Università degli Studi di Pisa

Dipartimento di Matematica

Tesi di Laurea Triennale

L'anello degli interi di un campo di numeri abeliano

10 giugno 2016

Candidato:
Giacomo Mezzedimi

Relatore:
Prof. Ilaria del Corso

Anno Accademico 2015/2016

Introduzione

Presa un'estensione L/K di campi di numeri di Galois con gruppo di Galois G, un classico problema di teoria di Galois è lo studio della struttura di L come $K[G]$-modulo; il teorema della base normale lo risolve completamente mostrando che L è sempre un $K[G]$-modulo libero di rango 1.
Una domanda analoga può essere posta riguardo agli anelli degli interi: se $\mathscr{O}_K$ e $\mathscr{O}_L$ denotano rispettivamente gli anelli degli interi di K e L, quale è la struttura di $\mathscr{O}_L$ come $\mathscr{O}_K[G]$-modulo? Innanzitutto il fatto che $\mathscr{O}_L$ sia un $\mathscr{O}_K[G]$-modulo libero di rango 1 è equivalente all'esistenza di un elemento ω che generi una cosiddetta base normale intera, o NIB, cioè una base di $\mathscr{O}_L$ su $\mathscr{O}_K$ formata da tutti i coniugati di ω tramite G.
Un primo risultato, conosciuto come teorema di Noether, afferma che, se l'estensione L/K ammette una NIB, allora necessariamente l'estensione L/K è tame. Il viceversa, però, non vale in generale, neppure nel caso in cui il campo base sia $\mathbb{Q}$: il primo risultato in questa direzione, dovuto a Martinet ([13]) e risalente agli anni '70, mostra l'esistenza di estensioni K di Galois tame di $\mathbb{Q}$ con gruppo di Galois isomorfo al gruppo dei quaternioni per cui $\mathscr{O}_K$ non è libero come $\mathbb{Z}[G]$-modulo.
D'altra parte, il teorema di Hilbert-Speiser afferma che il viceversa del teorema di Noether vale per le estensioni abeliane di $\mathbb{Q}$; in tale caso, quando $L/\mathbb{Q}$ è abeliana e tame, lo stesso risultato esibisce un generatore esplicito di $\mathscr{O}_L$ come $\mathbb{Z}[G]$-modulo libero.
In questo ordine di idee, possiamo dire che un campo di numeri è di Hilbert-Speiser se ogni sua estensione abeliana e tame ammette una base normale intera: un famoso articolo di Greither, Replogle e Rubin del 1999 ([8]) dimostra che l'unico campo di Hilbert-Speiser è $\mathbb{Q}$.
Partendo dall'osservazione che l'anello degli interi $\mathscr{O}_K$ di un campo di numeri abeliano con ramificazione wild non può mai essere libero su $\mathbb{Z}[G]$, viene naturale cercare un altro anello su cui poter studiare la struttura di $\mathscr{O}_K$; grazie alla proposizione 4.12, deduciamo che l'unico ordine di $\mathbb{Q}[G]$ da considerare è l'ordine associato $\mathcal{A}_{K/\mathbb{Q}}$. In generale, si può dimostrare che l'ordine associato a una qualunque estensione L/K coincide con l'anello di gruppo $\mathscr{O}_K[G]$ se e

solo se L/K ha ramificazione tame; inoltre un importante risultato, dovuto a Leopoldt ([10]), assicura che l'anello degli interi $\mathscr{O}_K$ di un campo di numeri abeliano è sempre libero di rango 1 sul suo ordine associato $\mathcal{A}_{K/\mathbb{Q}}$. Tale risultato generalizza dunque il teorema di Hilbert-Speiser, risolvendo completamente anche il caso di un campo di numeri abeliano con ramificazione wild.
In generale, però, l'anello degli interi di un campo di numeri non è sempre libero sul suo ordine associato: ad esempio, come visto da Bergè in [1], le estensioni diedrali K di $\mathbb{Q}$ di ordine diverso da $2p$, con p primo dispari, sono tali che $\mathscr{O}_K$ non è neanche proiettivo sull'ordine associato $\mathcal{A}_{K/\mathbb{Q}}$.
D'altra parte, articoli di Bergè e di Martinet ([1], [14]) dimostrano che l'anello $\mathscr{O}_K$ è libero sul suo ordine associato nel caso in cui K sia un'estensione diedrale di $\mathbb{Q}$ di ordine $2p$, con p primo dispari, o un'estensione di Galois di $\mathbb{Q}$ con ramificazione wild e con gruppo di Galois isomorfo al gruppo dei quaternioni.
Infine, analogamente a come fatto per il teorema di Hilbert-Speiser, possiamo dire che un campo di numeri K è di Leopoldt se ogni sua estensione L/K con $L/\mathbb{Q}$ abeliana è tale che $\mathscr{O}_L$ è libero sul suo ordine associato $\mathcal{A}_{L/K}$; lavori di Leopoldt ([10]), Cassou-Noguès e Taylor ([5]), Chan e Lim ([6]), Bley ([2]) e Byott e Lettl ([4]), mostrano che le estensioni ciclotomiche $\mathbb{Q}^{(n)}$ sono tutte di Leopoldt.

In questa tesi presento una dimostrazione del teorema di Leopoldt che segue la strada indicata da Lettl ([11]) nel suo articolo del 1990. Per rendere la trattazione completa e accessibile a chiunque abbia seguito un primo corso di teoria algebrica dei numeri, tutti i prerequisiti specifici sono inclusi con dimostrazione dettagliata.
Ho raccolto nel primo capitolo i risultati relativi al caso delle estensioni tame di $\mathbb{Q}$, che permettono di ottenere una dimostrazione piuttosto completa dei teoremi di Noether e di Hilbert-Speiser.
Nel secondo capitolo invece si introducono i risultati fondamentali relativi ai caratteri di Dirichlet, illustrandone i legami con i campi di numeri abeliani e la loro ramificazione. Più avanti vengono definite le somme di Gauss e presentate le loro principali proprietà.
Il capitolo 3 approfondisce lo studio delle rappresentazioni di Artin. Nel contesto della tesi servono a dimostrare la formula conduttore-discriminante, che però avrei potuto ottenere anche in modo più diretto; tale digressione ha però il merito di introdurre tale strumento, centrale nella teoria dei numeri, che mi ha appassionato molto e che dunque ho deciso di inserire in questo lavoro.
Infine, nell'ultimo capitolo, ripercorriamo l'articolo di Lettl ([11]) usando

tutta la precedente teoria: utilizzando strumenti introdotti già da Leopoldt in [10], come ad esempio gli idempotenti ortogonali e le coordinate di carattere, forniamo una dimostrazione dettagliata del teorema di Leopoldt caratterizzando esplicitamente l'ordine $\mathcal{A}_{K/\mathbb{Q}}$ e il generatore T di $\mathscr{O}_K$ su $\mathcal{A}_{K/\mathbb{Q}}$.

Indice

Capitolo 1

Il teorema di Hilbert - Speiser

In questo capitolo introduttivo cominceremo a richiamare alcune definizioni e risultati basilari, con cui tracceremo uno schema di dimostrazione del teorema di Hilbert-Speiser via teorema di Kronecker-Weber. Assumeremo inoltre alcuni fatti noti, le cui dimostrazioni possono essere trovate in [12].

Sia L/K un'estensione di Galois finita di campi di numeri, $G = \mathrm{Gal}(L/K)$ il suo gruppo di Galois e $\mathscr{O}_L, \mathscr{O}_K$ i rispettivi anelli degli interi. Denotando con $K[G]$ e $\mathscr{O}_K[G]$ gli usuali anelli di gruppo

$$K[G] = \left\{ \sum_{g \in G} \alpha_g g \;\middle|\; \alpha_g \in K \right\}, \qquad \mathscr{O}_K[G] = \left\{ \sum_{g \in G} \alpha_g g \;\middle|\; \alpha_g \in \mathscr{O}_K \right\},$$

è immediato osservare che L è un $K[G]$-modulo con l'azione

$$\left(\sum_{g \in G} \alpha_g g \right)(x) = \sum_{g \in G} \alpha_g g(x),$$

e $\mathscr{O}_L$ è un $\mathscr{O}_K[G]$-modulo per restrizione dell'azione precedente.
Detto n il grado dell'estensione L/K, sia L che $K[G]$ sono K-moduli di rango n, dunque, se si avesse che L è un $K[G]$-modulo libero, seguirebbe immediatamente che $L = K[G]\omega$, cioè L avrebbe rango 1 su $K[G]$. Questo è effettivamente il caso, come mostra il seguente classico risultato di teoria di Galois:

Teorema 1.1 (della base normale)**.** *L/K estensione finita di Galois con gruppo di Galois G. Allora L è un $K[G]$-modulo libero di rango* 1*, cioè $L = K[G]\omega$ per un certo $\omega \in L$; la base $\{\sigma(\omega) \mid \sigma \in G\}$ di L/K si chiama base normale e ω si dice generatore della base normale.*

Una dimostrazione di tale teorema può essere trovata in [3].

Un tale risultato è di fondamentale importanza, in quanto mostra la struttura di L come modulo di Galois su K nel caso generale di una qualsiasi estensione finita e di Galois; a questo punto diventa interessante cercare un teorema analogo per gli anelli degli interi.
Anche in questo caso, essendo sia $\mathscr{O}_L$ che $\mathscr{O}_K[G]$ $\mathscr{O}_K$-moduli di rango n, se $\mathscr{O}_L$ fosse un $\mathscr{O}_K[G]$-modulo libero, avrebbe rango 1 e quindi esisterebbe un elemento $\omega \in \mathscr{O}_L$ tale che $\mathscr{O}_L = \mathscr{O}_K[G]\omega$; tale elemento genererebbe una cosiddetta base normale intera, spesso abbreviata NIB, che evidentemente sarebbe una base normale per L/K.

Purtroppo, nel caso generale la situazione è piuttosto complessa; in questa tesi andremo a studiare il caso di un'estensione $K/\mathbb{Q}$ di Galois abeliana finita, che riusciremo a risolvere completamente.
Introduciamo ora i concetti fondamentali e i teoremi che ci serviranno in seguito.

Definizione 1.1. Sia L/K un'estensione di campi e P un primo di $\mathscr{O}_K$. P si dice tame in L se, per ogni primo Q di $\mathscr{O}_L$ sopra P, $p \nmid e(Q|P)$, dove $p = P \cap \mathbb{Z}$ e $e(Q|P)$ è l'indice di ramificazione di Q in P.
L'estensione L/K si dice tame se ogni primo di $\mathscr{O}_K$ è tame.

Indichiamo con $\mathrm{Tr}_{L/K} : L \to K$ e $\mathrm{N}_{L/K} : L \to K$ le funzioni traccia e norma dell'estensione L/K. Inoltre, considerato l'ideale frazionario di $\mathscr{O}_L$

$$\mathscr{O}_L^* = \{x \in L \mid \mathrm{Tr}_{L/K}(x\mathscr{O}_L) \subseteq \mathscr{O}_K\},$$

definiamo differente di L/K l'ideale frazionario di L $\mathfrak{D}_{L/K} = (\mathscr{O}_L^*)^{-1}$.
Evidentemente $\mathfrak{D}_{L/K}$ è invariante sotto l'azione degli automorfismi del gruppo di Galois G; per di più, vale la seguente importante caratterizzazione:

Proposizione 1.2. *Se I è un ideale frazionario di K e J uno di L, vale l'inclusione $\mathrm{Tr}_{L/K}(J) \subseteq I$ se e solo se $J \subseteq I\mathfrak{D}_{L/K}^{-1}$. In particolare:*

$$\mathrm{Tr}_{L/K}(\mathscr{O}_L) = \mathrm{lcm}\{I \subseteq \mathscr{O}_L \mid I\mathscr{O}_L \mid \mathfrak{D}_{L/K}\}.$$

Dimostrazione. Per la prima parte è sufficiente notare che la traccia di J è contenuta in I se e solo se la traccia di $I^{-1}J$ è contenuta in $\mathscr{O}_K$, cioè $I^{-1}J$ è contenuto in $\mathscr{O}_L^*$.
Per l'altra, applichiamo il risultato appena mostrato al caso $J = \mathscr{O}_L$: l'immagine della traccia sta in un certo ideale I se e solo se $\mathfrak{D}_{L/K} \subseteq I\mathscr{O}_L$, cioè se e solo se $I\mathscr{O}_L \mid \mathfrak{D}_{L/K}$. □

Lo studio del differente risulta utile anche per ottenere informazioni dettagliate sulla ramificazione: ad esempio il prossimo teorema mostra come la divisibilità del differente per un certo primo dipenda fortemente dal tipo di ramificazione che tale primo ha nell'estensione (cfr. [12], cap. 4).

Teorema 1.3. *Sia P un primo di $\mathscr{O}_K$, Q un primo di $\mathscr{O}_L$ sopra P ed $e = e(Q|P)$ il loro indice di ramificazione. Allora $Q^{e-1} \mid \mathfrak{D}_{L/K}$ e la divisibilità è esatta se e solo se $p \nmid e(Q|P)$, dove $p = P \cap \mathbb{Z}$.*

Teorema 1.4 (Noether)**.** *L'estensione L/K è tame se e solo se la traccia ristretta agli interi è surgettiva, cioè $\mathrm{Tr}_{L/K}(\mathscr{O}_L) = \mathscr{O}_K$.*

Dimostrazione. Supponiamo che L/K abbia ramificazione wild; sia dunque P un primo di $\mathscr{O}_K$ che ha ramificazione wild. Visto che l'estensione è di Galois, abbiamo che $P\mathscr{O}_L = (Q_1 \cdot \ldots \cdot Q_r)^e$, dove $Q_1, \ldots, Q_r$ sono i primi di $\mathscr{O}_L$ sopra P. Per il teorema precedente, esiste un indice i tale che $Q_i^e \mid \mathfrak{D}_{L/K}$; ma essendo l'azione di G transitiva su $Q_1, \ldots, Q_r$ e banale su $\mathfrak{D}_{L/K}$, segue che $Q_j^e \mid \mathfrak{D}_{L/K}$ per tutti i j, cioè $P\mathscr{O}_L \mid \mathfrak{D}_{L/K}$. A questo punto la proposizione 1.2 permette di concludere che $\mathrm{Tr}_{L/K}(\mathscr{O}_L) \subseteq P$.
Viceversa, se esiste un primo P di $\mathscr{O}_K$ per cui $\mathrm{Tr}_{L/K}(\mathscr{O}_L) \subseteq P$, allora $P\mathscr{O}_L = (Q_1 \cdot \ldots \cdot Q_r)^e \mid \mathfrak{D}_{L/K}$, cioè l'estensione è wild. □

Il teorema di Noether ha un'importante conseguenza:

Corollario 1.5. *Se l'estensione L/K ha una NIB, allora è tame.*

Dimostrazione. Sia α un generatore della NIB; vediamo che $\mathrm{Tr}_{L/K}(\mathscr{O}_L) = \mathscr{O}_K$. Preso $x = \sum_{g\in G} a_g g(\alpha) \in \mathscr{O}_K[G]\alpha = \mathscr{O}_L$, esso sta in $\mathscr{O}_K$ se e solo se è fissato da tutti gli elementi di G. Ora, scelto $\tau \in G$, si ha:

$$\tau(x) = \sum_{g\in G} a_g(\tau g)(\alpha) = \sum_{g\in G} a_{\tau^{-1}g} g(\alpha) = x \iff a_{\tau^{-1}g} = a_g = a \ \forall g \in G,$$

dunque $x \in \mathscr{O}_K$ se e solo se $x = a\sum_{g\in G} g(\alpha) \in \mathrm{Tr}_{L/K}(\mathscr{O}_L)$. □

Vediamo esplicitamente con un esempio che un'estensione wild non può avere una base normale intera.

Esempio. Consideriamo l'estensione $\mathbb{Q}(i)/\mathbb{Q}$; come è noto, l'estensione è wild, in quanto il primo 2 ha indice di ramificazione 2 in $\mathbb{Q}(i)$. Sia G il gruppo di Galois dell'estensione, composto dall'identità e dalla restrizione del coniugio di $\mathbb{C}$; se per assurdo l'anello degli interi $\mathbb{Z}[i]$ di $\mathbb{Q}(i)$ fosse uno $\mathbb{Z}[G]$-modulo libero, esisterebbe un elemento $\omega = \lambda + i\mu$ tale che $\mathbb{Z}[i] = \mathbb{Z}[G]\omega$. Osservato però che:

$$\mathbb{Z}[G]\omega = \{a(\lambda+i\mu)+b(\lambda-i\mu) \mid a,b \in \mathbb{Z}\} = \{(a+b)\lambda+i(a-b)\mu \mid a,b \in \mathbb{Z}\},$$

è immediato accorgersi che tale anello non può contenere sia 1 che i.

A questo punto viene spontaneo chiedersi se possa valere anche l'implicazione opposta, cioè L/K tame $\implies$ L/K ha una NIB; purtroppo in generale tale implicazione è falsa, in quanto si possono trovare estensioni tame con gruppo di Galois isomorfo al gruppo dei quaternioni che non ammettono una base normale intera: Martinet in [13] dimostra infatti che, fissato $K = \mathbb{Q}(\sqrt{5}, \sqrt{21})$ e $m = \frac{5+\sqrt{5}}{2}\frac{21+\sqrt{21}}{2}$, le due estensioni $L_1 = K(\sqrt{m})$ e $L_2 = K(\sqrt{-3m})$ sono di Galois su $\mathbb{Q}$ con gruppo di Galois isomorfo al gruppo dei quaternioni e tame, ma $L_1/\mathbb{Q}$ ammette una NIB, mentre $L_2/\mathbb{Q}$ non può averla.

