeliane di un campo ciclotomico hanno una base normale intera. Questo è falso perché vale il seguente risultato:

Teorema[GrReRuSr 1999] 4.1.4 *Tra tutti i campi di numeri, $\mathbb{Q}$ è l'unico per cui ogni estensione finita abeliana e tame ha una base normale intera.*

4.2 Un esempio

Vediamo ora di applicare il risultato di Byott e Lettl ad un caso in cui una base normale intera esiste per calcolarla esplicitamente. Sia $K = \mathbb{Q}(\zeta_5)$ e $L = \mathbb{Q}(\zeta_{15})$, L/K è un'estensione tame: l' unico primo che ramifica è 3 che ha indice di ramificazione 2, che è ovviamente primo con la caratteristica del campo residuo. Quindi una base normale intera esiste e sarà generata da $T_{L/K}$ del teorema 3.4.4. Con le notazioni di Byott e Lettl in questo caso $n = 15$, $m = 5 \cdot 3 = 15$, per cui

$$L_m = L \cap \mathbb{Q}(\zeta_m) = L = \mathbb{Q}(\zeta_m).$$

Allora

$$\Gamma = Gal(L/L_m) = \{\mathrm{id}\} \quad \text{e} \quad \Gamma^* = \{id\}.$$

L'unico carattere è i'identità per cui l'unico idempotente da calcolare è

$$\mathcal{E}_{\mathrm{id}} = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \left(\sum_{\sigma \in \mathfrak{G}} \sigma(\mathrm{id}(\gamma^{-1})) \right) \gamma,$$

dove $\mathfrak{G} = Gal(\mathbb{Q}/\mathbb{Q})$ e id è il carattere tale che $\mathrm{id}(\gamma) = 1 \ \forall \gamma \in \Gamma$, per cui si ha

$$\mathcal{E}_{\mathrm{id}} = \mathrm{id}.$$

In questo caso $\mathcal{A}_{L/K} = \mathcal{O}_K[G]$ per cui $\mathcal{O}_L \cong \mathcal{O}_K[G]T_{L/K}$; per trovare una base normale intera basta calcolare $T_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_5)}$.

$$G = Gal(\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_5)) \cong Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} = \{\mathrm{id}, g\},$$

dove $g(\zeta_5) = \zeta_5$ e $g(\zeta_3) = \zeta_3^2$. Siccome $\zeta_{15}^3 = \zeta_5$ e $\zeta_{15}^5 = \zeta_3$, abbiamo $g(\zeta_{15}) = \zeta_{15}^k$ con k che verifica

$$\begin{cases} k \equiv 2 \pmod 3 \\ k \equiv 1 \pmod 5), \end{cases}$$

cioè $k \equiv 11 \pmod{15}$ e $g(\zeta_{15}) = \zeta_{15}^{11}$.
Poiché in questo caso $\mathcal{D}(m,n) = \mathcal{D}(15,15) = \{15\}$ e $L_{15} = L \cap \mathbb{Q}(\zeta_{15}) = L = \mathbb{Q}(\zeta_{15})$, $T_{L/K}$ del teorema 3.4.4 diventa

$$T_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_5)} = \sum_{\sigma \in \mathcal{R}_{15}} \sigma(\zeta_{15}).$$

$\mathcal{R}_{15}$ è un insieme di rappresentanti per $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ come quoziente del gruppo $Gal(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$, come rappresentanti scegliamo $\{\tau_1, \tau_2, \tau_3, \tau_4\}$, tali che

$$\begin{aligned}\tau_1(\zeta_{15}) &= \zeta_{15}\\ \tau_2(\zeta_{15}) &= \zeta_3\zeta_5^2\\ \tau_3(\zeta_{15}) &= \zeta_3\zeta_5^3\\ \tau_4(\zeta_{15}) &= \zeta_3\zeta_5^4.\end{aligned}$$

Perciò $T_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_5)} = T = \zeta_{15}(1+\zeta_5+\zeta_5^2+\zeta_5^3) = -\zeta_3\zeta_5\zeta_5^4 = -\zeta_3$. Siccome $g(T) = -\zeta_3^2$ una base normale intera di $\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_5)$ è data da $\{-\zeta_3, -\zeta_3^2\}$.

4.3 $K = \mathbb{Q}(\zeta_q)$ e $L = \mathbb{Q}(\zeta_{qp^2})$, p e q primi dispari distinti

Nel caso di $K = \mathbb{Q}(\zeta_q)$ e $L = \mathbb{Q}(\zeta_{qp^2})$, con p e q entrambi diversi da 2, non abbiamo una base normale perché il primo p non è ramificato tamely. Vediamo di calcolare l'indice in questo caso. Applicando il teorema 3.4.4 si ha

$$\mathcal{A}_{L/K} = \bigoplus_{\psi\in\overline{\Gamma^*}} \mathbb{Z}[\zeta_q][G]\mathcal{E}_\psi.$$

Con le notazioni del teorema 3.4.4 abbiamo che

$$G = Gal(\mathbb{Q}(\zeta_{qp^2})/\mathbb{Q}(\zeta_q)) = \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/(p-1)\mathbb{Z},$$

$n = qp^2$, $m = qp$. Inoltre

$$\Gamma \cong Gal(L/L_m) \cong Gal(L/\mathbb{Q}(\zeta_{pq})) \cong \mathbb{Z}/p\mathbb{Z} = \{\mathrm{id}, \gamma, ..., \gamma^{p-1}\},$$

per cui

$$\Gamma \cong \Gamma^* = \{\mathrm{id}, \psi, ..., \psi^{p-1}\}.$$

Vediamo quali tra i caratteri di Γ sono equivalenti secondo la definizione 3.4.1. L'identità è di ordine 1, per cui $\mathfrak{G} = Gal(\mathbb{Q}/\mathbb{Q}) = \{\mathrm{id}\}$, allora

$$\mathcal{E}_{\mathrm{id}} = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\left(\sum_{\sigma\in\mathfrak{G}}\sigma(\mathrm{id}(\gamma^{-1}))\right)\gamma = \frac{1}{p}(\mathrm{id}+\gamma+...+\gamma^{p-1}).$$

