View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Electronic Thesis and Dissertation Archive - Università di Pisa

Università degli Studi di Pisa

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea in Matematica

Tesi di Laurea Specialistica
27 settembre 2007

Alcuni problemi di class field theory

Candidato
Gabriele Dalla Torre

Relatore
Prof. Roberto Dvornicich
Università di Pisa

Controrelatrice
Prof.ssa Ilaria Del Corso
Università di Pisa

Anno Accademico 2006/2007

Indice

Introduzione

Uno dei più noti teoremi dimostrati da Fermat afferma che un numero primo dispari può essere scritto come somma di due quadrati perfetti se e solo se è congruo a 1 modulo 4. Questo risultato può essere visto come una conseguenza del fatto che l'anello $\mathbb{Z}[\sqrt{-1}]$ è a fattorizzazione unica ed una possibile dimostrazione consiste nell'osservare che un primo dispari si spezza completamente in $\mathbb{Q}(\sqrt{-1})$ se e soltanto se è congruo a 1 modulo 4.

In modo analogo è possibile dimostrare, usando la fattorizzazione unica negli anelli $\mathbb{Z}[\sqrt{2}]$ e $\mathbb{Z}[\zeta_3]$[1], che per ogni primo p

$$\begin{aligned} p = x^2 + 2y^2 &\iff p = 2 \text{ o } p \equiv 1, 3 \mod 8, \\ p = x^2 + 3y^2 &\iff p = 3 \text{ o } p \equiv 1 \mod 3. \end{aligned}$$

In generale, però, gli anelli della forma $\mathbb{Z}[\sqrt{n}]$ con $n \in \mathbb{N}$ non sono a fattorizzazione unica e solo con i lavori sulle forme quadratiche di Lagrange e Gauss è stato possibile superare questa difficoltà.

Già da questi primi risultati si capisce perché sia interessante conoscere la fattorizzazione di un ideale primo di un campo di numeri K in un'estensione L, ma lo diventa ancor di più quando si scopre che l'insieme degli ideali primi di K che si spezzano completamente in un'estensione di Galois L determina l'estensione. Per classificare le estensioni di Galois di K è quindi sufficiente determinare quali sono gli insiemi di ideali primi che si spezzano completamente in un'estensione normale di K e a questo problema, nel caso di estensioni quadratiche di $\mathbb{Q}$, risponde la celebre legge di reciprocità quadratica.

Con lo scopo di estendere il risultato ad un qualunque campo di numeri nel suo famoso discorso del 1900 all'ICM di Parigi Hilbert propose come nono problema lo sviluppo di una legge di reciprocità il più generale possibile. Il problema fu risolto, nel caso di estensioni abeliane, da Artin nel 1927 e la soluzione è oggi conosciuta come legge di reciprocità di Artin.

Proprio questo risultato è uno dei teoremi fondamentali della *class field theory*, teoria che studia le estensioni abeliane di un campo di numeri. Più precisamente,

[1] Con ζ_3 indichiamo una radice terza primitiva dell'unità.

se per aritmetica di un campo di numeri K intendiamo lo studio degli ideali di K, degli anelli quoziente ottenuti da questi ideali e del gruppo delle classi di ideali, allora la class field theory si propone di classificare tutte le estensioni abeliane finite L di un campo di numeri K, di realizzare i gruppi $\mathrm{Gal}(L/K)$ e di descrivere la fattorizzazione degli ideali primi di K in L in termini esclusivamente dell'aritmetica di K.

Una delle principali estensioni abeliane di un campo di numeri K della quale la class field theory dimostra l'esistenza è l'*Hilbert class field* di K, che è la massima estensione abeliana non ramificata di K. Questo risultato non è costruttivo ed infatti è ancora aperto il dodicesimo problema di Hilbert che chiede di generalizzare il teorema di Kronecker e Weber sulle estensioni abeliane di $\mathbb{Q}$ alle estensioni abeliane di un campo di numeri qualunque.

In questa tesi affrontiamo vari problemi di class field theory, in particolare il primo di questi consiste proprio nella costruzione esplicita dell'Hilbert class field del ventinovesimo campo ciclotomico $\mathbb{Q}(\zeta_{29})$. Grazie ai risultati di Kummer [18] sulla struttura del gruppo delle classi ideali di $\mathbb{Q}(\zeta_{29})$, dei quali riportiamo la dimostrazione contenuta nell'articolo di Gerth [7], e di Washington [29], il problema diventa di tipo essenzialmente computazionale. Nonostante questo la maggior parte del lavoro consiste nel produrre un insieme sufficientemente piccolo di candidati generatori dell'estensione, da cui sia possibile estrarre rapidamente, grazie all'utilizzo di un calcolatore, gli elementi cercati.

L'Hilbert class field di un'estensione normale di $\mathbb{Q}$ è un'estensione di Galois di $\mathbb{Q}$ e sorge quindi naturale chiedersi quale sia il suo gruppo di Galois assoluto. La struttura di questo gruppo è stata a lungo studiata, soprattutto nel caso di campi di numeri quadratici. In questo lavoro calcoliamo il gruppo di Galois dell'Hilbert class field del ventinovesimo campo ciclotomico in modo indipendente dal modo in cui abbiamo costruito l'estensione.

Presentiamo poi brevemente la teoria dei nodi di Scholz [24] e Jehne [15] e studiamo, seguendo principalmente gli articoli di Gras [8], Cornell [3] e Inaba [11], le estensioni assolute cicliche di grado primo dispari ℓ con interesse rivolto soprattutto all'ℓ-rango del gruppo delle classi di ideali. Proponiamo infine una nuova dimostrazione di un risultato del 2007 di Nomura [23] che riguarda una condizione necessaria affinché la lunghezza dell'Hilbert 3-class field tower di un campo ciclico cubico assoluto sia strettamente maggiore di 1.

Elenco dei simboli

ζ_n	radice ennesima dell'unità
E	gruppo delle unità
$\mathrm{Cl}(K)$	gruppo delle classi di ideali del campo K
$\mathrm{Cl}_p(K)$	p-sottogruppo di Sylow di $\mathrm{Cl}(K)$
C_n	gruppo delle unità ciclotomiche del campo $\mathbb{Q}(\zeta_n)$
Ver	omomorfismo Verlagerung
G'	sottogruppo del gruppo G generato dai commutatori
K^1	Hilbert class field del campo K
Ω_K	gruppo delle radici dell'unità in un campo K
$\mathrm{Gal}(L/K)$	gruppo di Galois di L su K
h_K	numero delle classi di ideali del campo di numeri K
$\mathcal{O}_K$	interi algebrici del campo K
$e(\mathfrak{P}\|\mathfrak{p})$	indice di ramificazione dell'ideale primo $\mathfrak{P}$ su $\mathfrak{p}$
$f(\mathfrak{P}\|\mathfrak{p})$	indice di inerzia dell'ideale primo $\mathfrak{P}$ su $\mathfrak{p}$
$\mathrm{Aut}(G)$	gruppo degli automorfismi del gruppo G
$\mathrm{Ker}(\varphi)$	nucleo della funzione φ
$\mathrm{Im}(\varphi)$	nucleo della funzione φ
Coker	conucleo
S_n	gruppo delle permutazioni di n elementi
I	gruppo degli ideali frazionari
P	gruppo degli ideali frazionari principali
$\mathfrak{M}$	divisore
$\mathfrak{D}$	discriminante
N	norma
$\mathfrak{f}$	conduttore
K_F^*	relative genus field di K rispetto a F
$\mathcal{M}(G)$	moltiplicatore di Schur del gruppo finito G
$K_\mathfrak{p}$	completamento del campo K rispetto al valore assoluto $\mathfrak{p}$-adico
$U_\mathfrak{p}$	unità di $K_\mathfrak{p}$
$\mathcal{C}$	gruppo delle classi degli ideli
$\mathcal{E}$	gruppo delle classi delle unità degli ideli

Capitolo 1

Preliminari di teoria algebrica dei numeri

In questo primo capitolo introduttivo presentiamo sinteticamente i concetti fondamentali e alcuni dei primi risultati della teoria algebrica dei numeri. Per maggiori dettagli consigliamo di consultare i libri di Cassels e Fröhlich [2], di Marcus [20] e di Serre [26].