Il teorema di Hilbert-Speiser mostra tuttavia che, restringendosi alle estensioni abeliane di $\mathbb{Q}$, la condizione di avere una base normale intera è equivalente ad avere ramificazione tame. Cominciamo dal caso particolare delle estensioni ciclotomiche. Prima però richiamiamo un fatto generale sulle basi intere di un prodotto di campi di numeri:

Proposizione 1.6. *Siano $K_i/\mathbb{Q}$ estensioni finite di Galois e sia $\{\alpha_\lambda^{(i)}\}$ una base intera di K_i per ogni $i = 1, \ldots, m$. Supponiamo inoltre che $\big(\mathrm{disc}(K_i), \mathrm{disc}(K_j)\big) = 1$ per ogni $i \neq j$. Allora il composto $L = K_1 \cdot \ldots \cdot K_m$ ammette una base intera formata da tutti i prodotti $\prod_i \alpha_{\lambda_i}^{(i)}$.*

Tale fatto generale si applica ovviamente al caso particolare delle basi normali intere:

Proposizione 1.7. *Siano $K_i/\mathbb{Q}$ estensioni finite di Galois con basi intere generate da α_i per ogni $i = 1, \ldots, m$ tali che $\big(\mathrm{disc}(K_i), \mathrm{disc}(K_j)\big) = 1$ per ogni $i \neq j$. Allora $L = K_1 \cdot \ldots \cdot K_m$ ha una base normale intera generata da $\prod \alpha_i$.*

Dimostrazione. Sia $G_i = \mathrm{Gal}(K_i/\mathbb{Q})$; $\big\{\sigma^{(i)}(\alpha_i)\big\}_{\sigma^{(i)} \in G_i}$ è una base intera di $K_i/\mathbb{Q}$, dunque $\big\{\sigma^{(1)}(\alpha_1) \cdot \sigma^{(2)}(\alpha_2) \cdot \ldots \cdot \sigma^{(m)}(\alpha_m)\big\}_{\sigma^{(1)} \in G_1, \ldots, \sigma^{(m)} \in G_m}$ è una base intera di $\mathscr{O}_L$ per la proposizione precedente. Ma visto che $G = \mathrm{Gal}(L/\mathbb{Q}) \cong G_1 \times \ldots \times G_m$, si ha che $\{\sigma(\alpha_1 \cdot \ldots \cdot \alpha_m)\}_{\sigma \in G}$ coincide esattamente con la base $\big\{\sigma^{(1)}(\alpha_1) \cdot \sigma^{(2)}(\alpha_2) \cdot \ldots \cdot \sigma^{(m)}(\alpha_m)\big\}_{\sigma^{(1)} \in G_1, \ldots, \sigma^{(m)} \in G_m}$, che dunque è anche normale. □

Nel seguito indicheremo con ζ_m la radice m-esima dell'unità $e^{\frac{2\pi i}{m}}$ e con $\mathbb{Q}^{(m)} = \mathbb{Q}(\zeta_m)$ l'm-esima estensione ciclotomica dei razionali.

Corollario 1.8. *Le seguenti affermazioni sono equivalenti:*

1. *$\mathbb{Q}^{(m)}/\mathbb{Q}$ ha una base intera generata da ζ_m;*

2. $\mathbb{Q}^{(m)}/\mathbb{Q}$ *è tame;*

3. m *è squarefree.*

Dimostrazione. Se m non è squarefree e $p^2 \mid m$, allora p ha ramificazione wild in $\mathbb{Q}^{(p^2)} \subseteq \mathbb{Q}^{(m)}$, in quanto $p\mathbb{Z}[\zeta_{p^2}] = P^{\phi(p^2)}$ e $p \mid \phi(p^2)$. Per la moltiplicatività dei gradi nelle torri si ha che p ha ramificazione wild anche in $\mathbb{Q}^{(m)}$, che quindi non può avere una NIB su $\mathbb{Q}$.
Viceversa, supponiamo che m sia squarefree: in questo caso mostriamo che ζ_m genera una base normale intera per $\mathbb{Q}^{(m)}$ su $\mathbb{Q}$.
Sia $m = p_1 \cdot \ldots \cdot p_r$; se p è primo, $\mathbb{Q}^{(p)}/\mathbb{Q}$ ha una NIB data da $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^p\} = \{\sigma(\zeta_p)\}_{\sigma \in \mathrm{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q})}$. Inoltre $\mathrm{disc}(\mathbb{Q}^{(p)}/\mathbb{Q})$ è potenza di p e $\mathbb{Q}^{(m)} = \mathbb{Q}^{(p_1)} \cdot \ldots \cdot \mathbb{Q}^{(p_r)}$, dunque per la proposizione precedente l'elemento $\prod \zeta_{p_i}$, che è una radice m-esima primitiva dell'unità, genera una NIB per $\mathbb{Q}^{(m)}/\mathbb{Q}$. □

Abbiamo quindi ottenuto una completa caratterizzazione delle estensioni ciclotomiche che ammettono una base normale intera su $\mathbb{Q}$; tale risultato assume ancora più importanza anche in vista del teorema di Kronecker-Weber, che andiamo subito ad enunciare:

Teorema 1.9 (Kronecker-Weber)**.** *Ogni estensione abeliana finita K di $\mathbb{Q}$ è contenuta in un'estensione ciclotomica $\mathbb{Q}^{(n)}$; tale n viene detto conduttore del campo K. Se inoltre l'estensione $K/\mathbb{Q}$ è tame, n può essere scelto squarefree.*

Per poter dedurre informazioni su eventuali basi normali intere di estensioni abeliane finite di $\mathbb{Q}$, abbiamo perciò bisogno di mostrare che l'esistenza di una NIB passa alle sottoestensioni; per questo ci viene in aiuto la seguente proposizione:

Proposizione 1.10. *$L/\mathbb{Q}$ estensione di Galois con una NIB generata da α. Allora ogni estensione intermedia K di Galois su $\mathbb{Q}$ ha una NIB generata da $\beta = \mathrm{Tr}_{L/K}(\alpha)$.*

Dimostrazione. Sia $G = \mathrm{Gal}(L/\mathbb{Q})$ e $H \triangleleft G$ tale che K sia il campo fissato da H. Per ipotesi $\mathscr{O}_L = \mathbb{Z}[G]\alpha$. Sia $x = \sum_{g \in G} a_g g(\alpha) \in \mathscr{O}_L$; ragionando come in precedenza, si ha che $x \in \mathscr{O}_K$ se e solo se $a_{h^{-1}g} = a_g$ per ogni $h \in H$, cioè se e solo se gli a_g sono costanti sulle classi laterali sinistre di H (siano esse $\{H, Hg_1, \ldots, Hg_d\}$).

Si ha perciò:

$$x = \sum_{g\in G} a_g g(\alpha) = \sum_{i=1}^{d}\sum_{h\in H} a_{hg_i}(hg_i)(\alpha) = \sum_{i=1}^{d} a_{g_i}\sum_{h\in H}(hg_i)(\alpha) =$$
$$= \sum_{i=1}^{d} a_{g_i}\sum_{h\in H} g_i(g_i^{-1}hg_i)(\alpha) = \sum_{i=1}^{d} a_{g_i}\sum_{h\in H}(g_ih)(\alpha) =$$
$$= \sum_{i=1}^{d} a_{g_i} g_i\big(\mathrm{Tr}_{L/K}(\alpha)\big) = \sum_{\sigma\in G/H} a_\sigma\sigma(\beta),$$

cioè la tesi. □

A questo punto siamo pronti per enunciare e dimostrare il teorema di Hilbert-Speiser:

Teorema 1.11 (Hilbert-Speiser)**.** *Un'estensione abeliana finita $K/\mathbb{Q}$ è tame se e solo se ha una base normale intera.*

Dimostrazione. Per Kronecker-Weber, sia n squarefree tale che $K \subseteq \mathbb{Q}^{(n)}$. L'estensione $\mathbb{Q}^{(n)}/\mathbb{Q}$ ha una NIB generata da ζ_n, dunque $K/\mathbb{Q}$ ha una NIB generata da $\mathrm{Tr}_{\mathbb{Q}^{(n)}/K}(\zeta_n)$. □

Il teorema di Hilbert-Speiser conclude di fatto lo studio della struttura dell'anello $\mathscr{O}_K$ come $\mathbb{Z}[G]$-modulo, nel caso in cui $K/\mathbb{Q}$ sia un'estensione abeliana, finita e tame, mostrando esplicitamente un elemento ω tale che $\mathscr{O}_K = \mathbb{Z}[G]\omega$.

Tale teorema dimostra anche che un'estensione $K/\mathbb{Q}$ abeliana e wild non potrà mai avere una base normale intera, cioè l'anello $\mathscr{O}_K$ non potrà mai essere uno $\mathbb{Z}[G]$-modulo libero; nei prossimi capitoli mostreremo l'esistenza di un sottoanello $\mathcal{A}_K$ di $\mathbb{Q}[G]$, su cui $\mathscr{O}_K$ sarà sempre libero nel caso di estensioni abeliane di $\mathbb{Q}$.

Capitolo 2

Caratteri di Dirichlet e Somme di Gauss

In questo secondo capitolo cominciamo a costruire il background che ci servirà per dimostrare i punti focali di questa tesi; in particolare andremo a studiare i caratteri di Dirichlet di un gruppo di Galois G di un'estensione finita L/K per ricavarne informazioni interessanti sulla ramificazione e sull'anello degli interi.

Alla fine del capitolo, introdurremo particolari somme riguardanti tali caratteri, le cosiddette somme di Gauss, che, oltre ad essere interessanti di per sé, costituiscono un punto d'appoggio da cui svilupperemo la nostra teoria.

2.1 Prime proprietà dei caratteri di Dirichlet

Definizione 2.1. Un carattere di Dirichlet è un omomorfismo moltiplicativo $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$. Un carattere di Dirichlet χ si dice pari se $\chi(-1) = 1$, dispari altrimenti.

Osserviamo immediatamente che, se $n \mid m$ e $\pi_{nm} : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ è la proiezione usuale, χ induce un carattere di Dirichlet $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ per composizione; per questo è conveniente scegliere n minimale. Tale n si dice conduttore del carattere χ e viene denotato f_χ; un carattere visto modulo il suo conduttore viene detto primitivo. In questo modo imponiamo l'esistenza di un unico carattere banale, invece che uno per ogni n.
In seguito chiameremo caratteri di $(\mathbb{Z}/n\mathbb{Z})^*$ tutti i caratteri di conduttore divisore di n.

Spesso può essere utile considerare un carattere di Dirichlet come una funzione $\mathbb{Z} \to \mathbb{C}$ ponendo $\chi(a) = 0$ se $(a, f_\chi) \neq 1$. In questa ottica, un carattere è primitivo se riesce a minimizzare il numero di volte che 0 compare nell'immagine della corrispondente funzione $\mathbb{Z} \to \mathbb{C}$.
Un vantaggio evidente del considerare solo caratteri di Dirichlet primitivi è che si riesce a contenere più possibile la cardinalità del dominio; tale imposizione rende però più macchinosa la definizione del prodotto di due caratteri di Dirichlet.
Siano infatti χ, ψ caratteri di Dirichlet, e sia $k = \text{lcm}(f_\chi, f_\psi)$; si definisce prodotto fra χ e ψ il carattere primitivo $\chi\psi$ associato a $\gamma : (\mathbb{Z}/k\mathbb{Z})^* \to \mathbb{C}^*$ tale che $\gamma(a) = \chi(a)\psi(a)$.

Osservazioni.

1. Non necessariamente $\chi\psi(a) = \chi(a)\psi(a)$. Siano infatti $\chi : (\mathbb{Z}/12\mathbb{Z})^* \to \mathbb{C}^*$ e $\psi : (\mathbb{Z}/3\mathbb{Z})^* \to \mathbb{C}^*$ tali che $\chi(1) = \chi(11) = 1$, $\chi(5) = \chi(7) = -1$, $\psi(\pm 1) = \pm 1$. Con un banale calcolo si ottiene che $\chi\psi$ ha conduttore 4 e $\chi\psi(3) = -1 \neq \chi(3)\psi(3)$.

2. Se χ è un carattere di Dirichlet e $\overline{\chi}$ è il coniugato di χ, la finitezza dell'ordine di χ implica che $\overline{\chi}(a) = \chi(a)^{-1}$ per ogni a coprimo con il conduttore f_χ, cioè $\chi\overline{\chi}$ è il carattere banale.

Nel seguito, identificheremo spesso il gruppo $(\mathbb{Z}/n\mathbb{Z})^*$ con il gruppo $G^{(n)}$ di Galois dell'estensione ciclotomica $\mathbb{Q}^{(n)}/\mathbb{Q}$; in questa ottica, sia X un gruppo finito di caratteri di Dirichlet. Se $n = \text{lcm}\{f_\chi \mid \chi \in X\}$, evidentemente X è sottogruppo del gruppo $X^{(n)}$ dei caratteri di $G^{(n)}$, dunque, detta H l'intersezione dei nuclei dei caratteri di X e $K \subseteq \mathbb{Q}^{(n)}$ il campo fissato da H, diciamo che K è il campo associato a X.

Tale associazione può essere resa ancora più esplicita inserendo i caratteri di Dirichlet all'interno della teoria generale dei caratteri, che andremo brevemente a riprendere nella prossima sezione.

2.2 Teoria generale dei caratteri

Sia G un gruppo abeliano finito e denotiamo con $\hat{G}$ il suo gruppo dei caratteri, cioè l'insieme degli omomorfismi $G \to \mathbb{C}^*$.

Proposizione 2.1. *Esiste un isomorfismo (non canonico) fra G e $\hat{G}$.*

Dimostrazione. Supponiamo innanzitutto che G sia ciclico, isomorfo a $\mathbb{Z}/n\mathbb{Z}$. In questo caso, un carattere di G ha immagine contenuta in $\langle\zeta_n\rangle$, dunque

$\hat{G} = \mathrm{Hom}(G, \langle\zeta_n\rangle)$. Ma visto che sia G che $\langle\zeta_n\rangle$ sono isomorfi a $\mathbb{Z}/n\mathbb{Z}$, l'isomorfismo cercato si ottiene osservando che la mappa:

$$\begin{array}{ccc} \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ \chi & \longmapsto & \chi(1) \end{array}$$

è un isomorfismo.
Se invece G è abeliano, per il teorema di struttura dei gruppi abeliani finiti G è isomorfo a un prodotto diretto di gruppi ciclici, diciamo $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$. Osservato che $\mathrm{Hom}\left(\bigoplus_i \mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*\right) \cong \bigoplus_i \mathrm{Hom}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{C}^*)$, la tesi segue utilizzando il primo caso per ciascun fattore. □

Proposizione 2.2. *G e $\hat{\hat{G}}$ sono canonicamente isomorfi.*

Dimostrazione. Consideriamo la mappa $\varphi : G \to \hat{\hat{G}}$ tale che $\varphi(g)(\chi) = \chi(g)$ per $\chi \in \hat{G}$. φ è un omomorfismo, ed è iniettiva, perché se non lo fosse, preso $1 \neq g \in \mathrm{Ker}(\varphi)$ e $H = \langle g\rangle$, tutti i caratteri $\chi \in \hat{G}$ passerebbero al quoziente per H, e cioè $\hat{G} = \widehat{(G/H)}$, assurdo per cardinalità. La surgettività segue invece per cardinalità, applicando due volte la proposizione precedente. □

Il risultato appena ottenuto è molto importante: ci assicura ad esempio che esiste un accoppiamento di dualità non degenere:

$$\begin{array}{ccc} G \times \hat{G} & \longrightarrow & \mathbb{C}^* \\ (g, \chi) & \longmapsto & \chi(g) \end{array}$$

Tale accoppiamento permette di introdurre un concetto di ortogonalità: se H è un sottogruppo di G, poniamo:

$$H^\perp = \{\chi \in \hat{G} \mid \chi(h) = 1 \ \forall h \in H\}.$$

Identificando inoltre $\hat{\hat{G}}$ con G, deduciamo immediatamente l'analoga definizione: se X è un sottogruppo di $\hat{G}$, poniamo:

$$X^\perp = \{g \in G \mid \chi(g) = 1 \ \forall \chi \in X\} = \bigcap_{\chi \in X} \mathrm{Ker}(\chi).$$

Osservazioni.
1. $H^\perp \cong \widehat{(G/H)}$. Infatti i caratteri $\chi \in H^\perp$ passano al quoziente per H, diventando caratteri di G/H, mentre viceversa un carattere di G/H può essere visto come un carattere di G banale su H.
2. $\hat{H} \cong \hat{G}/H^\perp$. Infatti la mappa di restrizione $\hat{G} \to \hat{H}$ è surgettiva e il suo nucleo è $H^\perp$.

3. $(H^\perp)^\perp = H$ tramite l'identificazione $\hat{\hat{G}} = G$. Infatti, vedendo un elemento $h \in H$ come una mappa $h : \chi \mapsto \chi(h)$ e viceversa, abbiamo il contenimento:

$$\begin{aligned}(H^\perp)^\perp &= \{g \in G \mid \chi(g) = 1 \ \forall \chi \in H^\perp\} = \\ &= \{g \in G \mid \chi(g) = 1 \ \forall \chi \text{ t.c. } H \subseteq \mathrm{Ker}(\chi)\} \supseteq H,\end{aligned}$$

che per questioni di cardinalità deve essere un'uguaglianza.

2.3 Applicazioni dei caratteri di Dirichlet

A questo punto vogliamo usare la teoria appena svolta per studiare in che modo i caratteri di Dirichlet ci aiutano nello studio del gruppo di Galois e della ramificazione nei campi di numeri.