Tutti gli altri caratteri hanno ordine p, allora per questi caratteri il gruppo $\mathfrak{G} = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)\cap\mathbb{Q}(\zeta_q)) = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Sia ψ il generatore di Γ^*, esso ha ordine p; abbiamo che

$$\mathcal{E}_\psi = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\left(\sum_{\sigma\in\mathfrak{G}}\sigma(\psi(\gamma^{-1}))\right)\gamma = \frac{1}{p}\sum_{\gamma\in\Gamma}\left(\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\psi(\gamma^{-1}))\right)\gamma.$$

Per $\gamma = \mathrm{id}$, $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\psi(\mathrm{id}) = p-1$.
Per $\gamma \neq \mathrm{id}$, $\psi(\gamma^{-1})$ è una radice p-esima di uno, e non può essere 1 perché

se lo fosse avremmo che $\psi(\gamma^{-i}) = 1\ \forall i = 1, ...p-1$, (tutti i $\gamma \in \Gamma$ diversi dall'identità sono generatori), cioè ψ dovrebbe essere l'identità, che è assurdo. Quindi $\psi(\gamma^{-1}) = \zeta_p$.

Ma

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} = \zeta_p + \zeta_p^2 + ... + \zeta_p^{p-1} = -1,$$

per cui $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\psi(\gamma^{-1}) = -1$.
In conclusione

$$\mathcal{E}_\psi = \frac{1}{p}((p-1)\mathrm{id} - \gamma - \gamma^2 - ... - \gamma^{p-1}).$$

Inoltre è ovvio che $\mathcal{E}_\psi = \mathcal{E}_{\psi^i}$, $\forall i = 1, ..., p-1$, quindi la relazione di equivalenza 3.4.1 divide Γ^* in due classi, per le quali prendiamo come rappresentante rispettivamente ψ e l'identità.

$$G = \{\mathrm{id}, \gamma, ..., \gamma^{p-1}, \lambda, ..., \lambda\gamma^{p-1}, ..., \lambda^{p-2}, ..., \lambda^{p-2}\gamma^{p-1}\}$$

con $\lambda^{p-1} = 1$. Allora si ha che

$$\begin{aligned}
&\mathcal{E}_{\mathrm{id}}\mathrm{id} = \mathcal{E}_{\mathrm{id}} \\
&\mathcal{E}_{\mathrm{id}}\gamma = \mathcal{E}_{\mathrm{id}} \\
&\vdots \\
&\mathcal{E}_{\mathrm{id}}\gamma^{p-1} = \mathcal{E}_{\mathrm{id}}.
\end{aligned}$$

Cioè $\mathcal{E}_{id}$ moltiplicato per il sottogruppo generato da γ ha rango 1 come $\mathcal{O}_K$-modulo, quindi per base di $\mathcal{A}_{L/K}$ scegliamo tra gli elementi sopra elencati il primo.
Se moltiplichiamo per $\lambda^i\gamma^j$per $j = 0, ..., p-1$ troviamo ancora un rango 1, infatti

$$\begin{aligned}
&\mathcal{E}_{\mathrm{id}}\lambda^i\mathrm{id} = \mathcal{E}_{\mathrm{id}}\lambda^i \\
&\mathcal{E}_{\mathrm{id}}\lambda^i\gamma = \mathcal{E}_{\mathrm{id}}\lambda^i \\
&\vdots \\
&\mathcal{E}_{\mathrm{id}}\lambda^i\gamma^{p-1} = \mathcal{E}_{\mathrm{id}}\lambda^i.
\end{aligned}$$

Per ognuno di questi insiemi, per ogni $i = 0, ..., p-2$, scegliamo il primo elemento. Quindi $\mathcal{E}_{\mathrm{id}}$ moltiplicato per gli elementi del gruppo G ha rango $p-1$; infatti gli elementi scelti per formare la base sono indipedenti fra loro, differiscono per la moltiplicazione di λ^k. Vediamo ora che succede moltiplicando gli elementi di G per $\mathcal{E}_\psi$:

$$\begin{aligned}
&\mathcal{E}_\psi\mathrm{id} = \tfrac{1}{p}((p-1)\mathrm{id} - \gamma - \gamma^2 - ... - \gamma^{p-1}) \\
&\mathcal{E}_\psi\gamma = \tfrac{1}{p}((p-1)\gamma - \gamma^2 - \gamma^3 ... - \mathrm{id}) \\
&\vdots \\
&\mathcal{E}_\psi\gamma^{p-1} = \tfrac{1}{p}((p-1)\gamma^{p-1} - \mathrm{id} - \gamma ... - \gamma^{p-2}).
\end{aligned}$$

Per vedere il rango basta vedere il rango della matrice $p \times p$

$$\mathbf{M} = \frac{1}{p}\begin{pmatrix} p-1 & -1 & -1 & \dots & -1 \\ -1 & p-1 & -1 & \dots & -1 \\ -1 & -1 & p-1 & \dots & -1 \\ & \ddots & \ddots & \ddots & \\ -1 & -1 & -1 & \dots & p-1 \end{pmatrix}.$$