1.1 Campi di numeri

L'oggetto di studio principale della teoria algebrica dei numeri sono i campi di numeri.

Definizione 1.1 (Campo di numeri)**.** Un *campo di numeri* K è un'estensione algebrica finita di $\mathbb{Q}$.

Possiamo rappresentare un campo di numeri K come l'insieme di tutti i polinomi in un certo numero algebrico α a coefficienti in $\mathbb{Q}$:

$$K = \mathbb{Q}[\alpha] = \left\{ \sum_{n=0}^{m-1} a_n \alpha^n : a_n \in \mathbb{Q} \right\},$$

dove m è il grado di un polinomio irriducibile su $\mathbb{Q}$ avente α come radice.

Tra gli elementi della chiusura algebrica $\overline{\mathbb{Q}}$ di $\mathbb{Q}$ sono di interesse particolare quelli che sono interi su $\mathbb{Z}$.

Definizione 1.2 (Intero algebrico)**.** Un elemento α di $\overline{\mathbb{Q}}$ è un *intero algebrico* se è radice di un polinomio monico a coefficienti in $\mathbb{Z}$.

Proposizione 1.3. *L'insieme $\mathcal{O}_{\overline{\mathbb{Q}}}$ di tutti gli interi algebrici è un anello.*

All'interno di un campo di numeri K possiamo così individuare un anello.

Definizione 1.4 (Anello degli interi)**.** Definiamo *anello degli interi* di un campo di numeri K il sottoanello $\mathcal{O}_K = \mathcal{O}_{\overline{\mathbb{Q}}} \cap K$.

La struttura additiva dell'anello degli interi $\mathcal{O}_K$ di un campo di numeri K è ben nota.

Teorema 1.5. *Sia K un campo di numeri di grado n su $\mathbb{Q}$. Allora l'anello degli interi $\mathcal{O}_K$ di K è un gruppo abeliano libero di ordine n, cioè $\mathcal{O}_K \cong \mathbb{Z}^n$.*

Esistono perciò dei generatori di $\mathcal{O}_K$ come $\mathbb{Z}$-modulo.

Definizione 1.6 (Base intera)**.** Sia K un campo di numeri di grado n su $\mathbb{Q}$. Una *base intera* dell'anello $\mathcal{O}_K$ è una n-tupla di elementi $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ che generano $\mathcal{O}_K$ come $\mathbb{Z}$-modulo.

Una base intera di un campo di numeri non è un invariante del campo, in quanto non è unica.

Definizione 1.7 (Discriminante)**.** Sia K un campo di numeri di grado n su $\mathbb{Q}$ e siano $\sigma_1, \ldots, \sigma_n$ le n immersioni di K in $\mathbb{C}$. Per ogni n-tupla di elementi $\alpha_1, \ldots, \alpha_n \in K$ definiamo *discriminante* di $\alpha_1, \ldots, \alpha_n$ il numero

$$\mathfrak{D}(\alpha_1, \ldots, \alpha_n) = \det[\sigma_i(\alpha_j)]^2,$$

dove con $[a_{ij}]$ indichiamo la matrice tale che a_{ij} è l'elemento nella riga i-esima e nella colonna j-esima.

Il discriminante ci permette di definire un invariante di un campo di numeri, poiché tutte le basi intere di un campo di numeri hanno lo stesso discriminante.

Definizione 1.8 (Discriminante di un campo di numeri)**.** Sia K un campo di numeri. Chiamiamo *discriminante del campo di numeri K* o *discriminante dell'anello degli interi $\mathcal{O}_K$* e lo indichiamo con $\mathfrak{D}(K)$ o con $\mathfrak{D}(\mathcal{O}_K)$ il discriminante di una base intera di $\mathcal{O}_K$.

1.2 Fattorizzazione unica degli ideali

Da un dominio di integrità R possiamo costruire un campo che contiene R.

Definizione 1.9 (Campo delle frazioni)**.** Il *campo delle frazioni* di un dominio di integrità R è il campo

$$k = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in R,\ \beta \neq 0 \right\}.$$

Definizione 1.10 (Integralmente chiuso)**.** Un dominio di integrità R è *integralmente chiuso* nel suo campo delle frazioni k se ogni $\frac{\alpha}{\beta} \in k$ radice di un polinomio monico a coefficienti in R appartiene a R.

Definiamo ora un'importante classe di domini di integrità, della quale fa parte, in particolare, ogni anello degli interi di campo di numeri.

Definizione 1.11 (Dominio di Dedekind)**.** Un dominio d'integrità R è un *dominio di Dedekind* se verifica le seguenti proprietà:

- è noetheriano;
- ogni ideale primo diverso dallo zero è massimale;
- è integralmente chiuso nel suo campo delle frazioni.

Uno dei motivi di studio dei domini di Dedekind è la seguente proprietà di fattorizzazione.

Teorema 1.12 (Fattorizzazione unica degli ideali)**.** *In un dominio di Dedekind R ogni ideale proprio non nullo I di R può essere scritto come prodotto di ideali primi in modo unico a meno dell'ordine, cioè*

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i},$$

con $\mathfrak{p}_i$ ideali primi distinti e $e_i \geq 0$.

Ora che sappiamo come si fattorizzano gli ideali all'interno un campo di numeri K, possiamo chiederci cosa accade in un'estensione L di K. Per il teorema 1.12 è sufficiente limitarsi a studiare il caso di un ideale primo $\mathfrak{p}$ di $\mathcal{O}_K$. Quello che vogliamo studiare è quindi la decomposizione in ideali primi dell'ideale esteso $\mathfrak{p}\mathcal{O}_L$, visto che $\mathfrak{p}\mathcal{O}_L$ non è, in generale, un ideale primo.

Proposizione 1.13. *Sia L/K un'estensione di campi di numeri e siano $\mathfrak{p}$ e $\mathfrak{P}$ rispettivamente un ideale primo di $\mathcal{O}_K$ e un ideale primo di $\mathcal{O}_L$. Le seguenti condizioni sono allora equivalenti:*

- $\mathfrak{P} | \mathfrak{p}\mathcal{O}_L$;
- $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L$;
- $\mathfrak{P} \supseteq \mathfrak{p}$;
- $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$;

- $\mathfrak{P} \cap K = \mathfrak{p}$.

Definizione 1.14. Sia L/K un'estensione di campi di numeri e siano $\mathfrak{p}$ e $\mathfrak{P}$ rispettivamente un ideale primo di $\mathcal{O}_K$ e un ideale primo di $\mathcal{O}_L$. Diciamo che $\mathfrak{P}$ sta sopra $\mathfrak{p}$ o che $\mathfrak{p}$ sta sotto $\mathfrak{P}$ se valgono le condizioni della proposizione precedente 1.13.

Proposizione 1.15. *Ogni ideale primo $\mathfrak{P}$ di $\mathcal{O}_L$ sta sopra ad un unico ideale primo $\mathfrak{p}$ di $\mathcal{O}_K$; ogni ideale primo $\mathfrak{p}$ di $\mathcal{O}_K$ sta sotto ad almeno un ideale primo $\mathfrak{P}$ di $\mathcal{O}_L$.*

I primi sopra $\mathfrak{p}$ sono perciò i primi $\mathfrak{P}_i$ che compaiono nella fattorizzazione di $\mathfrak{p}\mathcal{O}_L$ in primi:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}.$$

1.3 Ramificazione ed inerzia

Dato un campo di numeri K useremo spesso l'espressione "ideale di K" per indicare invece un ideale dell'anello degli interi $\mathcal{O}_K$. In questa sezione studiamo più in dettaglio la fattorizzazione dell'ideale esteso $\mathfrak{p}\mathcal{O}_L$ di un ideale primo $\mathfrak{p}$ di K, dove L è un'estensione algebrica di un campo di numeri K. Cominciamo con alcune definizioni fondamentali.