Sia X un gruppo di caratteri di Dirichlet e sia K il suo campo associato. Abbiamo un accoppiamento di dualità non degenere:

$$\begin{array}{ccc}\mathrm{Gal}(K/\mathbb{Q}) \times X & \longrightarrow & \mathbb{C}^* \\ (\sigma, \chi) & \longmapsto & \chi(\sigma)\end{array}$$

analogo a quello visto nella sezione precedente.
Sia F un sottocampo di K; se $Y = \{\chi \in X \mid \chi(g) = 1 \ \forall g \in \mathrm{Gal}(K/F)\}$, da quanto visto abbiamo:

$$Y = \mathrm{Gal}(K/F)^\perp = (\mathrm{Gal}(K/\mathbb{Q})\hat{/}\,\mathrm{Gal}(K/F)) = (\mathrm{Gal}(\hat{F}/\mathbb{Q})).$$

Viceversa, se Y è un sottogruppo di X e F è il campo fissato da $Y^\perp$, allora $Y^\perp = \mathrm{Gal}(K/F)$, da cui $Y = (Y^\perp)^\perp = \mathrm{Gal}(K/F)^\perp = (\mathrm{Gal}(\hat{F}/\mathbb{Q}))$. Si ha dunque una corrispondenza biunivoca fra sottogruppi di X e sottocampi di K data da:

$$\begin{array}{ccc}\mathrm{Gal}(K/F)^\perp & \longleftrightarrow & F \\ Y & \longleftrightarrow & K^{Y^\perp}\end{array}$$

Come conseguenza otteniamo una corrispondenza biunivoca fra tutti i gruppi di caratteri di Dirichlet e sottocampi delle estensioni ciclotomiche.

Osservazioni. Siano $X_1, X_2 < X^{(n)}$ gruppi di caratteri di Dirichlet, e K_1, K_2 i rispettivi campi associati.

1. $X_1 \subseteq X_2 \iff K_1 \subseteq K_2$. Se infatti $H_i = \bigcap_{\chi \in X_i} \mathrm{Ker}(\chi)$, allora $X_1 \subseteq X_2 \iff H_1 \supseteq H_2 \iff (\mathbb{Q}^{(n)})^{H_1} \subseteq (\mathbb{Q}^{(n)})^{H_2}$.

2. Il campo associato al gruppo generato da X_1 e X_2 è il composto K_1K_2. Infatti $H = \bigcap_{\chi \in X_1X_2} \mathrm{Ker}(\chi) = H_1 \cap H_2$, dunque $(\mathbb{Q}^{(n)})^H = (\mathbb{Q}^{(n)})^{H_1 \cap H_2} = K_1K_2$.

Sia adesso $n = \prod_{i=1}^r p_i^{e_i}$. Data la decomposizione $(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{i=1}^r (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$, possiamo scomporre ogni carattere di Dirichlet χ definito modulo n come $\chi = \prod_{i=1}^r \chi_{p_i}$, dove χ_{p_i} è definito modulo $p_i^{e_i}$.
Tale decomposizione commuta con la moltiplicazione fra caratteri, cioè $(\chi\psi)_p = \chi_p\psi_p$. Inoltre, se χ è un carattere primitivo modulo p^a e ψ è un carattere primitivo modulo q^b, con p, q primi, $\chi\psi$ è un carattere primitivo modulo p^aq^b. Se infatti per assurdo il conduttore di $\chi\psi$ fosse un divisore di $p^{a-1}q^b$ (o simmetricamente di p^aq^{b-1}), allora scomponendo $\chi\psi = \chi'_p\psi'_q$ si avrebbe che χ deriva da χ'_p (o simmetricamente ψ deriva da ψ'_q), assurdo in quanto χ e ψ sono primitivi. Dunque, con una semplice induzione ricaviamo che, se $(f_\chi, f_\psi) = 1$, allora $\chi\psi(a) = \chi(a)\psi(a)$ per ogni a, cioè $f_{\chi\psi} = f_\chi f_\psi$.

Le prossime proposizioni forniscono alcune relazioni interessanti riguardanti somme di caratteri di Dirichlet, che ci saranno particolarmente utili nel prosieguo della trattazione.

Proposizione 2.3. *Sia χ un carattere non banale e $f = f_\chi$. Allora:*

$$\sum_{a=1}^{f} \chi(a) = \sum_{a \in (\mathbb{Z}/f\mathbb{Z})^*} \chi(a) = 0.$$

Dimostrazione. χ è non banale, quindi esiste b tale che $\chi(b) \neq 1$.

$$\chi(b) \sum_{a=1}^{f} \chi(a) = \sum_{a=1}^{f} \chi(ab) = \sum_{c=1}^{f} \chi(c),$$

dove $c = ab$, dunque segue la tesi. □

Proposizione 2.4. *Sia $n \in \mathbb{N}$ e scegliamo $a \in (\mathbb{Z}/n\mathbb{Z})^*$ diverso da 1. Allora:*

$$\sum_{\chi \in X^{(n)}} \chi(a) = 0.$$

Dimostrazione. Se riusciamo a trovare $\psi \in X^{(n)}$ tale che $\psi(a) \neq 1$, la tesi segue in modo analogo alla precedente. Indichiamo con $H = \bigcap_{\chi \in X^{(n)}} \mathrm{Ker}(\chi)$ l'ortogonale di $X^{(n)}$; se per assurdo $\chi(a) = 1$ per ogni $\chi \in X^{(n)}$, allora $\langle a \rangle$ sarebbe contenuto in H e cioè, posto $K = (\mathbb{Q}^{(n)})^H$, il grado $[\mathbb{Q}^{(n)} : K]$ sarebbe maggiore di 1, assurdo. □

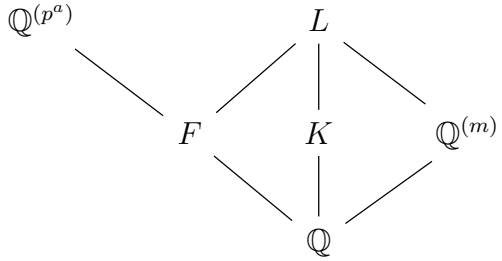
Corollario 2.5. *Sia $X < X^{(n)}$ un gruppo di caratteri e sia $a \in (\mathbb{Z}/n\mathbb{Z})^*$ diverso da 1. Allora:*

$$\sum_{\chi \in X} \chi(a) = 0.$$

Vediamo adesso come i caratteri di Dirichlet intervengono nello studio della ramificazione nelle estensioni dei razionali.

Teorema 2.6. *Sia X un gruppo di caratteri di Dirichlet e sia K il suo campo associato. Sia p un primo con indice di ramificazione e in K. Allora $e = |X_p|$, dove $X_p = \{\chi_p \mid \chi \in X\}$.*

Dimostrazione. Sia $n = \text{lcm}\{f_\chi \mid \chi \in X\}$. Allora $K \subseteq \mathbb{Q}^{(n)}$. Sia $n = p^a m$, con $(p, m) = 1$, e poniamo $L = K(\zeta_m) = K\mathbb{Q}^{(m)}$. Abbiamo dunque un diagramma:



dove $F \subseteq \mathbb{Q}^{(p^a)}$ è il campo associato a X_p. Infatti il gruppo dei caratteri di L è generato da X e dai caratteri di $(\mathbb{Z}/n\mathbb{Z})^*$ di conduttore coprimo con p, cioè i caratteri modulo m; dunque è il prodotto di X_p con i caratteri di $\mathbb{Q}^{(m)}$. Di conseguenza L è il composto di $\mathbb{Q}^{(m)}$ e del campo $F \subseteq \mathbb{Q}^{(p^a)}$ associato a X_p. Visto che p non ramifica in $\mathbb{Q}^{(m)}$, l'indice di ramificazione di p in K è lo stesso dell'indice di ramificazione di p in L, in quanto l'essere non ramificato si conserva nel traslato. Visto che per la stessa proprietà p non ramifica in L/F, l'indice di ramificazione di p in L è lo stesso di quello di p in F, che è $[F : \mathbb{Q}] = |X_p|$, in quanto p ramifica totalmente in F. □

Corollario 2.7. *Sia χ un carattere di Dirichlet e K il suo campo associato. Allora p ramifica in K se e solo se $\chi(p) = 0$, cioè $p \mid f_\chi$.*
Più in generale, se L è il campo associato a un gruppo X di caratteri di Dirichlet, p è non ramificato in L se e solo se $\chi(p) \neq 0$ per ogni $\chi \in X$.

Dimostrazione. p ramifica in $L \iff X_p \neq \{1\} \iff \exists \chi \in X$ tale che $\chi_p \neq 1 \iff \exists \chi \in X$ tale che $p \mid f_\chi \iff \exists \chi \in X$ tale che $\chi(p) = 0$. □

Teorema 2.8. *Sia X un gruppo di caratteri di Dirichlet e sia K il campo associato. Siano $Y = \{\chi \in X \mid \chi(p) \neq 0\}$ e $Z = \{\chi \in X \mid \chi(p) = 1\}$. Allora:*

$$e = [X : Y], \qquad f = [Y : Z], \qquad r = |Z|,$$

dove i numeri e, f, r sono rispettivamente l'indice di ramificazione di p in K, il grado del campo residuo e il numero di primi di K sopra p. Più precisamente:

$$\frac{X}{Y} \cong E, \qquad \frac{X}{Z} \cong D, \qquad \frac{Y}{Z} \cong \mathbb{Z}/f\mathbb{Z},$$

dove E e D sono rispettivamente il gruppo di inerzia e il gruppo di ramificazione di p in K.

Dimostrazione. Sia L il sottocampo di K associato a Y. Per il corollario precedente, L è la sottoestensione massimale di K in cui p non è ramificato. Dunque, per fatti standard di teoria algebrica dei numeri, $L = K^E$, cioè $E = \mathrm{Gal}(K/L)$.
Tramite la corrispondenza fra sottocampi di K e sottogruppi di X, abbiamo $Y = \mathrm{Gal}(K/L)^\perp$, quindi:

$$\frac{X}{Y} = \frac{(\mathrm{Gal}(\hat{K}/\mathbb{Q}))}{\mathrm{Gal}(K/L)^\perp} = (\mathrm{Gal}(\hat{K}/L)) \cong \mathrm{Gal}(K/L) \cong E.$$

Sia ora $n = \mathrm{lcm}\{f_\chi \mid \chi \in Y\}$; visto che p non ramifica in $L \subseteq \mathbb{Q}^{(n)}$, $p \nmid n$. Il Frobenius per p di $\mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ è la mappa $\zeta_n \mapsto \zeta_n^p$, che corrisponde a $p \in (\mathbb{Z}/n\mathbb{Z})^*$; visto che $\mathrm{Gal}(L/\mathbb{Q}) \cong \frac{(\mathbb{Z}/n\mathbb{Z})^*}{\mathrm{Gal}(\mathbb{Q}^{(n)}/L)}$, il Frobenius σ_p per p di $L/\mathbb{Q}$ è la classe laterale di p in tale quoziente. Ma gli elementi di Y sono banali su $\mathrm{Gal}(\mathbb{Q}^{(n)}/L)$, quindi $\chi(\sigma_p) = \chi(p)$ e $\chi(\sigma_p) = 1 \iff \chi(p) = 1$, cioè $Z = \langle\sigma_p\rangle^\perp$ tramite l'accoppiamento di dualità $\mathrm{Gal}(L/\mathbb{Q}) \times Y \to \mathbb{C}^*$. $\langle\sigma_p\rangle$ ha ordine f, e visto che $\frac{Y}{Z} \cong (\hat{\langle\sigma_p\rangle}) \cong \langle\sigma_p\rangle$ abbiamo anche la seconda uguaglianza.
Infine, ricordando che il gruppo di decomposizione D di p è generato da E e σ_p, come sopra otteniamo che $[X : Z] = ef$ e $\frac{X}{Z} \cong D$. □

2.4 Somme di Gauss

Come abbiamo già potuto vedere, esistono formule e relazioni interessanti riguardanti somme di caratteri di Dirichlet; un tipo di somme particolarmente utili sono le cosiddette somme di Gauss, di cui studieremo alcune proprietà.

Sia χ un carattere di Dirichlet di conduttore $f = f_\chi$ e sia ζ_f la radice f-esima primitiva di 1 scelta nel modo usuale, cioè $\zeta_f = e^{\frac{2\pi i}{f}}$.

Definizione 2.2. Si definisce somma di Gauss relativa a χ la somma:

$$g(\chi) = \sum_{a=1}^{f} \chi(a)\zeta_f^a.$$

Se χ ha ordine m, si ha che $g(\chi) \in \mathbb{Q}^{(mf)}$.

Lemma 2.9. *Sia $\chi \neq 1$ e poniamo $g_m(\chi) = \sum_{a=1}^{f} \chi(a)\zeta_f^{am}$. Allora $g_m(\chi) = \overline{\chi}(m)g(\chi)$.*

Dimostrazione. Assumiamo come primo caso che $(f, m) = 1$. Visto che $\overline{\chi}(m)\chi(m) = 1$, abbiamo:

$$g_m(\chi) = \overline{\chi}(m) \sum_{a=1}^{f} \chi(am)\zeta_f^{am} = \overline{\chi}(m) \sum_{a=1}^{f} \chi(a)\zeta_f^{a} = \overline{\chi}(m)g(\chi).$$

Se invece $g = \gcd(f, m) > 1$, supponiamo $m = m'g$ e $f = f'g$. Banalmente vale l'uguaglianza:

$$\sum_{a=1}^{f} \chi(a)\zeta_f^{am} = \sum_{s=1}^{f'} \left(\sum_{\substack{a=1 \\ a \equiv s \pmod{f'}}}^{f} \chi(a) \right) \zeta_{f'}^{m's}.$$

Se $S = \{k \in (\mathbb{Z}/f\mathbb{Z})^* \mid k \equiv 1 \pmod{f'}\} < (\mathbb{Z}/f\mathbb{Z})^*$, allora sappiamo che

$$\sum_{k \in S} \chi(k) = 0, \quad \text{da cui} \quad \sum_{k \in jS} \chi(k) = 0$$

per ogni j tale che $(\mathbb{Z}/f\mathbb{Z})^* = \bigsqcup_j jS$. Ma allora la somma fra parentesi della precedente uguaglianza è sempre 0, da cui la tesi. □

Proposizione 2.10. *1. $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$.*

2. Se $\chi \neq 1$, $|g(\chi)|^2 = g(\chi)\overline{g(\chi)} = f$.

3. Se $\chi \neq 1$, $g(\chi)g(\overline{\chi}) = \chi(-1)f$.

Dimostrazione. La prima identità è evidente, e l'ultima segue dalle prime due. Vediamo quindi la seconda. Per il lemma:

$$\begin{aligned} g(\chi)\overline{g(\chi)} &= \sum_{a=1}^{f} \overline{\chi}(a)g(\chi)\zeta_f^{-a} = \sum_{a=1}^{f} \sum_{b=1}^{f} \chi(b)\zeta_f^{ab}\zeta_f^{-a} = \\ &= \sum_{b=1}^{f} \chi(b) \sum_{a=1}^{f} \zeta_f^{(b-1)a} = f, \end{aligned}$$

in quanto l'ultima somma interna vale 0 se $b \neq 1$ e f se $b = 1$.

□

Capitolo 3

Rappresentazioni di Artin

Obiettivo di questo terzo capitolo è dimostrare la formula conduttore - discriminante, passando per la teoria delle rappresentazioni di Artin. Sottolineiamo che questa non è assolutamente la strada più breve né quella più semplice (ad esempio una dimostrazione basata sulle L-serie di Dirichlet può essere trovata in [17]), ma la preferiamo in quanto permette di introdurre concetti di fondamentale importanza in teoria dei numeri.

Come prima cosa rivediamo alcune definizioni base della teoria delle rappresentazioni; le dimostrazioni dei risultati che richiameremo possono essere consultate in [15]. Assumeremo inoltre molti fatti riguardanti i gruppi di ramificazione di campi locali; una trattazione completa che include tali risultati è contenuta in [16].

3.1 Richiami di teoria delle rappresentazioni

Sia G un gruppo finito di ordine g. Una funzione di classe su G è una funzione $f : G \to \mathbb{C}$ costante sulle classi di coniugio, cioè tale che $f(sts^{-1}) = f(t)$ per ogni $s, t \in G$. Indicheremo con $\mathbb{C}_{classe}(G)$ l'insieme delle funzioni di classe. Sia inoltre V uno spazio vettoriale di dimensione finita su $\mathbb{C}$ e sia $\mathrm{GL}(V) = \mathrm{Aut}_{\mathbb{C}}(V)$ il gruppo degli automorfismi di V come $\mathbb{C}$-spazio vettoriale. Definiamo una rappresentazione di G in V come un omomorfismo

$$\rho : G \longrightarrow \mathrm{GL}(V).$$

Si nota subito che, grazie a ρ, V assume una struttura di $\mathbb{C}[G]$-modulo. Definiamo inoltre il carattere della rappresentazione ρ come:

$$\chi_\rho(s) = \mathrm{tr}(\rho(s)),$$

dove tr indica la funzione traccia; evidentemente χ_ρ è una funzione di classe e, data la finitezza di G, vale anche la relazione $\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}$.
L'intero $\chi_\rho(1)$ non è altro che la dimensione di V, e viene chiamato grado della rappresentazione.

Esempi.