$\mathbf{M}$ è la matrice che esprime gli $\mathcal{E}_\psi\gamma^j$ in termini dei γ^j. La matrice $\mathbf{M}$ ha rango $p-1$, infatti la dimensione del Ker$\mathbf{M} = 1$. Scegliamo quindi $p-1$ tra gli $\mathcal{E}_\psi\gamma^j$ per la base; essendo la scelta indifferente, poiché sono elementi i cui coefficienti hanno somma 0, scegliamo i primi $p-1$.
Se consideriamo gli $\mathcal{E}_\psi\lambda\gamma^j$ in termini dei $\lambda\gamma^j$ troviamo la stessa matrice $\mathbf{M}$ e ne scegliamo $p-1$ per la base; e lo stesso discorso vale per gli $\mathcal{E}_\psi\lambda^i\gamma^j$ per ogni i. Si vede che tutti gli elementi scelti sono indipendenti. In conclusione, considerando anche $\mathcal{E}_{\mathrm{id}}$, si trova un rango pari a

$$(p-1)^2 + p - 1 = p^2 - p = p(p-1) = |G|.$$

Ricapitolando, una base di $\mathcal{A}_{L/K}$ è data da

$$\begin{aligned}
&\mathcal{E}_{\mathrm{id}} = \tfrac{1}{p}(\mathrm{id} + \gamma + ... + \gamma^{p-1}).\\
&\mathcal{E}_{\mathrm{id}}\lambda\mathrm{id} = \tfrac{1}{p}\lambda(\mathrm{id} + \gamma + ... + \gamma^{p-1})\\
&\vdots\\
&\mathcal{E}_{\mathrm{id}}\lambda^{p-2}\mathrm{id} = \tfrac{1}{p}\lambda^{p-2}(\mathrm{id} + \gamma + ... + \gamma^{p-1})\\
&\mathcal{E}_\psi\mathrm{id} = \tfrac{1}{p}((p-1)\mathrm{id} - \gamma - \gamma^2 - ... - \gamma^{p-1})\\
&\mathcal{E}_\psi\gamma = \tfrac{1}{p}((p-1)\gamma - \gamma^2 - \gamma^3 ... - \mathrm{id})\\
&\vdots\\
&\mathcal{E}_\psi\gamma^{p-2} = \tfrac{1}{p}((p-1)\gamma^{p-2} - \gamma^{p-1} - \mathrm{id} - ... - \gamma^{p-3}).\\
&\vdots\\
&\mathcal{E}_\psi\lambda^{p-1} = \tfrac{1}{p}\lambda^{p-1}((p-1)\mathrm{id} - \gamma - \gamma^2 - ... - \gamma^{p-1})\\
&\mathcal{E}_\psi\lambda^{p-1}\gamma = \tfrac{1}{p}\lambda^{p-1}((p-1)\gamma - \gamma^2 - \gamma^3 ... - \mathrm{id})\\
&\vdots\\
&\mathcal{E}_\psi\lambda^{p-1}\gamma^{p-2} = \tfrac{1}{p}\lambda^{p-1}((p-1)\gamma^{p-2} - \gamma^{p-1} - \mathrm{id} - ... - \gamma^{p-3}).
\end{aligned}$$

Consideriamo ora la matrice $\mathbf{D}$, che esprime la base di $\mathcal{A}_{L/K}$ in termini della base di $\mathcal{O}_K[G]$; vista l'espressione della base di $\mathcal{A}_{L/K}$ si vede che $\mathbf{D}$ è una matrice a blocchi, in particolare è nulla dappertutto tranne sulla diagonale, dove ci sono

i $p-1$ blocchi $\mathbf{D_j}$, $j=1,...,p-1$, ognuno di $p\times p$ elementi e

$$\mathbf{D_j}=\frac{1}{p}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1\\ p-1 & -1 & -1 & \dots & -1 & -1\\ -1 & p-1 & -1 & \dots & -1 & -1\\ \vdots & & \ddots & & \vdots & \vdots\\ -1 & -1 & \dots & p-1 & -1 & -1\\ -1 & -1 & \dots & -1 & p-1 & -1 \end{pmatrix}.$$

Si vede, sommmando la prima riga ad ognuna delle altre righe, dalla seconda all'ultima, che il determinante di $\mathbf{D_j}$ è $\frac{p^{p-1}}{p^p}=\frac{1}{p}$, per cui

$$\det\mathbf{D}=(\det\mathbf{D_j})^{p-1}=\frac{1}{p^{p-1}}.$$

Il determinante della matrice inversa di $\mathbf{D}$ è p^{p-1}; per calcolare l'indice basta calcolare la norma:

$$[\mathcal{A}_{L/K}:\mathcal{O}_K[G]]=\mathrm{N}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(p^{p-1})=p^{(p-1)(q-1)}.$$

4.4 Caso L/K con $K=\mathbb{Q}(\zeta_q)$ e L con conduttore p^2q

In questo caso (supporemo sempre che p e q siano primi distinti e diversi da 2) con le notazioni del teorema 3.4.4 $m=qp$ e $n=p^2q$. Consideriamo vari casi:

(i) Se $L\subset\mathbb{Q}(\zeta_m)$, allora abbiamo un assurdo, perché il conduttore di L è n.

(ii) Se $\mathbb{Q}(\zeta_m)\subset L$, allora $\mathbb{Q}(\zeta_m)\cap L=\mathbb{Q}(\zeta_m)$.
Siccome $[\mathbb{Q}(\zeta_{p^2q}):\mathbb{Q}(\zeta_{pq})]=p$ e L è un campo intermedio tra $\mathbb{Q}(\zeta_{pq})$ e $\mathbb{Q}(\zeta_{p^2q})$, o $L=\mathbb{Q}(\zeta_m)$ e questo non è possibile per l'ipotesi sul conduttore, o $L=\mathbb{Q}(\zeta_{p^2q})$. Questo è il caso discusso nel paragrafo precedente e l'indice è $p^{(p-1)(q-1)}$.