Definizione 1.16 (Indice di ramificazione)**.** Sia L/K un'estensione di campi di numeri e sia $\mathfrak{P}$ un ideale primo di $\mathcal{O}_L$ sopra un ideale primo $\mathfrak{p}$ di $\mathcal{O}_K$. Definiamo *indice di ramificazione* di $\mathfrak{P}$ sopra $\mathfrak{p}$ e lo indichiamo con $e(\mathfrak{P}|\mathfrak{p})$ l'esponente di $\mathfrak{P}$ che compare nella fattorizzazione di $\mathfrak{p}\mathcal{O}_L$, cioè l'esatta potenza di $\mathfrak{P}$ che divide $\mathfrak{p}\mathcal{O}_L$.

Definizione 1.17 (Grado d'inerzia)**.** Sia L/K un'estensione di campi di numeri e sia $\mathfrak{P}$ un ideale primo di $\mathcal{O}_L$ sopra un ideale primo di $\mathcal{O}_K$. Definiamo *grado d'inerzia* di $\mathfrak{P}$ sopra $\mathfrak{p}$ e lo indichiamo con $f(\mathfrak{P}|\mathfrak{p})$ il grado dell'estensione di campi finiti $\mathcal{O}_L/\mathfrak{P}$ su $\mathcal{O}_K/\mathfrak{p}$.

I prossimi due risultati sono molti utili per calcolare l'indice di ramificazione e il grado di inerzia.

Proposizione 1.18. *L'indice di ramificazione e il grado di inerzia sono moltiplicativi nelle torri di estensioni, cioè, se $\wp \subseteq \mathfrak{p} \subseteq \mathfrak{P}$ sono ideali primi rispettivamente di tre campi di numeri $F \subseteq K \subseteq L$, allora*

$$e(\mathfrak{P}|\wp) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|\wp),$$
$$f(\mathfrak{P}|\wp) = f(\mathfrak{P}|\mathfrak{p})f(\mathfrak{p}|\wp).$$

Teorema 1.19 (Formula dimensionale)**.** *Sia L/K un'estensione di campi di numeri di grado n e siano $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ gli ideali primi di L sopra un ideale primo $\mathfrak{p}$ di K. Allora, posto $e_i = e(\mathfrak{P}_i|\mathfrak{p})$ e $f_i = f(\mathfrak{P}_i|\mathfrak{p})$, vale la seguente uguaglianza:*

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

Definizione 1.20 (Ideale primo ramificato)**.** Sia L/K un'estensione di campo di numeri. Diciamo che un ideale primo di K è *ramificato* in L se $e(\mathfrak{P}|\mathfrak{p}) > 1$ per qualche ideale primo $\mathfrak{P}$ di $\mathcal{O}_L$ che sta sopra $\mathfrak{p}$, cioè se $\mathfrak{p}\mathcal{O}_L$ non è libero da quadrati.

Teorema 1.21. *Sia K un campo di numeri. Un ideale primo p di $\mathbb{Q}$ ramifica in K se e solo se $\mathfrak{p}|\mathfrak{D}(K)$.*

Dal precedente teorema otteniamo un interessante corollario.

Corollario 1.22. *Sia L/K un'estensione di campi di numeri. Gli ideali primi di K che ramificano in L sono in numero finito.*

Definizione 1.23 (Norma di un ideale)**.** La *norma di un ideale I* dell'anello degli interi $\mathcal{O}_K$ di un campo di numeri K è il numero di elementi di $\mathcal{O}_K/I$ e la indichiamo con $\|I\|$.

Proposizione 1.24. *La norma è moltiplicativa, cioè, dati due ideali I e J di R, $\|IJ\| = \|I\|\|J\|$.*

Consideriamo un'estensione L/K di campi di numeri di grado $[L : K] = n$. Fissiamo un elemento $\alpha \in \mathcal{O}_L$ di grado n su K, così che $L = K(\alpha)$. Allora $\mathcal{O}_K[\alpha]$ è un sottogruppo additivo di $\mathcal{O}_L$ tale che $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ è un gruppo finito.

Sia $g(x)$ il polinomio monico irriducibile di α su K. Riducendo i coefficienti modulo $\mathfrak{p}$, con $\mathfrak{p}$ ideale primo di K, otteniamo il polinomio $\bar{g}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$. Fattorizzando $\bar{g}(x)$ come prodotto di polinomi monici irriducibili distinti $\bar{g}_i(x)$ di $(\mathcal{O}_K/\mathfrak{p})[x]$, ricaviamo

$$\bar{g}(x) = \prod_{i=1}^{r} \bar{g}_i(x)^{e_i},$$

dove ogni $g_i(x)$ è un polinomio monico su $\mathcal{O}_K$.

Teorema 1.25. *Sia L/K un'estensione finita di campi di numeri. Se p non divide l'ordine di $\mathcal{O}_L/\mathcal{O}_K[\alpha]$, dove p è il primo di $\mathbb{Z}$ sotto $\mathfrak{p}$, allora la fattorizzazione di $\mathfrak{p}\mathcal{O}_L$ è*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i},$$

dove, per ogni $i \in \{1, \ldots, r\}$, $\mathfrak{q}_i$ è l'ideale primo $(\mathfrak{p}, g_i(\alpha))$ di $\mathcal{O}_L$. Inoltre $f(\mathfrak{q}_i|\mathfrak{p})$ è uguale al grado di g_i.

Osservazione 1.26. *La condizione per p è soddisfatta, in particolare, quando $L = \mathbb{Q}(\alpha)$ e $p^2 \nmid \mathfrak{D}(\alpha)$.*

1.4 Estensioni di Galois

Definizione 1.27 (Estensione normale e gruppo di Galois)**.** Sia L/K un'estensione di campi di numeri e sia $\mathrm{Aut}(L/K)$ il gruppo degli automorfismi di L che fissano puntualmente K. Diciamo che L/K è un'*estensione normale* (o *di Galois*) se $\#\,\mathrm{Aut}(L/K) = [L : K]$. In tal caso, inoltre, chiamiamo $\mathrm{Aut}(L/K)$ *gruppo di Galois* di L/K e lo indichiamo con $\mathrm{Gal}(L/K)$.

Proposizione 1.28. *Sia L/K un'estensione normale di campi di numeri. Sia inoltre $\sigma \in \mathrm{Gal}(L/K)$ e sia $\mathfrak{P}$ un ideale primo non nullo di $\mathcal{O}_L$ sopra l'ideale primo $\mathfrak{p}$ di $\mathcal{O}_K$. Allora $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ e $\sigma(\mathfrak{P})$ è un ideale primo di $\mathcal{O}_L$ sopra $\mathfrak{p}$.*

Dimostrazione. Se $x \in \mathcal{O}_L$, allora $\sigma(x) \in \mathcal{O}_L$, poiché la relazione di dipendenza integrale di x su $\mathcal{O}_L$ non viene modificata applicando σ. Quindi $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$, ma anche $\sigma^{-1}(\mathcal{O}_L) \subseteq \mathcal{O}_L$ e perciò

$$\mathcal{O}_L = \sigma\sigma^{-1}(\mathcal{O}_L) \subseteq \sigma(\mathcal{O}_L).$$

Estendiamo l'ideale primo non nullo $\mathfrak{p}$ di $\mathcal{O}_K$ all'ideale $\mathfrak{p}\mathcal{O}_L$ e fattorizziamolo in ideali primi di $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}.$$

Applicando σ ricaviamo

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \sigma(\mathfrak{P}_i)^{e_i},$$

con $\sigma(\mathfrak{P}_i)$ ideali primi, visto che σ conserva tutte le relazioni algebriche. Inoltre σ è un automorfismo di L che fissa K, quindi fissa ogni elemento di $\mathcal{O}_K$ e a maggior ragione ogni elemento di $\mathfrak{p}$ e dunque

$$\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \Rightarrow \sigma(\mathfrak{P}) \cap \mathcal{O}_K = \mathfrak{p}.$$

□

Teorema 1.29. *Sia L/K un'estensione normale di campi di numeri e siano $\mathfrak{P}_i$ e $\mathfrak{P}_j$ due ideali primi di $\mathcal{O}_L$ sopra l'ideale primo $\mathfrak{p}$ di $\mathcal{O}_K$. Allora l'azione del gruppo di Galois $\mathrm{Gal}(L/K)$ è transitiva sui primi sopra il primo $\mathfrak{p}$, esiste cioè $\sigma \in \mathrm{Gal}(L/K)$ tale che $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.*