1. Il carattere della rappresentazione banale è la funzione costantemente 1.

2. Il carattere della rappresentazione regolare di G (data dall'azione di G su $\mathbb{C}[G]$ per moltiplicazione a sinistra) è la mappa $r_G : G \to \mathbb{C}$ tale che $r_G(1) = g$ e $r_G(s) = 0$ per $s \neq 1$.

3. La rappresentazione banale si immerge in quella regolare; il loro quoziente prende il nome di rappresentazione di augmentazione e il suo carattere u_G è tale che $r_G = u_G + 1$; equivalentemente, la rappresentazione di augmentazione può essere vista come l'azione di G su $I_G = \langle s - 1 \mid s \in G \rangle \lhd \mathbb{C}[G]$, con I_G presente nella successione esatta:

$$0 \hookrightarrow I_G \longrightarrow \mathbb{C}[G] \xrightarrow{s \mapsto 1} \mathbb{C} \longrightarrow 0.$$

Diremo che il carattere di una rappresentazione è irriducibile se la rappresentazione è irriducibile, (equivalentemente se V è un $\mathbb{C}[G]$-modulo semplice, cioè non ha sottomoduli non banali). I caratteri irriducibili di G sono una base per $\mathbb{C}_{classe}(G)$ (cfr. [15], §1.4), e, posto in $\mathbb{C}_{classe}(G)$ il prodotto hermitiano:

$$(\varphi, \psi)_G = \frac{1}{g} \sum_{s \in G} \varphi(s)\overline{\psi(s)},$$

i caratteri irriducibili risultano ortonormali rispetto a tale prodotto. Da questo si ottiene che, se $\varphi = \sum_\chi c_\chi \chi$ è una funzione di classe decomposta nella somma di caratteri irriducibili, il coefficiente c_χ non è altro che $c_\chi = (\varphi, \chi)_G$. Usando inoltre la relazione $\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$ e la decomposizione di una rappresentazione in sottorappresentazioni irriducibili, abbiamo che una funzione di classe $\sum_\chi c_\chi \chi$ è un carattere di una rappresentazione se e solo se $c_\chi \geq 0$ per ogni χ.
Ad esempio è immediato osservare che valgono le decomposizioni:

$$r_G = \sum_\chi \chi(1)\chi, \qquad u_G = \sum_{\chi \neq 1} \chi(1)\chi.$$

Sia adesso H un gruppo finito e $\alpha : H \to G$ un omomorfismo; se $\varphi \in \mathbb{C}_{classe}(G)$, ovviamente $\alpha^*(\varphi) := \varphi \circ \alpha \in \mathbb{C}_{classe}(H)$, e se $\varphi = \chi_\rho$ è il carattere di una certa rappresentazione ρ, $\alpha^*(\varphi)$ è il carattere della rappresentazione

$\rho \circ \alpha$. Viceversa, se $\psi \in \mathbb{C}_{classe}(H)$, il teorema di Frobenius (cfr. [15], §7.2) garantisce per qualsiasi funzione di classe φ l'esistenza e unicità di $\alpha_*(\psi) \in \mathbb{C}_{classe}(G)$ tale che:

$$(\varphi, \alpha_*(\psi))_G = (\alpha^*(\varphi), \psi)_H.$$

Si osserva inoltre che se ψ è il carattere di una rappresentazione di H in V, allora $\alpha_*(\psi)$ è il carattere della rappresentazione $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ ottenuta per estensione degli scalari. In tale situazione $\alpha_*(\psi)$ è detta rappresentazione indotta di ψ in G.

Osservazione. Supponiamo che H sia un sottogruppo di G e α sia l'inclusione. Scriveremo allora φ per $\alpha^*(\varphi)$ e ψ^* per $\alpha_*(\psi)$. Vista l'unicità della rappresentazione indotta, una semplice verifica permette di ottenere la relazione:

$$\psi^*(s) = \sum_{t \in G/H} \psi(tst^{-1})$$

(con la convenzione che $\psi(a) = 0$ se $a \notin H$).
Se invece G è il quoziente H/N di H e $\alpha = \pi$ è la proiezione, scriveremo φ per $\alpha^*(\varphi)$ e $\psi^\natural$ per $\alpha_*(\psi)$. Come sopra, con una semplice verifica si ottiene che:

$$\psi^\natural(s) = \frac{1}{|N|} \sum_{t \to s} \psi(t),$$

dove $t \to s$ indica che $[t] = s$ in H/N.

3.2 Rappresentazioni di Artin in campi locali

Dopo questo riepilogo, poniamoci nell'ambiente più consono per lo studio delle rappresentazioni di Artin. Sia K un campo completo rispetto a una valutazione discreta v_K, $\mathscr{O}_K$ il suo anello di valutazione e P_K l'unico ideale massimale di $\mathscr{O}_K$. Indichiamo con k_K il campo residuo $\frac{\mathscr{O}_K}{P_K}$ e con $U_K = \mathscr{O}_K \backslash P_K$ l'insieme degli elementi invertibili di $\mathscr{O}_K$.
Se L è un'estensione finita e di Galois di K con gruppo di Galois G, denotiamo con $\mathscr{O}_L$ la chiusura integrale di $\mathscr{O}_K$ in L e supponiamo che l'estensione dei campi residui k_L/k_K sia separabile; indichiamo come al solito con $e = e_{L/K}$ e $f = f_{L/K}$ l'indice di ramificazione e il grado d'inerzia dell'estensione.

Sia $s \in G$ un elemento diverso dall'identità e definiamo la funzione i_G tale che $i_G(s) = v_L(s(x) - x)$, dove x è un generatore di $\mathscr{O}_L$ come $\mathscr{O}_K$-modulo; dalla definizione si ha che $i_G(s) \geq i + 1 \iff s \in G_i$, dove $G_i = \{s \in G \mid$

$v_L(s(x) - x) \geq i + 1\}$ indica l'i-esimo gruppo di ramificazione. Definiamo quindi una funzione:

$$a_G(s) = \begin{cases} -f \cdot i_G(s) & \text{se } s \neq 1 \\ f \cdot \sum_{s \neq 1} i_G(s) & \text{se } s = 1 \end{cases}$$

Evidentemente $\sum_{s \in G} a_G(s) = 0$. Inoltre $a_G(s) \in \mathbb{C}_{classe}(G)$, in quanto i G_i sono sottogruppi normali di G, quindi possiamo scriverla come una somma:

$$a_G = \sum_{\chi} c_\chi \chi,$$

dove:

$$c_\chi = (a_G, \chi)_G = \frac{1}{g} \sum_{s \in G} a_G(s)\chi(s^{-1}) = \frac{1}{g} \sum_{s \in G} a_G(s^{-1})\chi(s) = (\chi, a_G)_G.$$

Poniamo infine $f(\varphi) = (\varphi, a_G)_G$ per ogni $\varphi \in \mathbb{C}_{classe}(G)$.

Le prossime proposizioni saranno tutte incentrate sullo studio di tali numeri $f(\varphi)$; in particolare cercheremo formule esplicite che ci permetteranno di giungere a un punto di contatto fra la teoria dei caratteri di Dirichlet vista nel capitolo precedente e la teoria delle rappresentazioni di Artin che stiamo per sviluppare.

Proposizione 3.1. *La funzione a_G coincide con la funzione a_E^* indotta dalla corrispondente funzione relativa al gruppo d'inerzia $E = G_0$.*

Dimostrazione. Visto che $E \triangleleft G$, $a_E^*(s) = 0 = a_G(s)$ se $s \notin E$. Se invece $s \in E \backslash \{1\}$, allora:

$$a_E^*(s) = \sum_{t \in G/E} a_E(tst^{-1}) = -\sum_{t \in G/E} i_E(tst^{-1}) = -f \cdot i_G(s) = a_G(s),$$

in quanto G/E è il gruppo di Galois dell'estensione L^E/K, che non è ramificata.
Il caso $s = 1$ segue infine per differenza. □

Proposizione 3.2. *Sia u_i il carattere della rappresentazione di augmentazione di G_i e sia u_i^* il carattere di G indotto da u_i. Allora:*

$$a_G = \sum_{i=0}^{\infty} \frac{1}{[E : G_i]} u_i^*.$$

Dimostrazione. Posto $g_i = |G_i|$, dalla definizione di rappresentazione di augmentazione segue facilmente che $u_i^*(s) = -\frac{g}{g_i} = -f \cdot \frac{g_0}{g_i}$ per ogni $s \in G_i \backslash \{1\}$, mentre $u_i^*(s) = 0$ se $s \notin G_i$. Ma allora, se $s \in G_i \backslash G_{i+1}$, la somma sulla destra vale $-(i+1)f$, esattamente come $a_G(s)$. Il caso $s = 1$ può essere ottenuto facilmente per differenza osservando che entrambi i membri sono ortogonali alla funzione identicamente 1. □

Mantenendo la notazione precedente $g_i = |G_i|$, poniamo per ogni $\varphi \in \mathbb{C}_{classe}(G)$:

$$\varphi(G_i) = \frac{1}{g_i} \sum_{s \in G_i} \varphi(s).$$

Nel caso in cui φ sia il carattere χ di una rappresentazione ρ di G in V, il numero $\chi(G_i)$ coincide con la dimensione del sottospazio V^{G_i} di V fissato da G_i. Infatti, se ϕ è la mappa di G_i-moduli $\phi = \frac{1}{g_i} \sum_{s \in G_i} \rho(s)$ e $h \in G_i$, abbiamo:

$$h\phi(v) = h\left(\frac{1}{g_i} \sum_{s \in G_i} sv\right) = \frac{1}{g_i} \sum_{s \in G_i} (hs)v = \phi(v),$$

cioè l'immagine di ϕ è contenuta in V^{G_i} e ϕ agisce come l'identità su V^{G_i}. Da questo ricaviamo la formula:

$$\dim(V^{G_i}) = \mathrm{tr}(\varphi) = \frac{1}{g_i} \sum_{s \in G_i} \chi(s),$$

spesso chiamata prima formula di proiezione.

Corollario 3.3. *Se $\varphi \in \mathbb{C}_{classe}(G)$, allora:*

$$f(\varphi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} (\varphi(1) - \varphi(G_i)).$$

Dimostrazione. Basta notare che:

$$(\varphi, u_i^*)_G = (\varphi, u_i)_{G_i} = \frac{\varphi(1)(g_i - 1)}{g_i} - \frac{1}{g_i} \sum_{s \neq 1} \varphi(s) = \varphi(1) - \varphi(G_i).$$

□

Corollario 3.4. *Se χ è il carattere di una rappresentazione di G in V, allora:*

$$f(\chi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \,\mathrm{codim}(V^{G_i}),$$

dove V^{G_i} è il sottospazio di V fissato da G_i.

Dimostrazione. Segue immediatamente dal corollario precedente, in quanto $\chi(1) = \dim(V)$ e $\chi(G_i) = \dim(V^{G_i})$ per la prima formula di proiezione. □

Corollario 3.5. *Se χ è un carattere di G, allora $f(\chi) \in \mathbb{Q}_{\geq 0}$.*

Dimostrazione. Per il corollario precedente, $g_0 f(\chi)$ è un intero positivo. □

Proposizione 3.6. *Se $N \triangleleft G$, allora $a_{G/N} = a_G^\natural$.*

Dimostrazione. Se F è il sottocampo di L fissato da N, scrivendo $f = f_{L/F} f_{F/K}$ la tesi segue immediatamente dalla nota uguaglianza:

$$i_{G/N}(s) = \frac{1}{e_{L/F}} \sum_{\sigma \to s} i_G(\sigma).$$

□

Corollario 3.7. *Se $\varphi \in \mathbb{C}_{classe}(G/N)$ e $\varphi' \in \mathbb{C}_{classe}(G)$ è la corrispondente funzione di classe in G, allora $f(\varphi) = f(\varphi')$.*

Dimostrazione. Grazie alla proposizione precedente, abbiamo che:

$$f(\varphi) = (\varphi, a_G^\natural)_{G/N} = (\varphi', a_G)_G = f(\varphi').$$

□

Proposizione 3.8. *Sia H un sottogruppo di G e poniamo $K' = K^H$. Se $\lambda = v_K(\mathrm{disc}(K'/K))$, allora vale l'identità:*

$$a_G = \lambda r_H + f_{K'/K} \cdot a_H,$$

dove con a_G si indica il carattere a_G ristretto ad H.

Dimostrazione. Se $s \in H \backslash \{1\}$, $r_H(s) = 0$, quindi basta ricordare che $a_G(s) = -f_{L/K} i_G(s)$ e $a_H(s) = -f_{L/K'} i_H(s)$, e poiché $i_G(s) = i_H(s)$ la formula segue. Se invece $s = 1$, ricordiamo la formula che lega la valutazione di $\mathfrak{D}_{L/K}$ ai gruppi di ramificazione:

$$v_L(\mathfrak{D}_{L/K}) = \sum_{s \neq 1} i_G(s).$$

Da tale formula otteniamo $a_G(1) = f_{L/K} v_L(\mathfrak{D}_{L/K}) = v_K(\mathrm{disc}(L/K))$, in quanto $\mathrm{disc}(L/K) = \mathrm{N}_{L/K}(\mathfrak{D}_{L/K})$, e analogamente $a_H(1) = v_{K'}(\mathrm{disc}(L/K'))$. Riscrivendo la tesi come:

$$v_K(\mathrm{disc}(L/K)) = [L : K'] v_K(\mathrm{disc}(K'/K)) + f_{K'/K} v_{K'}(\mathrm{disc}(L/K')),$$

essa segue immediatamente dalla formula del discriminante nelle torri (cfr. [16], §3.4):

$$\mathrm{disc}(L/K) = (\mathrm{disc}(K'/K))^{[L:K']}\,\mathrm{N}_{K'/K}(\mathrm{disc}(L/K')).$$

□

Corollario 3.9. *Se ψ è un carattere di H e ψ^* è come al solito il carattere indotto su G, allora:*

$$f(\psi^*) = v_K(\mathrm{disc}(K'/K))\psi(1) + f_{K'/K}f(\psi).$$

Dimostrazione. La proposizione precedente dice subito:

$$\begin{aligned} f(\psi^*) &= (\psi^*, a_G)_G = (\psi, a_G)_H = \lambda(\psi, r_H)_H + f_{K'/K}(\psi, a_H)_H = \\ &= \lambda\psi(1) + f_{K'/K}f(\psi), \end{aligned}$$

dove $\lambda = v_K(\mathrm{disc}(K'/K))$. □

Con le formule appena mostrate riusciamo finalmente ad intuire il legame fra il discriminante di sottoestensioni di L/K e i numeri $f(\chi)$; per di più, assumendo alcuni forti teoremi riguardanti i gruppi di ramificazione con indice in alto, siamo in grado di dedurre relazioni ancora più affascinanti ed esplicative. Posto $G_t = G_{\lceil t \rceil}$ se $t \notin \mathbb{Z}$, indichiamo innanzitutto con

$$\varphi_{L/K}(u) = \int_0^u \frac{dt}{[G_0 : G_t]}$$

la funzione che permette di passare dalla numerazione dei gruppi di ramificazione in basso a quella in alto; richiamiamo poi i famosi teoremi di Herbrandt e Hasse-Arf, la cui dimostrazione è come al solito consultabile in [16]:

Teorema 3.10 (Herbrandt)**.** *Se H è un sottogruppo normale di G e K' è il campo fissato da H, allora $G_uH/H = (G/H)_v$, dove $v = \varphi_{L/K'}(u)$.*

Teorema 3.11 (Hasse-Arf)**.** *Se G è abeliano, i salti in alto della ramificazione sono numeri interi.*

Grazie a questi potenti risultati, deduciamo facilmente le seguenti relazioni:

Proposizione 3.12. *Sia χ un carattere di grado 1 su G. Sia c_χ il più grande intero per cui la restrizione di χ a G_{c_χ} sia diversa dal carattere banale (con la convenzione $c_1 = -1$). Allora:*

$$f(\chi) = \varphi_{L/K}(c_\chi) + 1.$$

Dimostrazione. Sapendo che per un carattere χ di grado 1 non banale vale la relazione $\sum_s \chi(s) = 0$, abbiamo facilmente che $\chi(G_i) = 0$ se $i \leq c_\chi$, mentre $\chi(G_i) = 1$ se $i > c_\chi$. Da questo segue:

$$f(\chi) = \sum_{i=0}^{c_\chi} \frac{g_i}{g_0} = \varphi_{L/K}(c_\chi) + 1.$$

□

Corollario 3.13. *Sia $H = \mathrm{Ker}(\chi)$ e sia K' il campo associato a $\langle\chi\rangle$, cioè $K' = L^H$. Indichiamo con c'_χ il più grande intero per cui $(G/H)_{c'_\chi} \neq 1$, cioè l'ultimo salto della ramificazione di G/H. Allora:*

$$f(\chi) = \varphi_{K'/K}(c'_\chi) + 1 \in \mathbb{N},$$

dove conveniamo che $c'_\chi = -1$ se $H = G$.