(iii) Se $\mathbb{Q}(\zeta_m)\not\subset L$, ci sono due casi: o $L_m=\mathbb{Q}(\zeta_q)$ oppure $L_m\neq\mathbb{Q}(\zeta_q)$. Nel primo caso $G=Gal(L/\mathbb{Q}(\zeta_q))=\Gamma$. Dal lemma 3.4.3 segue che $L\mathbb{Q}(\zeta_{pq})=\mathbb{Q}(\zeta_{p^2q})$, quindi, siccome abbiamo supposto che $L_m=L\cap\mathbb{Q}(\zeta_{pq})=\mathbb{Q}(\zeta_q)$, $[L:\mathbb{Q}(\zeta_q)]=[\mathbb{Q}(\zeta_{p^2q}):\mathbb{Q}(\zeta_{pq})]=p$; $G=Gal(L/\mathbb{Q}(\zeta_q))\cong\mathbb{Z}/p\mathbb{Z}$.
Siano

$$\Gamma=G=\{\mathrm{id},\gamma,\dots,\gamma^{p-1}\}\ \text{ e }\ \Gamma^*=\{\mathrm{id},\psi,\dots,\psi^{p-1}\}.$$

Per calcolare le classi di equivalenza in Γ^* e vedere l'espressione di $\mathcal{E}_{\mathrm{id}}$ e $\mathcal{E}_\psi$ basta ripetere il ragionamento esposto nel paragrafo 4.3. Quindi, come prima, gli unici caratteri da considerare sono id e ψ, e vale che

$$\mathcal{E}_{\mathrm{id}}=\tfrac{1}{p}(1+\gamma+\ldots+\gamma^{p-1})$$
$$\mathcal{E}_\psi=\tfrac{1}{p}((p-1)\mathrm{id}-\gamma-\ldots-\gamma^{p-1}).$$

A differenza di prima $\mathcal{E}_{\mathrm{id}}$ e $\mathcal{E}_\psi$ vanno ora moltiplicati solo per il sottogruppo generato da γ, perché in questo caso esso coincide con G.
Con gli stessi conti del paragrafo 4.3 si vede che $\mathcal{E}_{\mathrm{id}}$ moltiplicato per gli elementi di G dà rango 1 e $\mathcal{E}_\psi$ dà rango $p-1$. La matrice che rappresenta la base di $\mathcal{A}_{L/K}$ è:

$$\mathbf{D_j} = \frac{1}{p}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ p-1 & -1 & -1 & \dots & -1 \\ -1 & p-1 & -1 & \dots & -1 \\ -1 & -1 & p-1 & \dots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \dots & p-1 \end{pmatrix}.$$

L'indice, la norma dell'inverso del determinante di $\mathbf{D_j}$, è uguale a $p^{(q-1)}$.
Rimane da vedere il caso in cui $L_m \neq \mathbb{Q}(\zeta_{pq})$, cioè il caso in cui il grado $[L_m : \mathbb{Q}(\zeta_q)] > 1$. In questo caso il gruppo $\Gamma = Gal(L/L_m)$ è isomorfo al gruppo $Gal(\mathbb{Q}(\zeta_{p^2q})/\mathbb{Q}(\zeta_{pq}) \cong \mathbb{Z}/\,p\mathbb{Z}$. $G = Gal(L/\mathbb{Q}(\zeta_q))$ è ciclico, perché quoziente di $Gal(\mathbb{Q}(\zeta_{p^2q})/\mathbb{Q}(\zeta_q))$ che è ciclico e ha ordine multiplo di p, perché Γ è un suo sottogruppo. Supponiamo quindi che $[L : \mathbb{Q}(\zeta_q)] = p\,d$. Se

$$\Gamma = \{\mathrm{id}, \gamma, \dots, \gamma^{\,p-1}\} \ \text{ e } \ \Gamma^* = \{\mathrm{id}, \psi, \dots, \psi^{\,p-1}\}$$

allora

$$G = \{\mathrm{id}, \gamma, \dots, \gamma^{\,p-1}, \lambda, \lambda\gamma, \dots, \lambda\gamma^{\,p-1}, \dots, \lambda^{\,d-1}, \lambda^{\,d-1}\gamma, \dots, \lambda^{\,d-1}\gamma^{\,p-1}\}.$$

Come nel caso percedente c'è da considerare solo $\mathcal{E}_{\mathrm{id}}$ e $\mathcal{E}_\psi$, che hanno la stessa struttura di prima, dato che Γ è lo stesso, quindi

$$\begin{aligned} \mathcal{E}_{\mathrm{id}} &= \tfrac{1}{p}(1 + \gamma + \ldots + \gamma^{p-1}) \\ \mathcal{E}_\psi &= \tfrac{1}{p}((p-1)\mathrm{id} - \gamma - \ldots - \gamma^{p-1}). \end{aligned}$$

Per trovare la base di $\mathcal{A}_{L/K}$, basta modificare di poco i risultati di prima: infatti $\mathcal{E}_{\mathrm{id}}$ moltiplicato per gli elementi del sottogruppo generato da γ dà un rango 1 e anche moltiplicato per gli elementi $\{\lambda^j, \lambda^j\gamma, \dots, \lambda^j\gamma^{\,p-1}\}$ dà un rango 1 per ogni j, quindi $\mathcal{E}_{\mathrm{id}}$ dà rango d. Per $\mathcal{E}_\psi$ il discorso è analogo: $\mathcal{E}_\psi$ moltiplicato per gli elementi del sottogruppo generato da γ dà rango $p-1$ e anche moltiplicato per gli elementi $\{\lambda^j, \lambda^j\gamma, \dots, \lambda^j\gamma^{\,p-1}\}$ dà un rango $p-1$ per ogni j, quindi $\mathcal{E}_\psi$ dà rango $d(\,p-1)$. La matrice che rappresenta la base di $\mathcal{A}_{L/K}$ in termini degli elementi del gruppo G è una matrice nulla tranne d blocchi $p \times p$ sulla diagonale, ogni blocco uguale a $\mathbf{D_j}$. L'indice, quindi, in questo caso è $p^{\,d(q-1)}$.