Dimostrazione. Supponiamo, per assurdo, che non esista alcun $\sigma \in \mathrm{Gal}(L/K)$ per il quale $\sigma\mathfrak{P}_i = \mathfrak{P}_j$. Allora, per il teorema cinese del resto, esiste un elemento $x \in \mathfrak{P}_j$ di $\mathcal{O}_L$ tale che $x \notin \sigma(\mathfrak{P}_i)$ per ogni $\sigma \in \mathrm{Gal}(L/K)$. Calcolando la norma di x relativa a L/K otteniamo

$$N_K^L(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x).$$

Poiché uno dei fattori è $x \in \mathfrak{P}_j$ e $N_K^L(x) \in \mathcal{O}_K$, abbiamo che $N_K^L(x) \in \mathfrak{P}_j \cap K$. Però $\mathfrak{P}_j \cap \mathcal{O}_K = \mathfrak{p} = \mathfrak{P}_i \cap \mathcal{O}_K$ e quindi, essendo $\mathfrak{P}_i$ un ideale primo, esiste σ tale che $\sigma^{-1}(x) \in \mathfrak{P}_i$. Perciò $x \in \sigma(\mathfrak{P}_i)$ e questo è assurdo. □

Corollario 1.30. *Sia L/K un'estensione normale di campi di numeri e sia $\mathfrak{p}$ un ideale primo non nullo di $\mathcal{O}_K$ tale che*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

sia la fattorizzazione in $\mathcal{O}_L$ del suo ideale esteso $\mathfrak{p}\mathcal{O}_L$. Allora l'indice di ramificazione e_i è lo stesso per ogni i, così come il grado di inerzia relativo $f_i = f(\mathfrak{P}|\mathfrak{p})$. Pertanto, se definiamo con e l'indice di ramificazione e con f il grado d'inerzia comuni, la formula dimensionale si semplifica in

$$[L : K] = ref.$$

Dimostrazione. Segue immediatamente dal fatto che, per il teorema 1.29, l'azione di $\mathrm{Gal}(L/K)$ sull'insieme $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ è transitiva e che ogni automorfismo $\sigma \in \mathrm{Gal}(L/K)$ conserva tutte le le relazioni algebriche. □

1.5 Valori assoluti e valutazioni

Definizione 1.31 (Valore assoluto)**.** Un *valore assoluto* $|\cdot|$ su un campo k è una funzione da k nei numeri reali non negativi tale che, per ogni $x, y \in k$,

- $|x| = 0$ se e solo se $x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \leq |x| + |y|$.

Diciamo che il valore assoluto $|\cdot|$ è non archimedeo se inoltre vale

$$|x + y| \leq \max\{|x|, |y|\},$$

altrimenti diciamo che è archimedeo.

Il valore assoluto banale su K è la mappa che manda ogni $x \in K^*$ in 1 e 0 in 0.

Ogni valore assoluto $|\cdot|$ su k induce una metrica su k, definendo la distanza $d(x, y)$ tra due elementi x e y di k come

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

Viene quindi indotta anche una topologia su k che rende k un campo topologico. In questa topologia un insieme di intorni fondamentali dello 0 è dato dagli insiemi $\{x \in k : |x| \leq \epsilon, \epsilon \in \mathbb{R}^+\}$.

Definizione 1.32 (Equivalenza di valori assoluti)**.** Due valori assoluti $|\cdot|_1$ e $|\cdot|_2$ su k sono *equivalenti* se e solo se esiste $\lambda \in \mathbb{R}^+$ tale che $|\cdot|_2 = |\cdot|_1^{\lambda}$.

Proposizione 1.33. *Due valori assoluti sono equivalenti se gli spazi topologici che inducono sono omeomorfi.*

Strettamente legate ai valori assoluti sono le valutazioni.

Definizione 1.34 (Valutazione)**.** Una *valutazione* su un campo k è una funzione $v : k \to \mathbb{R} \cup \{+\infty\}$ tale che, per ogni $x, y \in k$,

- $v(x) = +\infty$ se e solo se $x = 0$;
- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \min\{v(x), v(y)\}$.

Diciamo che v è una valutazione discreta se l'immagine $v(k^*)$ è un sottogruppo discreto di $\mathbb{R}$. In questo caso possiamo normalizzare v in modo che $v(k^*) = \mathbb{Z}$.

Un modo per costruire dei valori assoluti è usare le valutazioni. Infatti, data una valutazione v su k, possiamo definire un valore assoluto $|\cdot|_v$ ponendo, per ogni $x \in k$, $|x|_v = s^{-v(x)}$, dove $s > 0$.

Definizione 1.35 (Valutazione $\mathfrak{p}$-adica)**.** Siano K un campo di numeri, $\mathcal{O}_K$ l'anello degli interi di K e $\mathfrak{p}$ un ideale primo di $\mathcal{O}_K$. Consideriamo la funzione $v_{\mathfrak{p}}$ tale che, per ogni $x \in \mathcal{O}_K$,

$$v_{\mathfrak{p}}(x) = \max\{n \in \mathbb{N} : x \in \mathfrak{p}^n\}.$$

Chiamiamo *valutazione* $\mathfrak{p}$*-adica* l'estensione di $v_{\mathfrak{p}}$ a K, ottenuta ponendo $v_p(x/y) = v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(y)$, dove $x, y \in K$. La definizione è chiaramente indipendente dalla scrittura in forma di frazione di x/y e si può inoltre verificare che $v_{\mathfrak{p}}$ è una valutazione discreta.

Definizione 1.36 (Valore assoluto $\mathfrak{p}$-adico)**.** Chiamiamo *valore assoluto* $\mathfrak{p}$*-adico* il valore assoluto $|\cdot|_\mathfrak{p}$ associato alla valutazione $\mathfrak{p}$-adica $v_\mathfrak{p}$ ottenuto ponendo, per ogni $x \in K$,

$$|x|_\mathfrak{p} = (N\mathfrak{p})^{-v_\mathfrak{p}(x)}.$$

Il teorema di Ostrowski fornisce la classificazione di tutti i valori assoluti su $\mathbb{Q}$.

Teorema 1.37 (Ostrowski)**.** *Ogni valore assoluto non banale su* $\mathbb{Q}$ *è equivalente ad un valore assoluto* $\mathfrak{p}$*-adico* $|\cdot|_\mathfrak{p}$ *o all'ordinario valore assoluto* $|\cdot|_\infty$*.*

In generale, per un campo di numeri K, possono esistere più valori assoluti archimedei, come possiamo vedere dalla prossima definizione.

Definizione 1.38 (Valori assoluti archimedei reali e complessi)**.** Sia K un campo di numeri di grado $n = r+2s$ su $\mathbb{Q}$. Per ognuna delle r immersioni reali $\sigma : K \hookrightarrow \mathbb{R}$ definiamo il seguente valore assoluto $|\cdot|_\sigma$:

$$|x|_\sigma = |\sigma(x)|, \quad \forall x \in K^*.$$

Similmente per ognuna delle s coppie di immersioni complesse coniugate $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$ definiamo il valore assoluto $|\cdot|_\sigma = |\cdot|_{\bar{\sigma}}$:

$$|x|_\sigma = |\sigma(x)|^2, \quad \forall x \in K^*.$$

Chiamiamo *valori assoluti archimedei reali* su K gli r valori assoluti su K ottenuti dalle immersioni reali di K, mentre chiamiamo *valori assoluti archimedei complessi* gli s valori assoluti su K ottenuti dalle immersioni complesse di K.

1.6 Completamenti

Definizione 1.39 (Campo completo)**.** Un campo k è *completo* rispetto ad un valore assoluto $|\cdot|$ se è uno spazio metrico completo rispetto alla distanza $d(x, y) = |x - y|$, dove $x, y \in k$, cioè se ogni successione di Cauchy ha limite in k.