Dimostrazione. Per il teorema di Herbrand, $c'_\chi = \varphi_{L/K'}(c_\chi)$, quindi l'uguaglianza della tesi segue dalla transitività della funzione φ. Inoltre il fatto $\varphi_{K'/K}(c'_\chi) \in \mathbb{Z}$ segue dal teorema di Hasse-Arf, in quando il quoziente G/H è abeliano. □

Richiamiamo un noto teorema, dovuto a Brauer, di cui tralasciamo la dimostrazione, anch'essa presente in [15]:

Teorema 3.14 (Brauer)**.** *Ogni carattere di G è combinazione lineare su $\mathbb{Z}$ di caratteri χ_i^* indotti da caratteri χ_i di grado 1 di sottogruppi H_i di G.*

Teorema 3.15. *$f(\chi) \in \mathbb{N}$ per ogni carattere χ di G.*

Dimostrazione. Per il teorema di Brauer, possiamo scrivere $\chi = \sum_i n_i \chi_i^*$, dove $n_i \in \mathbb{Z}$ e i χ_i sono caratteri di grado 1 di sottogruppi H_i di G. Ma visto che per l'ultimo corollario $f(\chi_i) \in \mathbb{N}$, la formula $f(\chi_i^*) = v_K(\mathrm{disc}(K'/K))\psi(1) + f_{K'/K} f(\chi_i)$ dà la tesi. □

Corollario 3.16. *a_G è il carattere di una rappresentazione di G, detta rappresentazione di Artin dell'estensione L/K.*

3.3 Rappresentazioni di Artin in campi di numeri

La teoria affrontata fino ad ora a livello locale ci permette di estendere tali risultati al livello globale, che è quello che veramente ci interessa. Diamo

quindi alcune notazioni per porsi nel setting adeguato.

Sia L/K un'estensione di Galois finita con gruppo di Galois G, siano $\mathscr{O}_K$ e $\mathscr{O}_L$ gli anelli degli interi e sia Q un primo di $\mathscr{O}_L$ sopra P primo di $\mathscr{O}_K$. Come ipotesi chiediamo anche che l'estensione dei campi residui k_L/k_K sia separabile. Sotto tali condizioni anche l'estensione completata L_Q/K_P risulta di Galois finita, con gruppo di Galois isomorfo al gruppo di decomposizione $D = D(Q|P)$. Denotiamo con a_Q il carattere della rappresentazione di Artin di L_Q/K_P definita sopra ed estendiamo il suo dominio a tutto G in modo che $a_Q(s) = 0$ se $s \notin D$. Poniamo:

$$a_P = \sum_{Q|P} a_Q.$$

È immediato osservare che $a_P = a_Q^*$ per ogni primo Q sopra P, cioè a_P è il carattere di una rappresentazione di G, detta la rappresentazione di Artin relativa a P dell'estensione L/K, e tale rappresentazione è indotta dalla rappresentazione di Artin di uno qualunque dei gruppi $D(Q|P)$. Inoltre, se χ è un carattere di G, poniamo:

$$f(\chi, P) = (\chi, a_P) = f(\chi_{|D(Q|P)})$$

e definiamo conduttore del carattere χ il prodotto:

$$f(\chi, L/K) = f(\chi) = \prod_P P^{f(\chi,P)}.$$

Notiamo subito che il precedente è un prodotto finito, in quanto $f(\chi, P) = 0$ se P non ramifica in L; inoltre tale definizione di conduttore estende quella da noi data nel caso particolare dei caratteri di Dirichlet. Infatti, se χ è un carattere di Dirichlet primitivo modulo p^e, per il corollario 3.13 abbiamo che $f(\chi, p) = e$, in quanto $\mathrm{Ker}(\chi) = \{1\}$ e l'ultimo salto in alto della ramificazione dell'estensione $\mathbb{Q}_p(\zeta_{p^e})/\mathbb{Q}_p$ è proprio $e - 1$.

Le proprietà viste precedentemente nel caso locale si estendono in modo naturale al caso globale grazie alla definizione precedente; in particolare i corollari 3.3, 3.9 e 3.7 si traducono:

Proposizione 3.17. *1.* $f(1) = (1)$.

2. $f(\chi + \chi') = f(\chi) \cdot f(\chi')$.

3. *Se H è un sottogruppo di G, $K' = K^H$ è il sottocampo fissato da H e ψ è un carattere di H, allora:*

$$f(\psi^*, L/K) = \mathrm{disc}(K'/K)^{\psi(1)}\, \mathrm{N}_{K'/K}(f(\psi, L/K')).$$

4. *Se K'/K è di Galois e χ è un carattere di G/H, allora $f(\chi, L/K) = f(\chi, K'/K)$.*

Da questa centrale proposizione siamo in grado di dedurre la formula conduttore-discriminante voluta: se infatti applichiamo il punto 3) al carattere $\psi = 1_H$ e denotiamo con $s_{G/H}$ il carattere indotto ψ^*, otteniamo:

Corollario 3.18. $\mathrm{disc}(K'/K) = f(s_{G/H}, L/K)$.

Infine, se $H = \{1\}$, allora $s_{G/H}$ non è altro che la rappresentazione regolare di G, e dunque, ricordando che

$$r_G = \sum_\chi \chi(1)\chi,$$

dove la somma varia su tutti i carattere irriducibili di G, abbiamo finalmente:

Corollario 3.19 (Formula conduttore-discriminante)**.** $\mathrm{disc}(L/K) = \prod_\chi f(\chi)^{\chi(1)}$*, dove il prodotto varia fra tutti i caratteri irriducibili di G.*

Se G è abeliano, la formula si semplifica, in quanto i caratteri irriducibili hanno tutti grado 1:

Corollario 3.20. *Se G è abeliano, allora* $\mathrm{disc}(L/K) = \prod_\chi f(\chi)$*, dove il prodotto varia fra tutti i caratteri irriducibili di G.*

Dopo tanto sforzo, siamo riusciti ad ottenere questa importantissima formula che collega due capitoli a prima vista separati della teoria dei numeri. Se ci limitiamo solamente al caso $K = \mathbb{Q}$, l'ultimo corollario fornisce un'uguaglianza fra ideali che non dà nessuna informazione sul segno del discriminante di L; per questo ci viene in aiuto un fatto standard di teoria algebrica dei numeri, che per completezza riportiamo di seguito:

Proposizione 3.21. *Sia L un campo di numeri e indichiamo con r il numero delle immersioni reali dell'estensione $L/\mathbb{Q}$ e con $2s$ quello delle immersioni complesse. Allora il segno del discriminante di L è $(-1)^s$.*

Ricapitolando, se L è un campo di numeri e il gruppo di Galois G dell'estensione $L/\mathbb{Q}$ è abeliano, allora vale la formula:

$$\mathrm{disc}(L) = (-1)^s \prod_{\chi \in X} f_\chi,$$

dove X indica il gruppo dei caratteri di Dirichlet di G.

Capitolo 4

Il teorema di Leopoldt

In questo ultimo capitolo ci accingiamo a dimostrare il teorema principale della trattazione, il teorema di Leopoldt. Per farlo abbiamo prima bisogno di studiare a fondo la struttura dell'anello degli interi di un campo di numeri abeliano: introdurremo perciò alcuni strumenti particolarmente utili, come gli idempotenti ortogonali e le coordinate di carattere, con cui otterremo risultati di estremo interesse.

Riprendiamo subito alcune notazioni. Per ogni $n \in \mathbb{N}$ denotiamo con ζ_n una radice n-esima primitiva dell'unità e con $\mathbb{Q}^{(n)} = \mathbb{Q}^{(n)}$ l'n-esima estensione ciclotomica dei razionali. Scegliamo inoltre le ζ_n in modo coerente, cioè in modo che, dati qualsiasi $k \mid l$, $\zeta_l^{\frac{l}{k}} = \zeta_k$.
Indichiamo con $G^{(n)} = \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ il gruppo di Galois dell'estensione $\mathbb{Q}^{(n)}/\mathbb{Q}$ e con $\sigma_k \in G^{(n)}$ l'automorfismo tale che $\sigma_k(\zeta_n) = \zeta_n^k$; identifichiamo inoltre il gruppo dei caratteri $\hat{G^{(n)}}$ con il gruppo $X^{(n)}$ dei caratteri modulo n, cioè con conduttore divisore di n.

Sia adesso $n \not\equiv 2 \pmod 4$ e scomponiamo $n = \prod_{i=1}^r p_i^{e_i}$ in fattori primi; per la teoria vista si ha una decomposizione di ogni carattere $\chi \in X^{(n)}$ come $\chi = \prod_{i=1}^r \chi_{p_i}$, dove χ_{p_i} è definito modulo $p_i^{e_i}$, cioè $\chi_{p_i} \in X^{(p_i^{e_i})}$. Dato che banalmente si ha l'uguaglianza:

$$X^{(p_i^{e_i})} = \{\chi_{p_i} \mid \chi \in X^{(n)}\},$$

otteniamo la decomposizione $X^{(n)} = \prod_{i=1}^r X^{(p_i^{e_i})}$. D'altra parte, vista la coprimalità dei p_i, segue che il conduttore di un carattere $\chi \in X^{(n)}$ coincide con il prodotto dei conduttori dei χ_{p_i}.

Restringiamoci perciò a studiare un primo alla volta: sia p primo e sia e tale che $p^e \not\equiv 2 \pmod 4$. Da risultati standard di teoria dei gruppi si

ha che $(\mathbb{Z}/p^e\mathbb{Z})^* \cong (\mathbb{Z}/\overline{p}\mathbb{Z})^* \times \frac{1+\overline{p}\mathbb{Z}}{1+p^e\mathbb{Z}}$, dove $\overline{p} = p$ se $p \neq 2$ e $\overline{p} = 4$ se $p = 2$. Passando al duale di tale decomposizione, otteniamo l'altra scrittura $X^{(p^e)} = \langle \omega_p \rangle \times \langle \psi_{p^e} \rangle$, dove $\langle \omega_p \rangle$ è il gruppo dei caratteri modulo $\overline{p}$ e $\langle \psi_{p^e} \rangle$ è il gruppo dei caratteri modulo p^e banali fuori da $1 + \overline{p}\mathbb{Z}$.

Sia $\chi = \omega_p^a \psi_{p^e}^b \in X^{(p^e)}$; ψ_{p^e} è banale sul dominio di ω_p, quindi riusciamo ad calcolare esplicitamente il conduttore di χ:

$$f_\chi = \begin{cases} p^{e-v_p(b)} & \text{se } b \not\equiv 0 \pmod{\frac{p^e}{\overline{p}}} \\ \overline{p} & \text{se } b \equiv 0 \pmod{\frac{p^e}{\overline{p}}} \wedge a \not\equiv 0 \pmod{\varphi(\overline{p})} \\ 1 & \text{se } b \equiv 0 \pmod{\frac{p^e}{\overline{p}}} \wedge a \equiv 0 \pmod{\varphi(\overline{p})} \end{cases}$$

dove φ è la funzione di Eulero e v_p è la valutazione p-adica normalizzata.

Ritornando al gruppo dei caratteri $X^{(n)}$ dell'n-esima estensione ciclotomica $\mathbb{Q}^{(n)}$, inserendo per ogni primo $p_i \mid n$ la decomposizione precedente di $X^{(p_i^{e_i})}$, otteniamo $X^{(n)} = \Omega^{(n)} \times \Psi^{(n)}$, dove $\Omega^{(n)} = \prod_{i=1}^r \langle \omega_{p_i} \rangle$ è detto gruppo dei caratteri di Dirichlet del primo tipo modulo n e $\Psi^{(n)} = \prod_{i=1}^r \langle \psi_{p_i^{e_i}} \rangle$ è detto gruppo dei caratteri di Dirichlet del secondo tipo modulo n.

Scegliamo ora X un gruppo di caratteri di Dirichlet e poniamo $n = \operatorname{lcm}\{f_\chi \mid \chi \in X\}$. X può essere visto come sottogruppo del gruppo $X^{(n)}$, e, detto K il campo associato a X, si ha che n è il conduttore del campo K.

Nel seguito denoteremo

$$\mathscr{D}(n) = \left\{ d \in \mathbb{N} \;\middle|\; \left(\prod_{p_i \neq 2} p_i \right) \;\middle|\; d,\ d \mid n,\ d \not\equiv 2 \pmod 4 \right\}$$

e

$$q(n) = \prod_{v_{p_i}(n) \geq 2} p_i^{v_{p_i}(n)},$$

la parte potente di n. Osserviamo che l'insieme $\mathscr{D}(n)$ è in corrispondenza biunivoca con tutte le possibili parti potenti dei conduttori f_χ per $\chi \in X^{(n)}$:

$$\begin{array}{ccc} \{q(f_\chi) \mid \chi \in X^{(n)}\} & \longleftrightarrow & \mathscr{D}(n) \\ \gamma & \longleftrightarrow & \prod_{p_i \neq 2} p_i \cdot \prod_{v_{p_i}(\gamma) \geq 2} p_i^{v_{p_i}(\gamma)-1} \end{array}$$

Definizione 4.1. Sia X un gruppo finito di caratteri di Dirichlet, $n = \operatorname{lcm}\{f_\chi \mid \chi \in X\}$ e $d \in \mathscr{D}(n)$. Allora

$$\Phi_d = \{\chi \in X \mid q(f_\chi) = q(d)\}$$

è chiamata classe di ramificazione di X relativa a d.

Vediamo che tali classi inducono una partizione di X:

$$X = \bigsqcup_{d \in \mathscr{D}(n)} \Phi_d,$$

dove il simbolo $\sqcup$ sta per l'unione disgiunta.

La prossima proposizione ci assicura che nella maggior parte dei casi lo studio delle classi di ramificazione semplifica lo studio del gruppo X.

Proposizione 4.1. *Sia X un gruppo finito di caratteri di Dirichlet, $n = \operatorname{lcm}\{f_\chi \mid \chi \in X\}$ e $d \in \mathscr{D}(n)$. Allora:*

1. *La proiezione $\pi : X \to \Psi^{(n)} \times Z$ è surgettiva, dove $Z = \langle \omega_2 \rangle$ se $n \equiv 4 \pmod 8$, mentre $Z = \{1\}$ altrimenti.*
2. *$\Phi_n \neq \emptyset$ e $\langle \Phi_n \rangle = X$.*
3. *Se $d \not\equiv 4 \pmod 8$, $\Phi_d \neq \emptyset$; se $d \equiv 4 \pmod 8$, $\Phi_d \neq \emptyset$ se e solo se esiste $\chi_0 \in X$ tale che $q(f_{\chi_0}) = 4$.*
4. *Se $\Phi_d \neq \emptyset$, allora $\langle \Phi_d \rangle = X \cap X^{(d)}$ e la proiezione $\pi : \langle \Phi_d \rangle \to \Psi^{(d)} \times Z$ è surgettiva.*

Dimostrazione. Lo studio del conduttore di caratteri $\chi \in X$ ci assicura che la parte potente di f_χ dipende solo dai caratteri del secondo tipo se $f_\chi \not\equiv 4 \pmod 8$, mentre dipende anche dalla potenza di ω_2 altrimenti.

1. Data la coprimalità dei p_i, basta dimostrare che la proiezione $\pi : X \to \prod_{p_i} \langle \psi_{p_i^{e_i}} \rangle \times Z$ è surgettiva su ogni componente, cioè che le mappe $\pi_{p_i} : X \to \langle \psi_{p_i^{e_i}} \rangle$ se $p_i \neq 2$ e $\pi_2 : X \to \langle \psi_{2^e} \rangle \times \langle \omega_2 \rangle$ con $e = v_2(n)$ sono surgettive. Ma questo è evidente in quanto, per ogni p_i, $v_{p_i}(n) = \max\{v_{p_i}(f_\chi) \mid \chi \in X\}$.

2. Per il punto 1), esiste $\chi \in X$ tale che $\pi(\chi) = \prod_{p_i} \psi_{p_i^{e_i}} \cdot \omega$. Allora evidentemente $\chi \in \Phi_n$ e $\pi(\langle \Phi_n \rangle) = \Psi^{(n)} \times Z$. Sia invece $\psi \in X$; se $\psi' \in \langle \Phi_n \rangle$ è tale che $\pi(\psi)\pi(\psi') = \pi(\chi)$, allora $\pi(\psi\psi')$ genera $\Psi^{(n)} \times Z$ e dunque $\psi\psi' \in \Phi_n$, da cui $\psi \in \langle \Phi_n \rangle$.

3. Se $d \not\equiv 4 \pmod 8$, la tesi segue immediatamente dal punto 1). Se invece $d \equiv 4 \pmod 8$, vediamo le due implicazioni. Se χ sta in Φ_d, semplicemente $\chi_0 = \chi_2$ funziona. Viceversa, se χ_0 è tale che $q(f_{\chi_0}) = 4$, presa la 2-componente χ' di χ_0 e preso un χ'' tale che $q(f_{\chi''}) = q\left(\frac{d}{4}\right)$ (che esiste in quanto $\frac{d}{4} \not\equiv 4 \pmod 8$), abbiamo che $\chi'\chi'' \in \Phi_d$.

4. Basta applicare i punti 1) e 2) sostituendo $d' = \mathrm{lcm}\{f_\chi \mid \chi \in X \cap X^{(d)}\}$ a n e $X \cap X^{(d')}$ a X.

□

Grazie a questi risultati introduttivi, siamo ora in grado di addentrarci nella parte interessante della teoria. Come prima cosa, fissiamo K un campo di numeri con gruppo di Galois G su $\mathbb{Q}$ abeliano e sia X il corrispondente gruppo dei caratteri. Per $\chi \in X$ definiamo

$$\varepsilon_\chi = \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma \in G} \overline{\chi(\sigma)}\sigma \in \mathbb{C}[G]$$

gli idempotenti ortogonali dell'anello di gruppo $\mathbb{C}[G]$.

Proposizione 4.2. *Si hanno le relazioni:*

$$\sum_{\chi \in X} \varepsilon_\chi = 1, \qquad \varepsilon_\chi \varepsilon_\psi = \begin{cases} 0 & \text{se } \chi \neq \psi \\ \varepsilon_\chi & \text{se } \chi = \psi \end{cases}$$

In particolare gli ε_χ sono linearmente indipendenti su $\mathbb{C}$.