In conclusione nel caso in cui L sia un'estensione abeliana di $\mathbb{Q}$ con conduttore $p\,q^2$, $K = \mathbb{Q}(\zeta_q)$ l'indice è

$$p^{\,[L_m:\mathbb{Q}(\zeta_q)](q-1)} = p^{\,[L_m:\mathbb{Q}]}$$

Ripercorrendo i conti svolti si nota che $K = \mathbb{Q}(\zeta_q)$ non è stato usato appieno: in particolare abbiamo usato il fatto che q fosse primo solo per calcolare la norma; in realtà il ragionamento precedente vale ugualmente fino al calcolo della norma se al posto di q mettiamo un intero m', tale che $(m', 2) = 1$ e $(m', p) = 1$. In questo caso infatti $n = p^2 m'$, $m = p\, m'$ e i conti fatti si ripetono identici: il calcolo dei gruppi di Galois intermedi dipende solo dal fatto che q sia primo con p e diverso da 2 , q non compare in questi calcoli perchè il fattore q è anche in n. Anche nel calcolo di $\mathfrak{G}$ per $\mathcal{E}_{\mathrm{id}}$ e $\mathcal{E}_\psi$ si usano solo queste proprietà di q, infatti $\mathfrak{G} = Gal(\mathbb{Q}(\zeta_l)/K \cap \mathbb{Q}(\zeta_l))$ per $\psi \in \Gamma^*$ di ordine l. Gli ordini possibili di ψ sono 1 oppure p ($\Gamma \cong \mathbb{Z}/p\mathbb{Z}$), per $l = 1$ si ha che $\mathfrak{G} = Gal(\mathbb{Q}/\mathbb{Q})$, per $l = p$ vale che $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{m'}) \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ e $\mathfrak{G} = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Inoltre nel calcolo della norma la differenza è minima: il risultato è

$$[\mathcal{A}_{L/\mathbb{Q}(\zeta_{m'})} : \mathcal{O}_{\mathbb{Q}(\zeta_{m'})}[G]] = \mathrm{N}_{\mathbb{Q}(\zeta_{m'})/\mathbb{Q}}(p^{[L_m:\mathbb{Q}(\zeta_{m'})]}) = p^{[L_m:\mathbb{Q}]}.$$

4.5 Composto

Vediamo ora come cambia l'indice se L è il composto di due estensioni di K, L_1 e L_2 tali che $G_i = Gal(L_i/K)$, $G = Gal(L/K) = G_1 \times G_2$ per le quali valga $\mathcal{O}_L = \mathcal{O}_{L_1} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}$.

Lemma 1 *Con le ipotesi suddette vale che* $\mathcal{A}_{L/K} \cong \mathcal{A}_{L_1/K} \otimes_{\mathcal{O}_K} \mathcal{A}_{L_2/K}$.

Dimostrazione

Se $G = Gal(L/K) = G_1 \times G_2$, allora ovviamente $K[G] \cong K[G_1] \otimes_K K[G_2]$, per cui ogni $\alpha \in K[G]$ si può scrivere come $\alpha_1 \otimes \alpha_2$, con $\alpha_1 \in K[G_1]$ e $\alpha_2 \in K[G_2]$. Sia α in $\mathcal{A}_{L/K}$, allora $\alpha\mathcal{O}_L \subset \mathcal{O}_L$, cioè

$$(\alpha_1 \otimes \alpha_2)\mathcal{O}_L = (\alpha_1 \otimes \alpha_2)(\mathcal{O}_{L_1} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}) \subset \mathcal{O}_L,$$

ovvero $\alpha_1\mathcal{O}_{L_1} \subset \mathcal{O}_{L_1}$ e $\alpha_2\mathcal{O}_{L_2} \subset \mathcal{O}_{L_2}$, quindi $\alpha \in \mathcal{A}_{L/K_1} \otimes_{\mathcal{O}_K} \mathcal{A}_{L/K_2}$. L'inclusione opposta è ovvia.

□

Nel caso in cui $K = \mathbb{Q}(\zeta_q)$, $L_1 = \mathbb{Q}(\zeta_{p^2 q})$, $L_2 = \mathbb{Q}(\zeta_{r^2 q})$ con p, q, r primi diversi da 2, e $L = L_1 L_2 = \mathbb{Q}(\zeta_{q\,p^2\,r^2})$, sono soddisfatte le ipotesi del lemma, per cui $\mathcal{A}_{\mathbb{Q}(\zeta_{q\,p^2\,r^2})/\mathbb{Q}(\zeta_q)} \cong \mathcal{A}_{\mathbb{Q}(\zeta_{p^2 q})/\mathbb{Q}(\zeta_q)} \otimes_{\mathcal{O}_{\mathbb{Q}(\zeta_q)}} \mathcal{A}_{\mathbb{Q}(\zeta_{r^2 q})/\mathbb{Q}(\zeta_q)}$. Ricordiamo che $G_1 \cong \mathbb{Z}/pZ \times \mathbb{Z}/(p-1)\mathbb{Z}$ e $G_2 \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/(r-1)\mathbb{Z}$.
Anche in questo caso vogliamo calcolare l'indice. Sappiamo intanto che