Definizione 1.40 (Numeri p-adici)**.** Il completamento di $\mathbb{Q}$ rispetto ad un valore assoluto p-adico è il campo dei *numeri* p*-adici* e lo indichiamo con il simbolo $\mathbb{Q}_p$. L'anello degli interi di $\mathbb{Q}_p$, che chiamiamo anello degli interi p-adici, è l'insieme

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Analogamente, per un campo di numeri K con un valore assoluto $\mathfrak{p}$-adico $|\cdot|_\mathfrak{p}$, indichiamo con $K_\mathfrak{p}$ il completamento di K rispetto al valore assoluto $|\cdot|_\mathfrak{p}$ e con $\mathcal{O}_\mathfrak{p}$ l'anello degli interi di $K_\mathfrak{p}$. Usiamo inoltre il simbolo $U_\mathfrak{p}$ per il gruppo $\mathcal{O}_\mathfrak{p}^*$ delle unità di $\mathcal{O}_\mathfrak{p}$.

Definizione 1.41 (Estensione di un valore assoluto)**.** Siano K e L due campi con $K \subseteq L$ e siano $|\cdot|_K$ e $|\cdot|_L$ due valori assoluti rispettivamente su K e L. Diciamo che il valore assoluto $|\cdot|_L$ è un'*estensione del valore assoluto* $|\cdot|_K$ se $|\alpha|_L = |\alpha|_K$ per ogni $\alpha \in K$.

Il vantaggio di lavorare con i campi completi è ben espresso dal seguente teorema.

Teorema 1.42. *Sia K un campo completo rispetto ad un valore assoluto $|\cdot|$ e sia L un'estensione finita di K di grado finito n. Esiste allora un'unica estensione del valore assoluto $|\cdot|$ a L, data dalla formula*

$$|\alpha| = |N_K^L(\alpha)|^{1/n},$$

dove α è un qualunque elemento di L.

Nel caso dei numeri p-adici l'anello degli interi $\mathbb{Z}_p$ è locale e quindi, se consideriamo un'estensione finita di $\mathbb{Q}_p$ e un ideale primo $\mathfrak{p}$ sopra p, il valore assoluto $\mathfrak{p}$-adico opportunamente rinormalizzato estende quello p-adico.

Sia K un campo di numeri. Poiché $K/\mathbb{Q}$ è un'estensione separabile, allora esiste, per il teorema dell'elemento primitivo, un elemento $\alpha \in K$ tale che $K = \mathbb{Q}(\alpha)$. Sia $f(x) \in \mathbb{Q}[x]$ il polinomio minimo di α. Se su K c'è con un valore assoluto v che ristretto a $\mathbb{Q}$ è il valore assoluto p-adico, possiamo considerare l'estensione dei completamenti $K_v/\mathbb{Q}_p$ e mostrare che $K_v = \mathbb{Q}(\alpha)$. Sia

$$f(x) = f_1(x) \cdots f_r(x)$$

la fattorizzazione del polinomio $f(x)$ su $\mathbb{Q}_p[x]$. Chiaramente il polinomio minimo di α su $\mathbb{Q}_p$ è uno dei fattori $f_i(x)$ di $f(x)$.

Dato invece un fattore $f_i(x)$ di $f(x)$, possiamo considerare il campo $\mathbb{Q}_p[x]/f_i(x)$ e osservare che, per il teorema 1.42, esiste un'unica estensione del valore assoluto p-adico. Poichè possiamo immergere K in $\mathbb{Q}_p[x]/f_i(x)$, restringendo a K l'estensione del valore assoluto p-adico otteniamo un valore assoluto su K che estende il valore assoluto p-adico.

Abbiamo così stabilito una corrispondenza biunivoca tra i valori assoluti su un campo K che estendono il valore assoluto p-adico e i fattori irriducibili di $f(x)$ su $\mathbb{Q}_p$. In maniera analoga possiamo dimostrare che ogni valore assoluto su K che estende l'ordinario valore assoluto su $\mathbb{Q}$ deriva da un'immersione di K in $\mathbb{C}$.

Osservando che ogni valore assoluto su K che estende il valore assoluto p-adico si ottiene restringendo un valore assoluto $\mathfrak{p}$-adico di un'estensione finita di $\mathbb{Q}_p$ e che le estensioni del valore assoluto ordinario a K non sono altro che i valori assoluti archimedei reali e complessi, riusciamo a classificare, a meno di equivalenza, tutti i valori assoluti su un campo di numeri K.

Teorema 1.43. *Ogni valore assoluto non banale su un campo di numeri K è equivalente ad un valore assoluto appartenente ad uno dei seguenti insiemi:*

- *i valori assoluti $\mathfrak{p}$-adici;*
- *i valori assoluti archimedei reali;*
- *i valori assoluti archimedei complessi.*

Possiamo pertanto dare la seguente definizione.

Definizione 1.44 (Primo)**.** Sia K un campo di numeri. Definiamo *primo* di K una classe di equivalenza di valori assoluti non banali su K.

1.7 Adeli ed ideli

Prima di introdurre il concetto di adele è utile definire il prodotto topologico ristretto. Facciamo presente che dato un insieme Λ useremo spesso, per brevità di scrittura, l'espressione "per quasi ogni λ in Λ" al posto della locuzione "per tutti i λ in Λ tranne un numero finito".

Definizione 1.45 (Prodotto topologico ristretto)**.** Sia X_λ, con $\lambda \in \Lambda$, una famiglia di spazi topologici e per quasi ogni $\lambda \in \Lambda$ sia $Y_\lambda \subseteq X_\lambda$ un sottoinsieme aperto di X_λ. Consideriamo lo spazio X che contiene le successioni $\alpha = \{\alpha_\lambda\}_{\lambda\in\Lambda}$, dove $\alpha_\lambda \in X_\lambda$ per ogni $\lambda \in \Lambda$ e $\alpha_\lambda \in Y_\lambda$ per quasi ogni $\lambda \in \Lambda$. Dotiamo X di una topologia definendo una base di aperti gli insiemi $\prod W_\lambda$, dove $W_\lambda \subseteq X_\lambda$ è aperto per ogni λ e $W_\lambda = Y_\lambda$ per quasi ogni λ. Con questa topologia chiamiamo lo spazio X *prodotto topologico ristretto* degli spazi X_λ rispetto agli insiemi Y_λ.

Definizione 1.46 (Anello degli adeli)**.** Sia K un campo di numeri. Chiamiamo *anello degli adeli* $\mathbb{A}_K$ di K l'anello topologico dato dal prodotto topologico ristretto degli spazi $K_\mathfrak{p}$, con $\mathfrak{p}$ che corre tra tutti i primi di K, rispetto agli insiemi $\mathcal{O}_\mathfrak{p}$ con le operazioni di somma e prodotto definite componente per componente.

Un adele α di K è pertanto una famiglia $\alpha = (\alpha_\mathfrak{p})$ di elementi $\alpha_\mathfrak{p}$ di $K_\mathfrak{p}$, dove $\mathfrak{p}$ corre tra tutti i primi di K, e tale che $\alpha_\mathfrak{p}$ è intero in $K_\mathfrak{p}$ per tutti i $\mathfrak{p}$ tranne un numero finito.

C'è un'inclusione continua naturale $K \hookrightarrow \mathbb{A}_K$ che mappa ogni $x \in K$ nell'adele che ha tutte le componenti uguali a x. Poiché questa mappa è iniettiva, identificando K con la sua immagine, possiamo considerare K un sottoanello di $\mathbb{A}_K$.

Definizione 1.47 (Anello degli adeli principali)**.** Chiamiamo *anello degli adeli principali* l'immagine dell'inclusione naturale $K \hookrightarrow \mathbb{A}_K$.

Dato un anello topologico commutativo R, l'insieme R^* degli elementi invertibili di R è un gruppo con la moltiplicazione. In generale, però, R^* non è un gruppo topologico con la topologia indotta dall'essere un sottoinsieme di R, in quanto l'inversione non è necessariamente continua. Per questo motivo dotiamo solitamente R^* della topologia indotta dall'essere un sottoinsieme del prodotto topologico $R \times R$ con l'inclusione $x \mapsto (x, x^{-1})$. Con questa topologia R^* è un gruppo topologico e l'inclusione $R^* \hookrightarrow R$ è continua.

Definizione 1.48 (Gruppo degli ideli)**.** Sia K un campo di numeri. Chiamiamo *gruppo degli ideli* J_K di K il prodotto topologico ristretto degli spazi K_v^* rispetto ai gruppi delle unità $U_v = \mathcal{O}_v^* \subseteq K_v$ con la topologia prodotto ristretta.