Dimostrazione. Per la prima relazione abbiamo le uguaglianze:

$$\sum_{\chi \in X} \varepsilon_\chi = \frac{1}{[K:\mathbb{Q}]} \sum_{\chi \in X} \sum_{\sigma \in G} \overline{\chi(\sigma)}\sigma = \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma \in G} \overline{\sum_{\chi \in X} \chi(\sigma)}\sigma = \frac{|X|}{[K:\mathbb{Q}]} = 1,$$

in quanto $\sum_{\chi \in X} \chi(\sigma)$ vale 0 se $\sigma \neq 1$ e $|X| = [K:\mathbb{Q}]$ se $\sigma = 1$. Per l'altra, abbiamo invece:

$$\varepsilon_\chi \varepsilon_\psi = \frac{1}{[K:\mathbb{Q}]^2} \sum_{\sigma,\tau \in G} \overline{\chi(\sigma)\psi(\tau)}\sigma\tau = \frac{1}{[K:\mathbb{Q}]^2} \sum_{\sigma,s \in G} \overline{\chi(\sigma)\psi(\sigma^{-1}s)}s =$$

$$= \frac{1}{[K:\mathbb{Q}]^2} \sum_{\sigma,s \in G} \overline{\chi(\sigma)\psi(\sigma^{-1})\psi(s)}s = \frac{1}{[K:\mathbb{Q}]^2} \sum_{s \in G} \left(\sum_{\sigma \in G} \chi^{-1}\psi(\sigma) \right) \overline{\psi(s)}s$$

e visto che $\sum_{\sigma \in G} \chi(\sigma)$ vale 0 se $\chi \neq 1$ e $|G| = [K:\mathbb{Q}]$ se $\chi = 1$, segue facilmente la relazione voluta. □

Come conseguenza abbiamo che l'anello di gruppo $\mathbb{C}[\varepsilon_\chi \mid \chi \in X]$ ha rango $|X| = |G|$ su $\mathbb{C}$, dunque $\mathbb{C}[\varepsilon_\chi \mid \chi \in X]$ coincide con $\mathbb{C}[G]$ grazie a un'ovvia inclusione.

Se $\chi \in X$, denoteremo $\mathbb{Q}(\chi) = \mathbb{Q}(\{\chi(\sigma) \mid \sigma \in G\}) = \mathbb{Q}^{(\mathrm{ord}(\chi))}$ e K_χ il sottocampo di K associato al sottogruppo $\langle\chi\rangle$ del gruppo dei caratteri X. Preso un qualunque $a \in K$, definiamo

$$y_K(\chi|a) = \frac{1}{\overline{\tau(\chi)}} \sum_{\sigma\in G} \overline{\chi(\sigma)}\sigma(a) \in \mathbb{C}$$

la coordinata di carattere di a rispetto a χ, dove $\tau(\chi) = \sum_{j=1}^{f_\chi} \chi(j)\zeta_{f_\chi}^j$ è la somma di Gauss relativa a χ.
Considerando l'azione di $\mathbb{Q}[G]$ su K, abbiamo l'ovvia uguaglianza:

$$\varepsilon_\chi a = \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma\in G} \overline{\chi(\sigma)}\sigma(a) = \frac{1}{[K:\mathbb{Q}]} y_K(\chi|a)\overline{\tau(\chi)}.$$

Andiamo ora a studiare le proprietà di base delle coordinate di carattere.

Proposizione 4.3. *1. Per ogni $a \in K$ vale l'uguaglianza:*

$$a = \frac{1}{[K:\mathbb{Q}]} \sum_{\chi\in X} y_K(\chi|a)\overline{\tau(\chi)}.$$

2. $y_K(\chi|a) \in \mathbb{Q}(\chi)$. Inoltre $y_K(\chi|a+b) = y_K(\chi|a) + y_K(\chi|b)$.

3. Se $\rho \in G$, $y_K(\chi|\rho(a)) = \chi(\rho)y_K(\chi|a)$.

4. Se χ appartiene a un sottocampo $F \subseteq K$, cioè χ è banale su $\mathrm{Gal}(K/F)$, allora $y_K(\chi|a) = y_F(\chi|\,\mathrm{Tr}_{K/F}(a))$.

5. Se $(r, \mathrm{ord}(\chi)) = (r, f_\chi) = 1$ e σ_r è l'automorfismo di $\mathbb{Q}(\chi)$ su $\mathbb{Q}$ tale che $\sigma_r(\chi(\sigma)) = \chi^r(\sigma)$ per ogni $\sigma \in G$, allora $\sigma_r(y_K(\chi|a)) = y_K(\chi^r|a)$.

6. Se $a = \frac{1}{[K:\mathbb{Q}]} \sum_{\chi\in X} y(\chi)\overline{\tau(\chi)}$ per certi $y(\chi)$ tali che $\sigma_r(y(\chi)) = y(\chi^r)$, con $r \in (\mathbb{Z}/\,\mathrm{ord}(\chi)\mathbb{Z})^*$, allora $y(\chi) = y_K(\chi|a)$.

Dimostrazione. 1. Segue dall'uguaglianza precedente e dalla relazione $\sum_{\chi\in X} \varepsilon_\chi = 1$.

2. Sicuramente $y_K(\chi|a) \in L = K\mathbb{Q}(\chi)\mathbb{Q}^{(f)}$, dove $f = f_\chi$. Scelto m in modo che $L \subseteq \mathbb{Q}^{(m)}$, possiamo vedere gli elementi del gruppo di Galois

$\mathrm{Gal}(L/\mathbb{Q}(\chi))$ come $\sigma_r \in \mathbb{Q}^{(m)}$, dove $r \in (\mathbb{Z}/m\mathbb{Z})^*$ e $\sigma_r(\zeta_m) = \zeta_m^r$. Ma allora, per ogni r coprimo con m:

$$\begin{aligned}\sigma_r(y_K(\chi|a)) &= \frac{1}{\sigma_r(\overline{\tau(\chi)})}\sum_{\sigma\in G}\overline{\chi(\sigma)}\sigma_r\sigma(a) = \\ &= \frac{1}{\chi(r)\overline{\tau(\chi)}}\chi(\sigma_r)\sum_{\sigma\in G}\overline{\chi(\sigma)}\sigma(a) = y_K(\chi|a),\end{aligned}$$

cioè $y_K(\chi|a) \in \mathbb{Q}^{(\chi)}$.

3. Banalmente $y_K(\chi|\rho(a)) = \chi(\rho)\overline{\chi(\rho)}y_K(\chi|\rho(a)) = \chi(\rho)y_K(\chi|a)$.

4. Decomponendo ogni $\sigma \in G$ come $\sigma = gh$, dove $g \in \mathrm{Gal}(F/\mathbb{Q})$ e $h \in \mathrm{Gal}(K/F)$, abbiamo:

$$\begin{aligned}y_K(\chi|a) &= \frac{1}{\overline{\tau(\chi)}}\sum_{g,h}\overline{\chi(gh)}(gh)(a) = \\ &= \frac{1}{\overline{\tau(\chi)}}\sum_{g}\overline{\chi(g)}g\left(\sum_h h(a)\right) = y_F(\chi|\,\mathrm{Tr}_{K/F}(a)),\end{aligned}$$

in quanto χ è banale su $\mathrm{Gal}(K/F)$.

5. Direttamente abbiamo:

$$\begin{aligned}\sigma_r(y_K(\chi|a)) &= \frac{1}{\overline{\sum_{j=1}^{f_\chi}\chi^r(j)\zeta_{f_\chi}^{rj}}}\sum_{\sigma\in G}\overline{\chi^r(\sigma)}\sigma_r\sigma(a) = \\ &= \frac{1}{\chi^r(r)\overline{\tau(\chi^r)}}\chi^r(\sigma_r)\sum_{\sigma\in G}\overline{\chi^r(\sigma)}\sigma(a) = y_K(\chi^r|a).\end{aligned}$$

6. Sia $m = \mathrm{lcm}\{\mathrm{ord}(\chi), f_\chi \mid \chi \in X\}$. Per avere la tesi basta vedere solo il caso $a = 0$; infatti, se $a = \frac{1}{[K:\mathbb{Q}]}\sum_{\chi\in X} y(\chi)\overline{\tau(\chi)} = \frac{1}{[K:\mathbb{Q}]}\sum_{\chi\in X} y_K(\chi|a)\overline{\tau(\chi)}$, allora
$$0 = \frac{1}{[K:\mathbb{Q}]}\sum_{\chi\in X}(y_K(\chi|a) - y(\chi))\overline{\tau(\chi)}$$
e per il punto precedente e per il caso $a = 0$ abbiamo $y(\chi) = y_K(\chi|a)$. Adesso, se abbiamo $0 = \frac{1}{[K:\mathbb{Q}]}\sum_{\chi\in X} y(\chi)\overline{\tau(\chi)}$, vediamo gli elementi del

gruppo G come elementi $\sigma_r \in G^{(m)}$, con $(r, m) = 1$. In questo modo:

$$\begin{aligned} 0 = \varepsilon_\psi(0) &= \frac{1}{[K:\mathbb{Q}]^2} \sum_{\sigma_r \in G} \overline{\psi(\sigma_r)} \sigma_r \left(\sum_{\chi \in X} y(\chi) \overline{\tau(\chi)} \right) = \\ &= \frac{1}{[K:\mathbb{Q}]^2} \sum_{\sigma_r \in G} \overline{\psi(\sigma_r)} \sum_{\chi \in X} y(\chi^r) \chi^r(r) \overline{\tau(\chi^r)} = \\ &= \frac{1}{[K:\mathbb{Q}]^2} \sum_{\sigma_r \in G} \overline{\psi(\sigma_r)} \sum_{\chi \in X} y(\chi) \chi(r) \overline{\tau(\chi)} = \\ &= \frac{1}{[K:\mathbb{Q}]^2} \sum_{\chi \in X} y(\chi) \overline{\tau(\chi)} \sum_{\sigma_r \in G} (\psi^{-1}\chi)(\sigma_r) = \\ &= \frac{1}{[K:\mathbb{Q}]} y(\psi) \overline{\tau(\psi)}, \end{aligned}$$

da cui $y(\psi) = 0$.

□

Come abbiamo già annunciato, le coordinate di carattere sono utilissime per lo studio dell'anello degli interi di K e dei suoi sottoanelli; il risultato più affascinante che coinvolge queste coordinate è senza dubbio il seguente:

Teorema 4.4. *Sia $a \in K$. Lo $\mathbb{Z}$-modulo $\mathbb{Z}[G]a$ ha rango massimo (cioè $[K:\mathbb{Q}]$) se e solo se $y_K(\chi|a) \neq 0$ per ogni $\chi \in X$. In tale caso, se $a \in \mathscr{O}_K$:*

$$[\mathscr{O}_K : \mathbb{Z}[G]a] = \left| \prod_{\chi \in X} y_K(\chi|a) \right|.$$

La dimostrazione di questo teorema sfrutta due importantissimi risultati: uno è la formula conduttore-discriminante, che abbiamo visto nel capitolo precedente, mentre l'altro è la formula del discriminante di un gruppo abeliano, che andiamo subito a enunciare e dimostrare.

Lemma 4.5 (Discriminante di un gruppo abeliano)**.** *Sia G un gruppo abeliano finito e sia f una funzione da G a un certo campo di caratteristica* 0*. Allora:*

$$\det\left(f(\sigma\rho^{-1})\right)_{\sigma,\rho \in G} = \prod_{\chi \in \hat{G}} \sum_{\sigma \in G} \chi(\sigma) f(\sigma).$$

Dimostrazione. Supponiamo che f abbia valori in un campo F algebricamente chiuso. Sia V lo spazio vettoriale di tutte le funzioni $h(x)$ da G a F; V ha dimensione finita e G agisce su V per traslazione, cioè $\sigma h(x) = h(\sigma x)$.

Definiamo la trasformazione lineare $t = \sum_{\sigma\in G} f(\sigma)\sigma$ e sia $\phi_\rho(x)$ la funzione indicatrice di $\{\rho\} \subseteq G$, cioè tale che $\phi_\rho(\sigma) = \delta_{\sigma\rho}$. Allora $\{\phi_\rho \mid \rho \in G\}$ è una base di V. Visto che si ha:

$$t\phi_\rho(x) = \sum_{\sigma\in G} f(\sigma)\phi_\rho(\sigma x) = \sum_{\sigma\in G} f(\sigma)\phi_{\sigma^{-1}\rho}(x) = \sum_{\alpha\in G} f(\rho\alpha^{-1})\phi_\alpha(x),$$

la matrice $(f(\sigma\rho^{-1}))_{\sigma,\rho\in G}$ è la matrice che rappresenta t rispetto a questa base. Visto che i caratteri $\chi \in \hat{G}$ sono linearmente indipendenti, formano un'altra base di V. Ma $t\chi(x) = \sum_{\sigma\in G} f(\sigma)\chi(\sigma)\chi(x)$, dunque il carattere χ è un autovettore di t rispetto all'autovalore $\sum_{\sigma\in G}\chi(\sigma)f(\sigma)$. Di conseguenza, t scritta tramite questa base è diagonale, quindi il suo determinante è il prodotto degli autovalori. □

Teorema 4.6. *Sia* $\mathrm{disc}(a) = \det(\sigma\rho(a))^2_{\sigma,\rho\in G}$ *il discriminante dei coniugati di* $a \in K$*. Se* $\mathrm{disc}(K)$ *è il discriminante di* K*, allora:*

$$\mathrm{disc}(a) = \prod_{\chi\in X} y_K(\chi|a)^2 \cdot \mathrm{disc}(K).$$

Dimostrazione. Visto che $\mathrm{disc}(a) = \det(\sigma\rho(a))^2_{\sigma,\rho\in G} = \det(\sigma\rho^{-1}(a))^2_{\sigma,\rho\in G}$, dalla formula del discriminante di un gruppo abeliano e dalla definizione di $y_K(\chi|a)$ abbiamo, ponendo $f(\sigma) = \sigma(a)$:

$$\begin{aligned}\mathrm{disc}(a) &= \prod_{\chi\in X}\left(\sum_{\sigma\in G}\chi(\sigma)\sigma(a)\right)^2 = \prod_{\chi\in X}\left(y_K(\chi|a)\tau(\overline{\chi})\right)^2 = \\ &= \prod_{\chi\in X} y_K(\chi|a)^2 \cdot \prod_{\chi\in X}\tau(\chi)\tau(\overline{\chi}),\end{aligned}$$

dunque la tesi segue dalla formula conduttore-discriminante, dato che $\prod_{\chi\in X}\tau(\chi)\tau(\overline{\chi}) = f_\chi$. □

Siamo adesso pronti per dimostrare il teorema 4.4.

Dimostrazione del teorema 4.4. Il teorema precedente assicura che lo $\mathbb{Z}$-modulo $\mathbb{Z}[G]a = \sum_{\sigma\in G}\sigma(a)\mathbb{Z}$ ha rango massimo se e solo se $y_K(\chi|a) \neq 0$ per ogni $\chi \in X$. Inoltre, se $a \in \mathscr{O}_K$, lo stesso risultato implica l'uguaglianza:

$$[\mathscr{O}_K : \mathbb{Z}[G]a] = \pm\prod_{\chi\in X} y_K(\chi|a),$$

in quanto $[\mathscr{O}_K : \mathbb{Z}[G]a]^2$ coincide con il rapporto $\frac{\mathrm{disc}(a)}{\mathrm{disc}(K)}$. □

Dopo questi risultati teorici, cominciamo a calcolare esplicitamente alcune coordinate di carattere che ci serviranno in seguito. In particolare, con la proposizione seguente siamo in grado di dire quando le coordinate di carattere delle radici dell'unità sono diverse da 0:

Proposizione 4.7. *Siano $k, n \in \mathbb{N}$ e $\zeta_n^k = \zeta_{n_0}^{k_0}$, con $(k_0, n_0) = 1$. Allora per ogni $\chi \in X^{(n)}$ vale l'uguaglianza:*

$$y_{\mathbb{Q}^{(n)}}(\chi|\zeta_n^k) = \begin{cases} 0 & \text{se } f \nmid n_0 \ \vee \ q(f) \neq q(n_0) \\ \frac{\varphi(n)}{\varphi(n_0)} \mu\left(\frac{n_0}{f}\right) \overline{\chi}\left(-\frac{n_0}{f}\right) \chi(k_0) \neq 0 & \text{se } f \mid n_0 \ \wedge \ q(f) = q(n_0) \end{cases}$$

dove μ denota la funzione di Möbius e $f = f_\chi$.

Dimostrazione. Osserviamo subito che $\overline{\tau(\chi)} y_{\mathbb{Q}^{(n)}}(\chi|\zeta_n^k) = \sum_{j=1}^n \overline{\chi}(j)\zeta_n^{kj}$; concentriamoci dunque sull'ultima somma di Gauss.
Denotiamo $\tau(\overline{\chi}_{n_0}|\zeta_{n_0}^{k_0}) = \sum_{j=1}^{n_0} \overline{\chi}(j)\zeta_{n_0}^{k_0 j}$; abbiamo l'uguaglianza:

$$\tau(\overline{\chi}_n|\zeta_n^k) = \sum_{j=1}^{n} \overline{\chi}(j)\zeta_n^{kj} = \frac{\varphi(n)}{\varphi(n_0)} \tau(\overline{\chi}_{n_0}|\zeta_{n_0}^{k_0}).$$

A questo punto supponiamo $f \nmid n_0$. Se per assurdo $\tau(\chi_{n_0}|\zeta_{n_0}^{k_0}) \neq 0$, per l'identità $\tau(\chi_{n_0}|\zeta_{n_0}^{k_0 c}) = \overline{\chi}(c)\tau(\chi_{n_0}|\zeta_{n_0}^{k_0})$ si ha che $\chi(c) = 1$ per ogni c tale che $k_0 c \equiv k_0 \pmod{n_0}$, cioè $c \equiv 1 \pmod{n_0}$. Ma questo significa che n_0 è un multiplo del conduttore di χ, cioè $f \mid n_0$.