$$[\mathcal{A}_{L_i/K} : \mathcal{O}_K[G_i]] = \mathrm{N}_{K/\mathbb{Q}}(\det(A_i^{-1}))$$

dove A_i è la matrice che ha per righe i coefficienti della base di $\mathcal{A}_{L_i/K}$ in termini degli elementi di G_i. Allo stesso modo per $\mathcal{A}_{L/K}$ vale che

$$[\mathcal{A}_{L/K} : \mathcal{O}_K[G]] = \mathrm{N}_{K/\mathbb{Q}}(\det(A^{-1}))$$

dove A è la matrice che ha per righe i coefficienti della base di $\mathcal{A}_{L/K}$ in termini degli elementi di G. In sostanza ci siamo ridotti ad un problema di algebra lineare, calcolare cioè la matrice A ed il suo determinante. Sia $\{\alpha_i\}_{i=1,\dots,n}$ una base di $\mathcal{A}_{L_1/K}$ e $\{\beta_j\}_{j=1,\dots,m}$ una base di $\mathcal{A}_{L_2/K}$, allora una base di $\mathcal{A}_{L/K}$ è data da $\{\alpha_i \otimes \beta_j\}_{(i=1,\dots,n,j=1,..,m)}$.
È un semplice esercizio di algebra lineare vedere che la matrice che ha per righe i coefficienti di $\{\alpha_i \otimes \beta_j\}$ in termini degli elementi di $G_1 \times G_2$ è quella che viene chiamata $A_1 \otimes A_2$, cioè

$$A_1 \otimes A_2 = \begin{pmatrix} C_{11} & \dots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \dots & C_{nn} \end{pmatrix}$$

dove C_{ij} è una matrice $m \times m$, $C_{ij} = (\mathrm{ent}_{ij}(A_1))A_2$; $\mathrm{ent}_{ij}(A_1)$ significa l'entrata (i, j) della matrice A_1.
Il determinante di A si riesce ad esprimere in termini dei determinanti di A_1 e A_2, vale infatti [AdWe 1992] che

$$\det(A_1 \otimes A_2) = (\det(A_1))^m (\det(A_2))^n.$$

Quindi

$$\det(A^{-1}) = (p^{p-1})^{r(r-1)} (r^{r-1})^{p(p-1)}.$$

In conclusione l'indice è

$$\mathrm{N}_{K/\mathbb{Q}}((p^{p-1})^{r(r-1)} (r^{r-1})^{p(p-1)}) = ((p^{p-1})^{r(r-1)} (r^{r-1})^{p(p-1)})^{q-1}.$$

Come prima non abbiamo usato che q sia primo. Il risultato precedente, quindi, si generalizza al caso in cui $K = \mathbb{Q}(\zeta_{m'})$, con m' primo con p e con r, tutti congrui ad uno modulo 2 in questo modo:

$$[\mathcal{A}_{L/\mathbb{Q}(\zeta_{m'})} : \mathcal{O}_{\mathbb{Q}(\zeta_{m'})}[G]] = ((p^{p-1})^{r(r-1)} (r^{r-1})^{p(p-1)})^{[\mathbb{Q}(\zeta_{m'}):\mathbb{Q}]}.$$

4.6 $K = \mathbb{Q}(\zeta_q)$ e $L = \mathbb{Q}(\zeta_{q^2})$, q primo diverso da 2

L'ultimo esempio che prendiamo in considerazione è il caso in cui $m' = q = m$, $n = q^2$ e $L_m = L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}(\zeta_q)$. Allora

$$\Gamma = Gal(L/L_m) = Gal(L/\mathbb{Q}(\zeta_q)) = G \cong \mathbb{Z}/q\mathbb{Z} = \{1, \gamma, ..., \gamma^{q-1}\}$$

e

$$\Gamma \cong \Gamma^* = \{1, \psi, ..., \psi^{q-1}\}.$$

Vale che

$$\mathcal{A}_{L/K} = \bigoplus_{\psi \in \overline{\Gamma^*}} \mathbb{Z}[\zeta_q][G]\mathcal{E}_\psi.$$

Si può calcolare ripetendo il ragionamento svolto in precedenza. Esattamente come prima abbiamo che

$$\mathcal{E}_{\mathrm{id}} = \frac{1}{q}(\mathrm{id} + \gamma + ... + \gamma^{q-1}).$$

Consideriamo ora invece ψ, che ha ordine q, per cui $\mathfrak{G} = Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q}(\zeta_q)) = \{id\}$; inoltre, come prima, $\psi(\gamma^{-1})$ deve essere una radice q-esima dell'unità diversa da 1, altrimenti $\psi = \mathrm{id}$, quindi $\psi(\gamma^{-1}) = \zeta_q$. Allora

$$\mathcal{E}_{\psi} = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\left(\sum_{\sigma\in\mathfrak{G}}\sigma(\psi(\gamma^{-1}))\right)\gamma = \frac{1}{q}\sum_{\gamma\in\Gamma}\psi(\gamma^{-1})\gamma = \frac{1}{q}(\mathrm{id}+\zeta_q\gamma+...+\zeta_q^{q-1}\gamma^{\,q-1}).$$