Il gruppo degli ideli J_K di un campo di numeri K è un sottoinsieme dell'anello degli adeli, ma è importante fare la seguente precisazione.

Osservazione 1.49. *Il gruppo degli ideli J_K di un campo di numeri K è il gruppo $\mathbb{A}_K^*$ degli elementi invertibili di $\mathbb{A}_K$, ma la topologia di J_K non è quella indotta dall'essere un sottoinsieme di $\mathbb{A}_K$.*

Nello stesso modo in cui K si immerge naturalmente in $\mathbb{A}_K$, così anche K^* si immerge naturalmente in J_K.

Definizione 1.50 (Gruppo degli ideli principali)**.** Chiamiamo *gruppo degli ideli principali* l'immagine dell'inclusione naturale $K^* \hookrightarrow J_K$.

Capitolo 2

Class field theory

Per class field theory si intende solitamente lo studio delle estensioni abeliane finite di un campo di numeri K. In questo capitolo presentiamo i risultati classici di questa teoria.

2.1 Divisori e ray class group

Sia K un campo di numeri, sia $\mathcal{O}_K$ l'anello degli interi di K e sia E il gruppo delle unità di K. Per una valutazione v di K intendiamo, con un piccolo abuso di linguaggio, una classe di equivalenza di valori assoluti non banali di K, cioè un primo di K. Dal teorema 1.43 sappiamo che esistono due diversi tipi di valori assoluti: i valori assoluti archimedei e quelli non archimedei. Inoltre ogni classe di equivalenza di valori assoluti non archimedei è in corrispondenza biunivoca con l'insieme degli ideali primi di K e pertanto talvolta indichiamo una valutazione non archimedea con l'ideale primo corrispondente. Per uniformità di scrittura introduciamo quindi anche i cosiddetti primi infiniti che corrispondono alle valutazioni archimedee. Con questa notazione, dato un elemento $x \in K$ e un primo infinito reale $\mathfrak{p}$, indichiamo con $x_\mathfrak{p}$ l'immagine di x tramite l'immersione $\sigma : K \hookrightarrow \mathbb{R}$ associata al valore assoluto archimedeo reale corrispondente a $\mathfrak{p}$.

Siano inoltre I e P rispettivamente il gruppo degli ideali frazionari di K ed il gruppo degli ideali frazionari principali di K. Con $\mathrm{Cl}(K)$ indichiamo il gruppo delle classi ideali di K, cioè il quoziente I/P e con h_K il numero delle classi di K.

Definizione 2.1 (Divisore)**.** Sia V l'insieme delle valutazioni di un campo di numeri K. Un *divisore* $\mathfrak{M}$ di K è una funzione

$$\mathfrak{M} : V \to \mathbb{N}$$

tale che

- $\mathfrak{M}(v) = 0$ per tutte le valutazioni ν tranne un numero finito;
- $\mathfrak{M}(v) \in \{0, 1\}$ se v è archimedea e reale;
- $\mathfrak{M}(v) = 0$ se v è archimedea e complessa.

In maniera equivalente possiamo definire un divisore come un elemento del semigruppo libero generato dalle valutazioni di K con le relazioni $v^2 = 1$ se v è archimedea reale e $v = 1$ se v è archimedea complessa.

Spesso scriviamo

$$\mathfrak{M} = \prod_{v_\mathfrak{P} \in V} \mathfrak{P}^{\mathfrak{M}(v_\mathfrak{P})} = \mathfrak{M}_0 \mathfrak{M}_\infty,$$

dove $\mathfrak{M}_0$ indica un ideale di K, scritto come prodotto di potenze di ideali primi, e $\mathfrak{M}_\infty$ un prodotto formale libero da quadrati di valutazioni archimedee reali, eventualmente anche vuoto.

In modo analogo a quanto accade per gli ideali definiamo una relazione di divisibilità per i divisori: un divisore $\mathfrak{M}$ divide un divisore $\mathfrak{N}$ se $\mathfrak{M}(v) \leq \mathfrak{N}(v)$ per ogni valutazione v. Fissato un divisore $\mathfrak{M}$ diciamo inoltre che un elemento x di K^* è congruo a 1 modulo $\mathfrak{M}$ e scriviamo $x \equiv 1 \bmod \mathfrak{M}$ se $\mathrm{ord}_\mathfrak{P}(x-1) \geq \mathfrak{M}(v_\mathfrak{P})$ per tutti i primi $\mathfrak{P}$ che dividono $\mathfrak{M}_0$ e $x_\mathfrak{P} > 0$ per tutte le valutazioni reali che dividono $\mathfrak{M}_\infty$.

Indichiamo con $I^\mathfrak{M}$ il gruppo degli ideali frazionari relativamente primi con $\mathfrak{M}$ e con $P^{\mathfrak{M},1}$ il gruppo degli ideali frazionari principali che hanno un generatore $x \in K^*$ tale che $x \equiv 1 \bmod \mathfrak{M}$. Siamo ora in grado di definire il ray group group modulo $\mathfrak{M}$.

Definizione 2.2 (Ray class group)**.** Sia $\mathfrak{M}$ un divisore di un campo di numeri K. Chiamiamo *ray class group* modulo $\mathfrak{M}$ il quoziente $I^\mathfrak{M}/P^{\mathfrak{M},1}$.

Dalla precedente definizione, notando che $P^{1,1} = P$, segue immediatamente la seguente osservazione.

Osservazione 2.3. *Il ray class group modulo* 1 *di un campo di numeri K è il gruppo delle classi di ideali di K, cioè*

$$I^1/P^{1,1} = I/P = \mathrm{Cl}(K).$$

Teorema 2.4. *Sia $\mathfrak{M}$ un divisore di un campo di numeri K. Vale allora la successione esatta*

$$1 \to E/E^{\mathfrak{M},1} \to K^\mathfrak{M}/K^{\mathfrak{M},1} \to I^\mathfrak{M}/P^{\mathfrak{M},1} \to Cl(K) \to 1$$

e gli isomorfismi canonici

$$K^{\mathfrak{M}}/K^{\mathfrak{M},1} \cong \prod_{\mathfrak{p}|\mathfrak{M}_\infty} \{\pm\} \times \prod_{\mathfrak{p}|\mathfrak{M}_0} (\mathcal{O}_K/\mathfrak{p}^{\mathfrak{M}(\mathfrak{p})})^* \cong \prod_{\mathfrak{p}|\mathfrak{M}_infty} \{\pm\} \times (\mathcal{O}_K/\mathfrak{M}_0)^*,$$

dove

$$\begin{aligned} K^{\mathfrak{M}} &= \{x \in K | \operatorname{ord}_{\mathfrak{p}}(x) = 0 \ \forall \mathfrak{p} \mid \mathfrak{M}_0\}, \\ K^{\mathfrak{M},1} &= \{x \in K | \operatorname{ord}_{\mathfrak{p}}(x-1) \geq \mathfrak{M}(\mathfrak{p}) \ \forall \mathfrak{p} \mid \mathfrak{M}_0,\ x_{\mathfrak{p}} > 0 \ \forall \mathfrak{p} \mid \mathfrak{M}_\infty\}, \\ E^{\mathfrak{M},1} &= E \cap K^{\mathfrak{M},1}. \end{aligned}$$

Inoltre $I^{\mathfrak{M}}/P^{\mathfrak{M},1}$ è un gruppo finito di ordine

$$h_{\mathfrak{M}} = h \cdot (E : E^{\mathfrak{M},1})^{-1} \cdot 2^{r_0} \cdot \|\mathfrak{M}_0\| \cdot \prod_{\mathfrak{p}|\mathfrak{M}_0} \left(1 - \frac{1}{\|\mathfrak{p}\|}\right),$$

dove h è il numero delle classi di ideali di K, r_0 è il numero di primi reali che dividono $\mathfrak{M}$ e $\|\mathfrak{p}\|$ è uguale a $|\mathcal{O}_K/\mathfrak{p}|$.