Supponiamo invece che $f \mid n_0$ e sia p primo tale che $n_0 = p n_0'$ e $f \mid n_0'$. Spezzando la somma, si ha facilmente:

$$\tau(\chi_{n_0}|\zeta_{n_0}^{k_0}) = \sum_{x' \in (\mathbb{Z}/n_0'\mathbb{Z})^*} \chi(x')\zeta_{n_0}^{k_0 x'} \sum_{y n_0' \not\equiv -x' \pmod{p}} \zeta_p^{k_0 y}.$$

Ora, se $p \mid n_0'$, la seconda somma fa 0, in quanto $(k_0, n_0) = 1$ implica $(k_0, p) = 1$ e cioè k_0 è invertibile modulo p.
Se invece $p \nmid n_0'$, sia y_0 l'unico y tale che $y n_0' \equiv -x' \pmod{p}$. Allora la seconda somma vale $-\zeta_p^{k_0 y_0} = -\zeta_{n_0}^{k_0 y_0 n_0'}$. Si può quindi riscrivere la somma precedente come:

$$\tau(\chi_{n_0}|\zeta_{n_0}^{k_0}) = -\sum_{x' \in (\mathbb{Z}/n_0'\mathbb{Z})^*} \chi(x')\zeta_{n_0}^{k_0(x' + y_0 n_0')}.$$

Ma se scegliamo x'' in modo che $x' + y_0 n_0' \equiv x'' p \pmod{n_0}$, abbiamo:

$$\tau(\chi_{n_0}|\zeta_{n_0}^{k_0}) = -\sum_{x'' \in (\mathbb{Z}/n_0'\mathbb{Z})^*} \chi(x'' p)\zeta_{n_0'}^{k_0 x''} = -\chi(p)\tau(\chi_{n_0'}|\zeta_{n_0'}^{k_0}).$$

Ripetendo questo ragionamento per tutti i primi che dividono $\frac{n_0}{f}$, osserviamo che $\tau(\chi_{n_0}|\zeta_{n_0}^{k_0})$ fa 0 se $\frac{n_0}{f}$ non è libero da quadrati, mentre è uguale a quanto appena visto altrimenti. Tutto questo si può riassumere usando la funzione di Möbius:

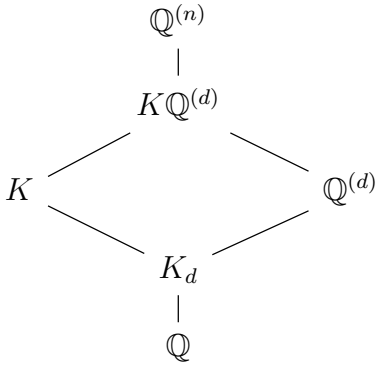
$$\tau(\chi_{n_0}|\zeta_{n_0}^{k_0}) = \mu\left(\frac{n_0}{f}\right)\chi\left(\frac{n_0}{f}\right)\tau(\chi|\zeta_f^{k_0}).$$

Infine, usando l'identità $\tau(\chi|\zeta_f^{k_0}) = \overline{\chi}(k_0)\tau(\chi)$, abbiamo:

$$\tau(\overline{\chi}_{n_0}|\zeta_{n_0}^{k_0}) = \mu\left(\frac{n_0}{f}\right)\overline{\chi}\left(\frac{n_0}{f}\right)\chi(k_0)\tau(\overline{\chi}),$$

da cui la tesi in quanto $\tau(\overline{\chi}) = \overline{\chi}(-1)\overline{\tau(\chi)}$. □

Fissiamo ora $d \in \mathscr{D}(n)$, dove n è il conduttore del campo di numeri abeliano K, e poniamo $K_d = K \cap \mathbb{Q}^{(d)}$ e $\eta_d = \mathrm{Tr}_{\mathbb{Q}^{(d)}/K_d}(\zeta_d)$. Abbiamo quindi un diagramma:



Usando l'ovvia uguaglianza $\mathrm{Tr}_{\mathbb{Q}^{(n)}/\mathbb{Q}^{(d)}}(\zeta_d) = [\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}]\zeta_d$ otteniamo l'altra uguaglianza:

$$y_K(\chi|\eta_d) = \frac{[K : K_d]}{[\mathbb{Q}^{(n)} : \mathbb{Q}^{(d)}]} y_{\mathbb{Q}^{(n)}}(\chi|\zeta_d).$$

Per la proposizione precedente $y_K(\chi|\eta_d) \neq 0$ se e solo se $q(d) \mid f_\chi \mid d$, cioè se e solo se χ appartiene alla classe di ramificazione Φ_d di X rispetto a d. Dunque η_d ammette una rappresentazione in coordinate di carattere:

$$\eta_d = \frac{1}{[K : \mathbb{Q}]} \sum_{\chi \in \Phi_d} [K : K_d]\mu\left(\frac{d}{f_\chi}\right)\overline{\chi}\left(-\frac{d}{f_\chi}\right)\overline{\tau(\chi)}.$$

Osserviamo che, per l'ultimo punto della proposizione 4.3, η_d vale 0 solo nel caso in cui la classe di ramificazione Φ_d è vuota, che per la proposizione 4.1 può accadere solo se $d \equiv 4 \pmod 8$. Siamo dunque pronti per definire:

$$T = \sum_{d \in \mathscr{D}(n)} \eta_d = \sum_{d \in \mathscr{D}(n)} \mathrm{Tr}_{\mathbb{Q}^{(d)}/K_d}(\zeta_d).$$

Visto che $y_K(\chi|T) \neq 0$ per ogni $\chi \in X = \bigsqcup_{d\in\mathscr{D}(n)} \Phi_d$, abbiamo che l'indice $[\mathscr{O}_K : \mathbb{Z}[G]T]$ è finito, da cui $\mathbb{Q}[G]T = K$; T è dunque il generatore di una base normale per l'estensione $K/\mathbb{Q}$.

Ora, posto $l = \operatorname{lcm}\{\operatorname{ord}(\chi) \mid \chi \in \Phi_d\}$, essendo la classe di ramificazione Φ_d chiusa sotto l'azione degli automorfismi $\sigma_r \in G^{(l)}$, abbiamo che l'elemento

$$\varepsilon_d = \sum_{\chi\in\Phi_d} \varepsilon_\chi = \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma\in G} \overline{\left(\sum_{\chi\in\Phi_d} \chi(\sigma)\right)} \sigma$$

appartiene all'anello di gruppo $\mathbb{Q}[G]$ e quindi

$$\mathcal{A}_K = \mathbb{Z}[G][\{\varepsilon_d \mid d \in \mathscr{D}(n)\}]$$

è un sottoanello di $\mathbb{Q}[G]$ con lo stesso elemento 1. Inoltre $\mathcal{A}_K$ è un ordine di $\mathbb{Q}[G]$, cioè un sottoanello e $\mathbb{Z}$-reticolo massimale di $\mathbb{Q}[G]$ con lo stesso elemento 1 che genera $\mathbb{Q}[G]$ su $\mathbb{Q}$. Infatti ogni elemento ε_d sta in $\frac{1}{s_d}\mathbb{Z}[G]$ per un certo s_d numero naturale, quindi, se $s = \prod s_d$, $\mathcal{A}_K$ è contenuto in $\frac{1}{s}\mathbb{Z}[G]$, che ha rango $[K : \mathbb{Q}]$ su $\mathbb{Z}$; viceversa, visto che la somma degli ε_d fa 1, si ha anche l'inclusione $\mathbb{Z}[G] \subseteq \mathcal{A}_K$, e perciò $\mathcal{A}_K$ ha rango $[K : \mathbb{Q}]$ su $\mathbb{Z}$.

Proposizione 4.8. *Vale la relazione* $\varepsilon_d T = \eta_d$. *Inoltre* $\operatorname{rk}_\mathbb{Z}(\mathbb{Z}[G]\eta_d) = \operatorname{rk}_\mathbb{Z}(\mathbb{Z}[G]\varepsilon_d) = |\Phi_d|$ *e:*

$$K = \mathbb{Q}[G]T = \bigoplus_{d\in\mathscr{D}(n)} \mathbb{Q}[G]\eta_d.$$

Dimostrazione. Direttamente abbiamo:

$$\begin{aligned}\varepsilon_d T = \sum_{\chi\in\Phi_d} \varepsilon_\chi T = \frac{1}{[K:\mathbb{Q}]} \sum_{\chi\in\Phi_d} y_K(\chi|T)\overline{\tau(\chi)} = \frac{1}{[K:\mathbb{Q}]} \sum_{\chi\in\Phi_d} y_K(\chi|\eta_d)\overline{\tau(\chi)} = \\ = \frac{1}{[K:\mathbb{Q}]} \sum_{\chi\in X} y_K(\chi|\eta_d)\overline{\tau(\chi)} = \eta_d,\end{aligned}$$

in quanto $y_K(\chi|\eta_d) \neq 0$ solamente se $\chi \in \Phi_d$. Da questo si ricava che $\operatorname{rk}_\mathbb{Z}(\mathbb{Z}[G]\eta_d) = \operatorname{rk}_\mathbb{Z}(\mathbb{Z}[G]\varepsilon_d)$. Infatti, se $\sum_d a_d\varepsilon_d = 0$, anche $\sum_d a_d\varepsilon_d T = \sum_d a_d\eta_d$ fa 0; viceversa, se $\sum_d a_d\eta_d = (\sum_d a_d\varepsilon_d)\, T = 0$, necessariamente $\sum_d a_d\varepsilon_d = 0$, in quanto $K = \mathbb{Q}[G]T$.
Per vedere che tale rango coincide con $|\Phi_d|$, osserviamo innanzitutto che, per l'indipendenza degli ε_d, $\sum_{d\in\mathscr{D}(n)} \operatorname{rk}_\mathbb{Z}(\mathbb{Z}[G]\varepsilon_d) = \operatorname{rk}_\mathbb{Z}(\mathcal{A}_K) = [K : \mathbb{Q}] = \sum_{d\in\mathscr{D}(n)} |\Phi_d|$; dunque ci basta mostrare la disuguaglianza $\operatorname{rk}_\mathbb{Z}(\mathbb{Z}[G]\varepsilon_d) \geq |\Phi_d|$

e avremmo l'uguaglianza voluta.
In modo del tutto analogo a prima, si ha che $\sum_{d\in\mathscr{D}(n)} \mathrm{rk}_{\mathbb{C}}(\mathbb{C}[G]\varepsilon_d) = \sum_{d\in\mathscr{D}(n)} |\Phi_d|$; in questo caso però vale l'inclusione $\mathbb{C}[G]\varepsilon_d \subseteq \mathbb{C}[\varepsilon_\chi \mid \chi \in \Phi_d]$ in quanto

$$\sigma \cdot \varepsilon_d = \sigma \cdot \sum_{\chi\in\Phi_d} \varepsilon_\chi = \sum_{\chi\in\Phi_d} \chi(\sigma)\varepsilon_\chi,$$

dunque $\mathrm{rk}_{\mathbb{C}}(\mathbb{C}[G]\varepsilon_d) = |\Phi_d|$. Adesso, se per assurdo $\mathbb{Z}[G]\varepsilon_d$ fosse generato su $\mathbb{Z}$ da meno di $m = |\Phi_d|$ elementi, potremmo trovare $m-1$ elementi $\alpha_1, \dots, \alpha_{m-1}$ di $\mathbb{Z}[G]\varepsilon_d$ e degli $a_i^{(\sigma)}$ tali che:

$$\sigma \cdot \varepsilon_d = \sum_{i=1}^{m-1} a_i^{(\sigma)} \alpha_i$$

per ogni $\sigma \in G$. Questo però è evidentemente un assurdo, in quanto si avrebbe che anche $\mathbb{C}[G]\varepsilon_d$ è generato su $\mathbb{C}$ da meno di $m = |\Phi_d|$ elementi.
Infine la decomposizione di K segue dal fatto che entrambi sono moduli liberi di rango $[K : \mathbb{Q}]$ su $\mathbb{Q}$ e da un'ovvia inclusione. □

Finalmente siamo giunti alla dimostrazione del teorema di Leopoldt; abbiamo però prima bisogno di due lemmi.

Lemma 4.9. *Sia p un primo, $n \in \mathbb{N}$ e $\zeta \in \langle\zeta_{np}\rangle \backslash \langle\zeta_n\rangle$; sia inoltre $\sigma \in G^{(n)}$ e $M = \{\rho \in G^{(np)} \mid \rho_{|\mathbb{Q}^{(n)}} = \sigma\}$. Allora:*

$$\sum_{\rho\in M} \rho(\zeta) = \begin{cases} 0 & \text{se } p \mid n \\ -\varphi(p)^{-1}\sigma(\zeta^p) & \text{se } p \nmid n \end{cases}$$

dove $\varphi(p) \in G^{(np)}$ è il Frobenius scelto in modo che $\varphi_{|\mathbb{Q}^{(n)}} = \sigma_p \in G^{(n)}$.

Dimostrazione. Diciamo $\sigma = \sigma_k$, con $k \in (\mathbb{Z}/n\mathbb{Z})^*$. Se $p \mid n$ abbiamo subito:

$$\sum_{\rho\in M} \rho(\zeta) = \sum_{j=0}^{p-1} \zeta^{k+jn} = \zeta^k \sum_{j=0}^{p-1} (\zeta^n)^j = 0,$$

in quanto ζ^n è una radice p-esima di 1. Se invece $p \nmid n$, con un conto analogo abbiamo:

$$\sum_{\rho\in M} \rho(\zeta) = \sum_{\substack{0\le j<p-1 \\ k+jn\not\equiv 0 \pmod p}} \zeta^{k+jn} = -\zeta^{k+j_0 n},$$

dove $j_0 \in \{0, \dots, p-1\}$ è l'unico $j \in \{0, \dots, p-1\}$ tale che $k + jn \equiv 0 \pmod p$. Visto che $\frac{k+j_0 n}{p} \equiv kp^{-1} \pmod n$, si ottiene facilmente $-\zeta^{k+j_0 n} = -(\zeta^p)^{kp^{-1}} = -\varphi(p)^{-1}\sigma_k(\zeta^p)$. □

Lemma 4.10. *Sia $d \in \mathscr{D}(n)$ con $\Phi_d \neq \emptyset$ e $U = \mathrm{Gal}(\mathbb{Q}^{(d)}/K_d)$. Allora esiste un sottoinsieme $B \subseteq G^{(d)}$ tale che $BU = B$ e $\mathbb{Z}[G^{(d)}]\zeta_d = \bigoplus_{\beta \in B} \beta(\zeta_d)\mathbb{Z}$.*

Dimostrazione. Per una proposizione vista in precedenza abbiamo che $\langle \Phi_d \rangle = X \cap X^{(d)}$ è il gruppo dei caratteri di K_d. Poniamo $d_0 = z \cdot \prod_{p \neq 2,\ p|n} p$, dove $z = 1$ se $v_2(d) \leq 2$, mentre $z = 4$ altrimenti. Allora $\mathbb{Q}^{(d_0)}$ corrisponde a $\Omega^{(d)}$ se $d \not\equiv 4 \pmod 8$, mentre corrisponde a $\prod_{p \neq 2,\ p|n} \langle \omega_p \rangle$ se $d \equiv 4 \pmod 8$, dove $\Omega^{(d)}$ è il gruppo dei caratteri modulo d del primo tipo. Posto $G' = \mathrm{Gal}(\mathbb{Q}^{(d)}/\mathbb{Q}^{(d_0)}) = \{\sigma_l \mid l \in (\mathbb{Z}/d\mathbb{Z})^*,\ l \equiv 1 \pmod{d_0}\}$, vogliamo vedere che $U \cap G' = \{1\}$.
Sia dunque $\sigma \in U \cap G'$; se $\pi : X^{(d)} \to \Psi^{(d)} \times Z$ denota l'usuale proiezione, dove $Z = \langle \omega_2 \rangle$ se $d \equiv 4 \pmod 8$ ed è banale altrimenti, dalla definizione di G' è evidente che $\chi(\sigma) = (\pi(\chi))(\sigma)$ per ogni $\sigma \in G'$ e per ogni $\chi \in X^{(d)}$. Dato un qualunque $\chi \in X^{(d)}$, per surgettività di $\pi_{|X \cap X^{(d)}}$ si ha che $\pi(\chi) = \pi(\chi_0)$ per un certo $\chi_0 \in X \cap X^{(d)}$. Ma allora $\chi(\sigma) = \chi_0(\sigma) = 1$, in quanto $\sigma \in U$ e $X \cap X^{(d)}$ è banale su U, da cui $\sigma \in \bigcap_{\chi \in X^{(d)}} \mathrm{Ker}(\chi) = \{1\}$.
Essendo G' il nucleo della restrizione $G^{(d)} \to G^{(d_0)}$, abbiamo che $\gamma : U \to G^{(d_0)}$ è iniettiva, quindi si possono scegliere dei rappresentanti $y_1, \ldots, y_l$ tali che le classi laterali $y_i U$ siano a due a due disgiunte e $\gamma : U' \to G^{(d_0)}$ sia bigettiva, dove $U' = \bigsqcup_{i=1}^{l} y_i U$. È immediato osservare che $G^{(d)} = U'G'$, quindi ogni $\sigma \in G^{(d)}$ si scrive come $\sigma = \nu\rho$, dove $\nu \in U'$ e $\rho \in G'$; tale fattorizzazione è però unica, poiché se $\nu\rho = \sigma = \nu'\rho'$, necessariamente $\rho\rho'^{-1} = \mathrm{id}$, in quanto altrimenti $\nu\nu'^{-1}\rho\rho'^{-1} = \mathrm{id}$ non sarebbe l'identità su $\mathbb{Q}^{(d_0)}$.
Siano $p_1, \ldots, p_r$ i primi distinti che dividono $\frac{d}{d_0}$ e poniamo $e_i = v_{p_i}(d)$, $c_i = v_{p_i}(d_0)$; inoltre, per ogni i, poniamo $H_i = \mathrm{Gal}(\mathbb{Q}^{(p_i^{e_i})}/\mathbb{Q}^{(p_i^{c_i})})$ e sia $H_i' \subseteq H_i$ un insieme di rappresentanti di $\mathrm{Gal}(\mathbb{Q}^{(p_i^{e_i-1})}/\mathbb{Q}^{(p_i^{c_i})})$ in H_i. Se λ è l'omomorfismo

$$\lambda : \prod_{i=1}^{r} G^{(p_i^{e_i})} \xrightarrow{i} \prod_{p|d} G^{(p^{v_p(d)})} \xrightarrow{\sim} G^{(d)},$$

abbiamo $G' = \lambda\left(\prod_{i=1}^{r} H_i\right)$. Ponendo $H = \lambda\left(\prod_{i=1}^{r} (H_i \backslash H_i')\right)$ e $B = U'H$, vogliamo verificare che B soddisfa le proprietà volute.
Innanzitutto è evidente che $BU = B$; inoltre $|U'| = |G^{(d_0)}| = \varphi(d_0)$ e $|H_i \backslash H_i'| = p_i^{e_i - c_i} - p_i^{e_i - c_i - 1} = \varphi(p_i^{e_i - c_i})$, quindi:

$$|B| = \begin{cases} \varphi(d_0) \prod_{i=1}^{r} \varphi(p_i^{e_i - c_i}) & \text{se } d \not\equiv 4 \pmod 8 \\ \varphi(d_0) \prod_{\substack{1 \leq i \leq r \\ p_i \neq 2}} \varphi(p_i^{e_i - c_i}) & \text{se } d \equiv 4 \pmod 8 \end{cases}$$

in quanto se $d \equiv 4 \pmod 8$, allora $|H_{(p=2)} \backslash H'_{(p=2)}| = 1$. Osserviamo però che il numero precedente coincide con $|\Phi^{(d)}|$, dove $\Phi^{(d)} = \{\chi \in X^{(d)} \mid q(f_\chi) =$