A differenza di prima $\mathcal{E}_{\psi} \neq \mathcal{E}_{\psi^2}$: $\mathfrak{G}$ è banale, per cui non compare la traccia nell'espressione degli $\mathcal{E}_{\psi}$, che dipendono da ψ in modo esplicito. Il valore di ψ^2 è semplice da calcolare:

$$\psi^2(\gamma^{-1}) = \psi(\gamma^{-1})\psi(\gamma^{-1}) = \zeta_q^{\,2}.$$

Per cui

$$\mathcal{E}_{\psi^2} = \frac{1}{q}(\mathrm{id} + \zeta_q^{\,2}\gamma + ... + \zeta_q^{\,2(q-1)}\gamma^{\,q-1}).$$

Lo stesso discorso si fa per $\mathcal{E}_{\psi^{\,i}}$, quindi

$$\mathcal{E}_{\psi^i} = \frac{1}{q}(\mathrm{id} + \zeta_q^{\,i}\gamma + ... + \zeta_q^{\,i(q-1)}\gamma^{\,q-1}).$$

Questa volta dobbiamo moltiplicare gli $\mathcal{E}_{\chi}$ solo per gli elementi di Γ, perché in questo caso $\Gamma = G$. Quindi $\mathcal{E}_{\mathrm{id}}$ ha rango 1: infatti, moltiplicato per tutti gli elementi di Γ, dà sempre se stesso. Ma anche $\mathcal{E}_{\psi^i}$ moltiplicato per tutti gli elementi di Γ dà rango uno: infatti se $\gamma_1 \in \Gamma$, vale che

$$\begin{aligned}\mathcal{E}_{\psi^i}\gamma_1 = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\psi^{\,i}(\gamma^{\,-1})\gamma\gamma_1 = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\psi^{\,i}(\gamma_1\gamma_1^{-1}\gamma^{\,-1})\gamma\gamma_1 = \\ = \psi^{\,i}(\gamma_1)\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\psi^{\,i}(\gamma_1^{-1}\gamma^{\,-1})\gamma\gamma_1 = \\ = \psi^{\,i}(\gamma_1)\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\psi^{\,i}((\gamma\gamma_1)^{\,-1})\gamma\gamma_1 = \psi^i(\gamma_1)\mathcal{E}_{\psi^{\,i}}.\end{aligned}$$

Allora $\mathcal{E}_{\psi^{\,i}}\gamma^{\,j}$ è un multiplo di $\mathcal{E}_{\psi^{\,i}}\mathrm{id}$ per ogni j, quindi $\mathcal{E}_{\psi^{\,i}}$, moltiplicato per tutti gli elementi di Γ, dà rango 1. Questo stesso ragionamento vale per ψ^i, per ogni i.
In conclusione come base di $\mathcal{A}_{L/K}$ scegliamo

$$\begin{aligned}&\mathcal{E}_{\mathrm{id}} = \tfrac{1}{q}(\mathrm{id} + \gamma + ... + \gamma^{q-1})\\ &\mathcal{E}_{\psi} = \tfrac{1}{q}(\mathrm{id} + \zeta_q\gamma + ... + \zeta_q^{\,(q-1)}\gamma^{\,q-1})\\ &\mathcal{E}_{\psi^{\,2}} = \tfrac{1}{q}(\mathrm{id} + \zeta_q^{\,2}\gamma + ... + \zeta_q^{\,2(q-1)}\gamma^{\,q-1})\\ &\vdots\\ &\mathcal{E}_{\psi^{q-1}} = \tfrac{1}{q}(\mathrm{id} + \zeta_q^{\,q-1}\gamma + ... + \zeta_q^{\,(q-1)(q-1)}\gamma^{\,q-1}).\end{aligned}$$

La matrice che esprime la base di $\mathcal{A}_{L/K}$ in termini di $\{\mathrm{id}, \gamma, ..., \gamma^{q-1}\}$ è

$$\mathbf{D} = \frac{1}{q}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta_q & \zeta_q^2 & \dots & \zeta_q^{q-1} \\ 1 & \zeta_q^2 & \zeta_q^4 & \dots & \zeta_q^{2(q-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \zeta_q^{q-1} & \zeta_q^{2(q-1)} & \dots & \zeta_q^{(q-1)(q-1)} \end{pmatrix}.$$

Per calcolare il determinante della matrice $\mathbf{D}$ sommiamo all'ultima colonna tutte le altre: troviamo una matrice $\mathbf{D}'$

$$\mathbf{D}' = \frac{1}{q}\begin{pmatrix} 1 & 1 & \dots & 1 & q \\ 1 & \zeta_q & \dots & \zeta_q^{(q-2)} & 0 \\ 1 & \zeta_q^2 & \dots & \zeta_q^{2(q-2)} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \zeta_q^{q-1} & \dots & \zeta_q^{(q-1)(q-2)} & 0 \end{pmatrix}.$$

Ovviamente $\det(D) = \det(D')$, ma a questo punto $\det(D')$ è molto semplice da calcolare: il determinante della sottomatrice $(q-1)\times(q-1)$ ottenuta togliendo la prima riga e l'ultima colonna è la radice quardata del $\mathrm{disc}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(1, \zeta_q, ..., \zeta_q^{q-2})$. $\mathrm{disc}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(1, \zeta_q, ..., \zeta_q^{q-2}) = \pm q^{q-2}$, vale il $+$ se e solo se $q \equiv 1 \pmod 4$. Se $q \equiv 1 \pmod 4$

$$\det(D') = \frac{1}{q^q} q \sqrt{\mathrm{disc}(1, \zeta_q, \zeta_q^2, ..., \zeta_q^{q-2})} = \frac{q}{q^q}\sqrt{q^{q-2}} = \frac{q^{\frac{q-2}{2}}}{q^{q-1}}$$

e

$$[\mathcal{A}_{L/K} : \mathcal{O}_K[G]] = \left| \mathrm{N}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}\left(\frac{q^{q-1}}{q^{\frac{q-2}{2}}}\right)\right| = \frac{q^{(q-1)(q-1)}}{q^{\frac{(q-2)(q-1)}{2}}} = q^{\frac{q(q-1)}{2}}.$$