2.2 Gruppi di decomposizione e di inerzia

Consideriamo ora un'estensione normale L/K di campi di numeri. Sia $\mathfrak{p}$ un ideale primo di K e $\mathfrak{P}$ un ideale primo di L sopra $\mathfrak{p}$. Richiamiamo i risultati principali relativi al gruppo di decomposizione e al gruppo di inerzia.

Definizione 2.5 (Gruppo di decomposizione)**.** Sia L/K un'estensione di campi di numeri e sia $\mathfrak{P}$ un ideale primo di L sopra l'ideale primo $\mathfrak{p}$ di K. Definiamo *gruppo di decomposizione* di $\mathfrak{P}$ e lo indichiamo con $D(\mathfrak{P}|\mathfrak{p})$ lo stabilizzatore di $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$, cioè

$$D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

È interessante notare che il gruppo di decomposizione di $\mathfrak{P}$ è strettamente legato all'estensione di campi locali $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.

Osservazione 2.6. *Il gruppo di decomposizione $D(\mathfrak{P}|\mathfrak{p}) \subseteq \mathrm{Gal}(L/K)$ è l'insieme degli elementi del gruppo di Galois che, agendo in modo continuo rispetto alla topologia $\mathfrak{P}$-adica, si estendono ad automorfismi del completamento $L_{\mathfrak{P}}$. Questo implica che*

$$D(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

Per ogni $\sigma \in \mathrm{Gal}(L/K)$ abbiamo che $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ e inoltre, se $\sigma \in D(\mathfrak{P}|\mathfrak{p})$, per definizione vale che $\sigma(\mathfrak{P}) = \mathfrak{P}$. Dunque $\sigma \in D(\mathfrak{P}|\mathfrak{p})$ induce un automorfismo $\overline{\sigma}$ di $\mathcal{O}_L/\mathfrak{P}$, dal momento che, se x e y sono elementi di $\mathcal{O}_L$,

$$x \equiv y \bmod \mathfrak{P} \quad \Longleftrightarrow \quad \sigma(x) \equiv \sigma(y) \bmod \mathfrak{P}.$$

Poiché σ fissa K, allora $\bar{\sigma}$ fissa $\mathcal{O}_K/\mathfrak{p}$ e pertanto si ottiene un omomorfismo

$$\psi : D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}[(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})]$$

che associa ad ogni σ l'automorfismo indotto $\bar{\sigma}$.

Definizione 2.7 (Gruppo di inerzia)**.** Sia L/K un'estensione di campi di numeri e sia $\mathfrak{P}$ un ideale primo di L sopra l'ideale primo $\mathfrak{p}$ di K. Definiamo *gruppo d'inerzia* di $\mathfrak{P}$ e lo indichiamo con $T(\mathfrak{P}|\mathfrak{p})$ il nucleo dell'omomorfismo ψ, cioè

$$T(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) \equiv x \bmod \mathfrak{P} \quad \forall x \in K^*\}.$$

Dal calcolo della cardinalità dei gruppi $D(\mathfrak{P}|\mathfrak{p})/T(\mathfrak{P}|\mathfrak{p})$ e $\mathrm{Gal}[(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})]$, che qui non riportiamo, otteniamo che i due gruppi hanno lo stesso numero di elementi e quindi l'omomorfismo ψ è surgettivo. Pertanto, detti l e k i campi residui $\mathcal{O}_L/\mathfrak{P}$ e $\mathcal{O}_K/\mathfrak{p}$, otteniamo la seguente successione esatta:

$$1 \to T(\mathfrak{P}|\mathfrak{p}) \to D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(l/k) \to 1. \tag{2.1}$$

2.3 Automorfismo di Frobenius

Ci restringiamo ora a lavorare con un'estensione di campi di numeri L/K in cui l'ideale primo $\mathfrak{P}$ di L è non ramificato sopra l'ideale primo $\mathfrak{p}$ di K. In questo caso possiamo identificare il gruppo di decomposizione di P con il gruppo di Galois dell'estensione dei campi residui, dato che vale il seguente lemma.

Lemma 2.8. *Sia L/K un'estensione di campi di numeri e sia $\mathfrak{P}$ un ideale primo di L non ramificato sopra l'ideale primo $\mathfrak{p}$ di K. Allora*

$$D(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}(l/k).$$

Dimostrazione. Poiché $\mathfrak{P}$ è non ramificato su $\mathfrak{p}$, il gruppo $T(\mathfrak{P}|\mathfrak{p})$ è il gruppo banale. La successione esatta 2.1 produce perciò l'isomorfismo che cerchiamo tra il gruppo di decomposizione $D(\mathfrak{P}|\mathfrak{p})$ e il gruppo di Galois $\mathrm{Gal}(l/k)$. □

Il campo finito l è un'estensione finita di k, perciò il gruppo $\mathrm{Gal}(l/k)$ è ciclico e ha un generatore canonico, il Frobenius φ, tale che per ogni $x \in l$ vale $\varphi(x) = x^q$, dove q è la cardinalità del campo k. Pertanto anche il gruppo di decomposizione $D(\mathfrak{P}|\mathfrak{p})$ è ciclico e possiamo quindi cercare in questo gruppo l'elemento che corrisponde, attraverso l'isomorfismo tra $D(\mathfrak{P}|\mathfrak{p})$ e $\mathrm{Gal}(l/k)$, al Frobenius.

Definizione 2.9 (Automorfismo di Frobenius)**.** Sia L/K un'estensione di campi di numeri e sia $\mathfrak{P}$ un ideale primo di L non ramificato sopra l'ideale primo $\mathfrak{p}$ di K. Chiamiamo *automorfismo di Frobenius* di $\mathfrak{P}$ relativo all'estensione L/K e lo indichiamo con $(\mathfrak{P}, L/K)$ l'automorfismo $\varphi \in D(\mathfrak{P}|\mathfrak{p})$ tale che

$$\varphi(x) \equiv x^{N\mathfrak{p}} \bmod \mathfrak{P}, \quad \forall x \in \mathcal{O}_L. \tag{2.2}$$

Un automorfismo σ di $\mathrm{Gal}(L/K)$ permuta i primi sopra un primo $\mathfrak{p}$. Perciò, se $\mathfrak{P}$ è un ideale primo sopra $\mathfrak{p}$, allora anche $\sigma\mathfrak{P}$ è un ideale primo sopra $\mathfrak{p}$ ed è quindi naturale domandarsi che relazione intercorre tra gli automorfismi $(\sigma\mathfrak{P}, L/K)$ e $(\mathfrak{P}, L/K)$.

Teorema 2.10. *Sia L/K un'estensione di campi di numeri e sia $\mathfrak{P}$ un ideale primo di L non ramificato sopra l'ideale primo $\mathfrak{p}$ di K. Per ogni $\sigma \in \mathrm{Gal}(L/K)$ abbiamo che*

$$(\sigma\mathfrak{P}, L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}.$$

Dimostrazione. Sia $x \in \mathcal{O}_L$. Allora

$$(\mathfrak{P}, L/K)\sigma^{-1}(x) \equiv (\sigma^{-1}(x))^{N\mathfrak{p}} \equiv \sigma^{-1}(x^{N\mathfrak{p}}) \bmod \mathfrak{P}.$$

Applicando σ ad entrambi i membri dell'ultima uguaglianza, ricaviamo che

$$\sigma(\mathfrak{P}, L/K)\sigma^{-1}(x) \equiv x^{N\mathfrak{p}} \bmod \sigma\mathfrak{P}$$

e quindi $\sigma(\mathfrak{P}, L/K)\sigma^{-1}$ soddisfa l'equazione che definisce $(\sigma\mathfrak{P}, L/K)$. Dato che l'automorfismo di Frobenius è unicamente determinato da quest'ultima equazione, segue la tesi. □

Dal teorema 1.29 sappiamo che il gruppo $Gal(L/K)$ agisce transitivamente sugli ideali primi sopra $\mathfrak{p}$ e dunque, fissato un ideale primo $\mathfrak{P}$ sopra $\mathfrak{p}$, ogni primo sopra $\mathfrak{p}$ è della forma $\sigma(\mathfrak{P})$ per qualche $\sigma \in \mathrm{Gal}(L/K)$. Possiamo pertanto dedurre, grazie al teorema 2.10, che la classe di coniugio dell'elemento $(\mathfrak{P}, L/K)$ è univocamente determinata dall'ideale primo $\mathfrak{p}$; indichiamo questa classe di coniugio con $(\mathfrak{p}, L/K)$.