$q(d)\}$: infatti il carattere del primo tipo di $\chi = \chi_1\chi_2 \in \Phi^{(d)}$ può essere un qualunque $\chi_1 \in \Omega^{(d)}$, mentre fra i caratteri del secondo tipo χ_2 deve essere scelto fra quelli di conduttore esattamente d, che sono $\varphi\left(\frac{d}{d_0}\right)$ se $d \not\equiv 4 \pmod 8$ e $\frac{1}{2}\varphi\left(\frac{d}{d_0}\right)$ altrimenti. Visto che $|\Phi^{(d)}| = \mathrm{rk}_{\mathbb{Z}}(\mathbb{Z}[G^{(d)}]\zeta_d)$, deduciamo che gli $\mathbb{Z}$-moduli liberi di cui vogliamo dimostrare l'uguaglianza hanno lo stesso rango, perciò rimane solo da vedere che $\sigma(\zeta_d) \in \sum_{\beta\in B}\beta(\zeta_d)\mathbb{Z}$ per ogni $\sigma \in G^{(d)}$.
Sia $\sigma = \nu\lambda(\rho_1, \ldots, \rho_r)$, con $\nu \in U'$ e $\rho_i \in H_i$, e poniamo

$$M_i = \begin{cases} \{\tau \in H_i \mid \tau_{|\mathbb{Q}^{(p_i^{e_i-1})}} = \rho_{|\mathbb{Q}^{(p_i^{e_i-1})}}\}\backslash\{\rho_i\} & \text{se } \rho_i \in H_i' \\ \{\rho_i\} & \text{se } \rho_i \notin H_i' \end{cases}$$

È immediato osservare che in ogni caso $M_i \subseteq H_i\backslash H_i'$. Sia i tale che $\rho_i \in H_i'$. Allora, per il lemma precedente, abbiamo:

$$\sigma(\zeta_d) = -\sum_{\tau\in M_i} \nu\lambda(\rho_1, \ldots, \tau, \ldots, \rho_r)(\zeta_d),$$

dove τ sta nell'i-esima componente. Visto che l'identità precedente vale anche se $\rho_i \notin H_i'$ a meno di moltiplicare per -1, usandola ripetutamente otteniamo:

$$\sigma(\zeta_d) = (-1)^m \sum_{\tau_i\in M_i} \nu\lambda(\tau_1, \ldots, \tau_r)(\zeta_d) \in \sum_{\beta\in B}\beta(\zeta_d)\mathbb{Z},$$

dove $m = |\{i \in \{1, \ldots, r\} \mid \tau_i \in H_i'\}|$, cioè la tesi. □

Teorema 4.11 (Leopoldt)**.** *Sia K un campo di numeri abeliano. Allora $\mathscr{O}_K$ è uno $\mathcal{A}_K$-modulo libero di rango* 1*; in particolare:*

$$\mathscr{O}_K = \bigoplus_{d\in\mathscr{D}(n)} \mathbb{Z}[G]\eta_d = \mathcal{A}_K T.$$

Dimostrazione. Vista l'indipendenza degli ε_d per $d \in \mathscr{D}(n)$ e vista l'identità $\varepsilon_d T = \eta_d$, la seconda uguaglianza segue da una facile inclusione e dall'uguaglianza dei ranghi su $\mathbb{Z}$. Dato che $\eta_d \in \mathscr{O}_K$, dobbiamo mostrare solo l'inclusione $\mathscr{O}_K \subseteq \bigoplus_{d\in\mathscr{D}(n)} \mathbb{Z}[G]\eta_d$.
Vediamolo prima nel caso ciclotomico, $K = \mathbb{Q}^{(n)}$. Dalla teoria di base sappiamo che $\mathscr{O}_{\mathbb{Q}^{(n)}} = \mathbb{Z}[\zeta_n]$, quindi basta vedere che $\zeta_n^k \in \bigoplus_{d\in\mathscr{D}(n)} \mathbb{Z}[G]\zeta_d$ per ogni $k \in \mathbb{Z}/n\mathbb{Z}$. Supponiamo che $\zeta_n^k = \pm\zeta_{n_0}^{k_0}$, con $k_0, n_0 \in \mathbb{N}$, $(k_0, n_0) = (k_0, n) = 1$

e $n_0 \not\equiv 2 \pmod 4$ (infatti, se k_0 non fosse coprimo con n, basterebbe sostituire k_0 con $k_0 + jn_0$ per un opportuno $j \in \mathbb{N}$); se poniamo

$$d = n_0 \prod_{\substack{p \mid n \\ p \nmid 2n_0}} p \in \mathscr{D}(n),$$

abbiamo $n_0 \mid d$. Sia p un primo che divide $\frac{n_0}{d}$; applicando il lemma 4.9 con $\sigma = \mathrm{id}$, abbiamo:

$$\mathrm{Tr}_{\mathbb{Q}^{(d)}/\mathbb{Q}^{(\frac{d}{p})}}(\zeta_d) = -\varphi(p)^{-1}(\zeta_d^p) = -\varphi(p)^{-1}(\zeta_{\frac{d}{p}}).$$

Quindi, iterando questo ragionamento per tutti i primi p che dividono $\frac{d}{n_0}$ e scendendo lungo la torre di estensioni $\mathbb{Q}^{(d)} \supseteq \mathbb{Q}^{(\frac{d}{p})} \supseteq \ldots \supseteq \mathbb{Q}^{(n_0)}$, otteniamo l'uguaglianza:

$$\mathrm{Tr}_{\mathbb{Q}^{(d)}/\mathbb{Q}^{(n_0)}}(\zeta_d) = \prod_{p \mid \frac{d}{n_0}} (-\varphi(p)^{-1})\zeta_{n_0} = \mu\left(\frac{d}{n_0}\right)\sigma_l(\zeta_{n_0}),$$

per qualche $\sigma_l \in G^{(d)}$. Dunque $\zeta_n^k = \pm\sigma_{k_0}\sigma_l^{-1}\,\mathrm{Tr}_{\mathbb{Q}^{(d)}/\mathbb{Q}^{(n_0)}}(\zeta_d) \in \mathbb{Z}[G^{(d)}]\zeta_d = \mathbb{Z}[G^{(n)}]\zeta_d$.
Supponiamo invece K generico di conduttore n; sia $\alpha \in \mathscr{O}_K$. Visto che il teorema vale per le estensione ciclotomiche, allora $\alpha = \sum_{d \in \mathscr{D}(n)} \alpha_d$ per certi $\alpha_d \in \mathbb{Z}[G^{(d)}]\zeta_d$. Inoltre la decomposizione $\mathbb{Q}^{(n)} = \bigoplus_{d \in \mathscr{D}(n)} \mathbb{Q}[G^{(d)}]\zeta_d$ mostra l'unicità degli α_d, dunque, visto che $\alpha = \sum_{d \in \mathscr{D}(n)} \varepsilon_d \alpha$, abbiamo che $\alpha_d = \varepsilon_d \alpha$ se $\Phi_d \neq \emptyset$ e $\alpha_d = 0$ altrimenti. Per di più α_d è fissato da $\mathrm{Gal}(\mathbb{Q}^{(d)}/K_d)$, quindi ci basta dimostrare che, se $x \in \mathbb{Z}[G^{(d)}]\zeta_d$ è fissato da $U = \mathrm{Gal}(\mathbb{Q}^{(d)}/K_d)$, allora $x \in \mathbb{Z}[G]\eta_d$. Per il lemma precedente esiste $B \subseteq G^{(d)}$ tale che $BU = B$ e $x = \sum_{\beta \in B} x_\beta \beta(\zeta_d)$, con gli $x_\beta \in \mathbb{Z}$ unicamente determinati. Per ogni $\tau \in U$, $\tau^{-1}(x) = x$, quindi l'uguaglianza $BU = B$ implica la relazione $x_{\tau\beta} = x_\beta$. Ma allora, scegliendo un sottoinsieme $B' \subseteq B$ tale che $B = \bigsqcup_{\beta \in B'} \beta U$, otteniamo:

$$x = \sum_{\beta \in B'} x_\beta \left(\sum_{\tau \in U} \tau\beta(\zeta_d) \right) = \sum_{\beta \in B'} x_\beta \beta(\eta_d) \in \mathbb{Z}[G]\eta_d.$$

□

La versione del teorema di Leopoldt proposta in questa tesi è una fra le più esplicite e semplici da dimostrare, ma ha il "difetto" di introdurre l'ordine $\mathcal{A}_K$ in modo diverso dalla maggior parte della letteratura a riguardo. Infatti

usualmente, data un'estensione di campi di numeri L/K finita e di Galois, si definisce ordine associato a L/K

$$\mathcal{A}_{L/K} = \{\lambda \in K[G] \mid \lambda \mathscr{O}_L \subseteq \mathscr{O}_L\}.$$

Evidentemente questo è un ordine di $K[G]$, in quanto contiene l'anello di gruppo $\mathscr{O}_K[G]$. Per completare la nostra trattazione, vorremmo dimostrare che nel caso di un'estensione $K/\mathbb{Q}$ abeliana, il nostro $\mathcal{A}_K$ non è altro che l'ordine $\mathcal{A}_{K/\mathbb{Q}}$ associato all'estensione $K/\mathbb{Q}$.
Questo può essere fatto in modo piuttosto agevole usando il seguente peculiare risultato:

Proposizione 4.12. *Sia L/K un'estensione di campi di numeri finita e di Galois con gruppo di Galois G. Se $\mathscr{O}_L$ è libero su un ordine Γ di $K[G]$, allora $\Gamma = \mathcal{A}_{L/K}$.*

Dimostrazione. Se $\mathscr{O}_L = \Gamma\alpha$ è libero di rango 1 come Γ-modulo per un certo $\alpha \in \mathscr{O}_L$, allora vale l'uguaglianza $L = K[G]\alpha$. Sia $x \in \mathcal{A}_{L/K}$. Visto che $x\alpha$ sta in $\mathscr{O}_L$, allora esiste un $y \in \Gamma$ tale che $x\alpha = y\alpha$; ma L è libero come $K[G]$-modulo con base α, quindi necessariamente $x = y$. Da questo abbiamo l'inclusione $\mathcal{A}_{L/K} \subseteq \Gamma$. Sia ora per assurdo $x \in \Gamma \backslash \mathcal{A}_{L/K}$; per definizione di $\mathcal{A}_{L/K}$ esiste $\beta \in \mathscr{O}_L$ tale che $x\beta \notin \mathscr{O}_L$. D'altra parte, esiste $y \in \Gamma$ tale che $\beta = y\alpha$, dunque:

$$x\beta = x(y\alpha) = (xy)\alpha \in \Gamma\alpha = \mathscr{O}_L,$$

assurdo.

□

Grazie alla precedente proposizione siamo inoltre in grado di mostrare che l'ordine associato $\mathcal{A}_K$ coincide con l'anello di gruppo $\mathbb{Z}[G]$ nel caso in cui l'estensione $K/\mathbb{Q}$ sia tame; con questa osservazione risulta dunque evidente che il teorema di Leopoldt è una generalizzazione del teorema di Hilbert-Speiser.

L'importanza centrale che riveste il teorema di Leopoldt all'interno della teoria algebrica dei numeri non è data solamente dal fatto che dimostra l'esistenza di un anello $\mathcal{A}_K$ su cui l'anello degli interi $\mathscr{O}_K$ è sempre libero nel caso abeliano, ma anche perché esibisce esplicitamente un generatore T particolarmente semplice.
Alcuni studi di Bergè ([1]) successivi all'articolo di Leopoldt mostrano come l'ipotesi che il campo K sia abeliano su $\mathbb{Q}$ sia necessaria nell'enunciato del teorema di Leopoldt: lo stesso Bergè ha infatti dimostrato che le estensioni diedrali K di $\mathbb{Q}$ di ordine diverso da $2p$, con p primo dispari, sono tali che l'anello $\mathscr{O}_K$ non è neanche proiettivo sul suo ordine associato $\mathcal{A}_{K/\mathbb{Q}}$.

Parallelamente, però, sono state trovate altre estensioni di $\mathbb{Q}$ che si comportano in modo più simile alle estensioni abeliane: ad esempio Bergè in [1] e Martinet in [14] mostrano come le estensioni diedrali di $\mathbb{Q}$ di ordine $2p$, con p primo dispari, e le estensioni di Galois su $\mathbb{Q}$ con ramificazione wild e gruppo di Galois isomorfo al gruppo dei quaternioni sono tali che $\mathscr{O}_K$ è sempre libero sul suo ordine associato.

Ringraziamenti

In quest'ultima pagina vorrei ringraziare tutte le persone che più o meno direttamente mi hanno aiutato a raggiungere questo traguardo.
Innanzitutto un ringraziamento speciale va alla mia relatrice, la professoressa Ilaria Del Corso, per la pazienza e la disponibilità che mi ha sempre mostrato.
Un ringraziamento a tutti i miei amici di Pisa, in particolare agli amici del dipartimento, ai membri dei Cavalieri Jedi e agli inquilini di Casa Montello, per questi splendidi tre anni di università.
Un grazie ai miei amici di Poggibonsi e Colle, per le avventure vissute e il tempo trascorso insieme.
E infine grazie alla mia famiglia, senza il cui supporto non sarei mai diventato chi sono adesso.

Bibliografia

[1] A. M. Bergé, *Sur l'arithmétique d'une extension diédrale*, Annales de l'Institut Fourier 22, no 2, 1972.

[2] W. Bley, *A Leopoldt-type result for rings of integers of cyclotomic extensions*, Canad. Math. Bull. 38, 1995.

[3] S. Bosch, *Algebra*, Springer-Verlag, 2013.

[4] N. P. Byott, G. Lettl, *Relative Galois module structure of integers of Abelian fields*, J. Th. Nombres, 8, 1996.

[5] Ph. Cassou-Noguès, M. J. Taylor, *Elliptic functions and rings of integers*, Progress in Mathematics, Vol. 66, 1987.

[6] S. P. Chan, C.-H. Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, Journal f. d. reine u. angewandte Mathematik, 434, 1993.

[7] K. Girstmair, *An Index Formula for the Relative Class Number of an Abelian Number Field*, Journal of Number Theory 32, 1989.

[8] C. Greither, D. Replogle, K. Rubin, A. Srivastav, *Swan modules and Hilbert Speiser number fields*, Journal of Number Theory 79, 1999.

[9] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer-Verlag, 1950.

[10] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines Abelschen Zahlkörpers*, Journal f. d. reine u. angewandte Mathematik, 201, 1959.

[11] G. Lettl, *The ring of integers of an abelian number field*, Journal f. d. reine u. angewandte Mathematik, 404, 1990.

[12] D. A. Marcus, *Number Fields*, Springer-Verlag, 1977.

[13] J. Martinet, *Modules sur l'algèbre du groupe quaternionien*, Ann. Sc. de l'ENS, 4ème série, 1971.

[14] J. Martinet, *Sur les extensions à groupe de Galois quaternionien*, C.R. Acad. Sc. Paris 274-A, 1972.

[15] J. P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, 1977.

[16] J. P. Serre, *Local Fields*, Springer-Verlag, 1979.

[17] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.