Invece se $q \equiv -1 \pmod 4$,

$$\det(D') = \frac{1}{q^q} q \sqrt{\mathrm{disc}(1, \zeta_q, \zeta_q^2, ..., \zeta_q^{q-2})} = \frac{q}{q^q}\sqrt{-q^{q-2}} = \frac{\sqrt{-}q^{q-2}}{q^{q-1}}.$$

Ma

$$\mathrm{N}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\sqrt{-q}) = \mathrm{N}_{\mathbb{Q}(\sqrt{-q})/\mathbb{Q}}(\mathrm{N}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}(\sqrt{-q})}(\sqrt{-q})) = \mathrm{N}_{\mathbb{Q}(\sqrt{-q})/\mathbb{Q}}(\sqrt{-q}^{\frac{q-1}{2}})$$

e

$$\mathrm{N}_{\mathbb{Q}(\sqrt{-q})/\mathbb{Q}}(\sqrt{-q}^{\frac{q-1}{2}}) = (\mathrm{N}_{\mathbb{Q}(\sqrt{-q})/\mathbb{Q}}(\sqrt{-q}))^{\frac{q-1}{2}} = (-q)^{\frac{q-1}{2}}.$$

Quindi anche per $q \equiv -1 \pmod 4$

$$[\mathcal{A}_{L/K} : \mathcal{O}_K[G]] = \left| \mathrm{N}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}\left(\frac{q^{q-1}}{-q^{\frac{q-2}{2}}}\right)\right| = \frac{q^{(q-1)(q-1)}}{q^{\frac{(q-2)(q-1)}{2}}} = q^{\frac{q(q-1)}{2}}.$$

Bibliografia

[AdWe 1992] W. A. Adkins, S. H. Weintraub, *Algebra: an approach via module theory*, **GTM** 136, Springer-Verlag, New York, 1992.

[AtMD 1969] M. F. Atiyah, I. G. MacDonald, *Introduction to commutative algebra*, Perseus Books Publishing, 1969.

[BiPa 1976] R. H. Bird, C. J. Parry, *Integral bases for bicyclic biquadratic fields over quadratic subfields*, Pacific Journal of Mathematics, **66**, 29-36, (1976).

[ByLe 1996] N. P. Byott e G. Lettl, *Relative Galois module structure of integers of abelian fields*. Journal de Théorie des Nombres de Bordeaux, **8**, 125-141, (1996).

[ChLi 1993] S.-P. Chan, C.-H. Lim, *Relative Galois modules structure of rings of integers of cyclotomic fields*, Journal für die reine und angewandte Mathematik, **434**, 205-220, (1993).

[Ch 2000] L. N. Childs, *Taming wild extensions: Hopf algebras and local Galois theory*, American Mathematical Society, 2000.

[Fr 1983] A. Fröhlich, *Galois module stucture of algebraic integers*, Springer-Verlag, Berlin Heidelberg, 1983.

[FrTa 1991] A. Fröhlich, M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1991.

[GrReRuSr 1999] C. Greither, D. R. Replogle, K. Rubin, A. Srivastav, *Swan modules and Hilbert-Speiser number fields*, Journal of Number Theory, **79**, 164-173, (1999).

[Hi 1897] D. Hilbert, The theory of algebraic number fields, translated from the German by I. T. Adamson, Sringer-Verlag, Berlin Heidelberg, 1998.

[Ka 1984] F. Kawamoto, *On Normal Integral Bases*, Tokyo Journal of Mathematics, **1**, 221-230, (1984).

[Ka 1986] F. Kawamoto, *On Normal Integral Bases of Local Fields*, Journal of Algebra, **98**, 197-199, (1986).

[La 1970] S. Lang, *Algebraic number theory*, Addison-Wesley, 1970.

[La 2002] S. Lang, *Algebra-Revised third edition*, **GTM** 211, Springer Verlag, New York, 2002.

[Lo 1959] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, Journal für die reine und angewandte Mathematik, **201**, 119-149, (1959).

[Le 1990] G. Lettl, *The ring of integers of an abelian number field*, Journal für die reine und angewandte Mathematik, **404**, 162-170, 1990.

[Ma 1977] D. A. Marcus, *Numberfields*, Springer, 1977.

[MKSc 1971] R. MacKenzie, J. Scheunemann, *A number fields without a relative integral basis*, The American Mathematical Monthly, **78**, 882-883, (1971).

[Na 1990] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, second edition, 1990.

[No 1931] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, Journal für die reine und angewandte Mathematik, **167**, 147-152, (1931).

[Ri 1959] D. S. Rim, *Modules over finite groups*, Annals of Mathematics, **69**, 700-712, (1959).

[Sa 1967] P. Samuel, *Théorie Algébrique des Nombres*, Hermann, Paris, 1967.

[Se 1995] J.-P. Serre, *Local fields*, **GTM** 67, Springer-Verlag, 1995.

[Sp 1916] A. Speiser, *Gruppendeterminante und Körper diskriminante*, Mathematische Annalen, **77**, 546-562, 1916.

[Sw 1960] R. G. Swan, *Induced representations and projective modules*, Annals of Mathematics, **71**, 552-578, (1960).

[Ul 1970] S. Ullom *Integral normal bases in Galois extensions of local fields*, Nagoya Mathematical Journal, **39**, 141-148, (1970).

[Wa 1982] L. C. Washington, *Introduction to cyclotomic fields*, **GTM** 83, Springer-Verlag, New York.