Lemma 2.11. *Sia L/K un'estensione abeliana di campi di numeri e sia $\mathfrak{P}$ un ideale primo di L sopra l'ideale primo non ramificato $\mathfrak{p}$ di K. Allora l'automorfismo $(\mathfrak{P}, L/K)$ è determinato unicamente dal primo non ramificato $\mathfrak{p}$ ed inoltre abbiamo che*

$$(\mathfrak{P}, L/K)(x) \equiv x^{N\mathfrak{p}} \bmod \mathfrak{p}\mathcal{O}_L, \qquad \forall x \in \mathcal{O}_L. \tag{2.3}$$

Dimostrazione. Dal momento che $\mathrm{Gal}(L/K)$ è un gruppo abeliano, la classe di coniugio di $(\mathfrak{P}, L/K)$ è composta da un solo elemento e quindi $(\mathfrak{P}, L/K)$ è univocamente determinato dal primo $\mathfrak{p}$. L'equazione 2.3 deriva perciò dal fatto che $(\mathfrak{P}, L/K)$ soddisfa la stessa congruenza 2.2 per tutti i primi sopra $\mathfrak{p}$. □

Il lemma appena dimostrato ci permette di dare la prossima definizione.

Definizione 2.12 (Simbolo di Artin)**.** Sia L/K un'estensione abeliana di campi di numeri e sia $\mathfrak{p}$ un ideale primo di K che non ramifica in L. Chiamiamo *simbolo di Artin* l'elemento $(\mathfrak{P}, L/K)$ del gruppo di Galois $\mathrm{Gal}(L/K)$, dove $\mathfrak{P}$ è un qualunque ideale primo sopra $\mathfrak{p}$, e lo indichiamo con $(\mathfrak{p}, L/K)$.

2.4 Teoremi principali

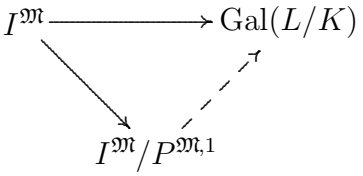
Restringiamoci a considerare un'estensione abeliana di campi di numeri L/K. Sia S un insieme di primi di K che contiene tutti i primi che ramificano in L e sia I_K^S il sottogruppo degli ideali frazionari di K generato dagli ideali primi che non appartengono a S.

Definizione 2.13 (Mappa di Artin)**.** Sia L/K un'estensione abeliana di campi di numeri. Chiamiamo *mappa di Artin* l'omomorfismo

$$(\cdot, L/K) : I_K^S \to \mathrm{Gal}(L/K), \quad \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r} \mapsto \prod_{i=1}^{r} (\mathfrak{p}_i, L/K)^{n_i},$$

ottenuto estendendo per moltiplicatività a I^S la funzione che associa a $\mathfrak{p}$ il simbolo di Artin $(\mathfrak{p}, L/K)$.

Sia S un insieme finito di ideali primi di K. Dato un divisore $\mathfrak{M}$ di K sia $S(\mathfrak{M})$ l'insieme degli ideali primi che dividono $\mathfrak{M}$. Diciamo che la mappa di Artin $(\cdot, L/K) : I^S \to \mathrm{Gal}(L/K)$ ammette un divisore $\mathfrak{M}$ se esiste un divisore $\mathfrak{M}$, con $S(\mathfrak{M}) \subseteq S$, tale che $P^{\mathfrak{M},1} \subseteq \mathrm{Ker}(\cdot, L/K)$, cioè se la mappa di Artin si fattorizza attraverso il ray class group $I^{\mathfrak{M}}/P^{\mathfrak{M},1}$ per qualche divisore $\mathfrak{M}$ tale che $S(\mathfrak{M}) \subseteq S$ e vale quindi il seguente diagramma commutativo:



Teorema 2.14 (Legge di reciprocità)**.** *Sia L un'estensione abeliana finita di un campo di numeri K e sia S l'insieme degli ideali primi di K che ramificano in L. Allora la mappa di Artin $(\cdot, L/K) : I_K^S \to \mathrm{Gal}(L/K)$ ammette un divisore $\mathfrak{M}$ con $S(\mathfrak{M}) = S$ ed induce un isomorfismo*

$$I_K^{\mathfrak{M}}/P^{\mathfrak{M},1} \cdot N_{L/K} I_L^{\mathfrak{M}} \cong \mathrm{Gal}(L/K).$$

Possiamo finalmente dare due definizioni che sono centrali nello studio delle estensioni abeliane di un campo di numeri.

Definizione 2.15 (Divisore di definizione)**.** Sia L un'estensione abeliana finita di un campo di numeri K. Chiamiamo *divisore di definizione* di L un divisore $\mathfrak{M}$ di K che soddisfa la legge di reciprocità (teorema 2.14).

Definizione 2.16 (Sottogruppo di congruenza)**.** Sia $\mathfrak{M}$ un divisore di un campo di numeri K e sia L un'estensione abeliana finita di K. Diciamo che un sottogruppo H di $I_K^{\mathfrak{M}}$ è un *sottogruppo di congruenza* modulo $\mathfrak{M}$ se $P^{\mathfrak{M},1} \subseteq H \subseteq I^{\mathfrak{M}}$.

Teorema 2.17 (Teorema di esistenza)**.** *Sia $\mathfrak{M}$ un divisore di un campo di numeri K e sia H un sottogruppo di congruenza modulo $\mathfrak{M}$. Esiste allora un'unica estensione abeliana L/K, detta class field di H, ramificata solo sui primi che dividono $\mathfrak{M}$, tale che*

$$H = P^{\mathfrak{M},1} \cdot N_{L/K} I_L^{\mathfrak{M}}.$$

Inoltre la mappa di Artin $(\cdot, L/K)$ induce un isomorfismo

$$I^{\mathfrak{M}}/H \cong \mathrm{Gal}(L/K).$$

Se nel teorema di esistenza (teorema 2.17) poniamo il sottogruppo di congruenza modulo $\mathfrak{M}$ uguale a $P^{\mathfrak{M},1}$, troviamo un campo particolarmente importante.

Definizione 2.18 (Ray class field)**.** Sia $\mathfrak{M}$ un divisore di un campo di numeri K. Chiamiamo *ray class field* modulo $\mathfrak{M}$ l'estensione abeliana $L_{\mathfrak{M}}$ di K tale che la mappa di Artin definisce un isomorfismo

$$I^{\mathfrak{M}}/P^{\mathfrak{M},1} \cong \mathrm{Gal}(L/K).$$

Corollario 2.19. *Sia $\mathfrak{M}$ un divisore di un campo di numeri K. Allora la mappa $L \mapsto H^{\mathfrak{M}}$, dove $H_L^{\mathfrak{M}} = P^{\mathfrak{M},1} \cdot N_{L/K} I_L^{\mathfrak{M}}$, definisce una corrispondenza biunivoca tra le sottoestensioni del ray class field $L_{\mathfrak{M}}$ modulo $\mathfrak{M}$ e i sottogruppi di congruenza modulo $\mathfrak{M}$. In particolare, se L_1 e L_2 sono due sottoestensioni di $L_{\mathfrak{M}}$ e H_1 e H_2 i rispettivi sottogruppi di congruenza modulo $\mathfrak{M}$, valgono le seguenti proprietà:*

- $H_1 \subseteq H_2 \iff L_1 \supseteq L_2$*;*
- $L_1 L_2$ *corrisponde a* $H_1 \cap H_2$*;*
- $L_1 \cap L_2$ *corrisponde a* $H_1 H_2$*;*
- *se* $L_1 \subseteq L_2$*, allora* $\mathrm{Gal}(L_2/L_1) \cong H_1/H_2$*.*

Data un'estensione abeliana finita L/K, per la legge di reciprocità (teorema 2.14) sappiamo che esiste un divisore $\mathfrak{M} = \mathfrak{M}_\infty \mathfrak{M}_0$, divisibile per tutti i primi di K che ramificano in L, tale che la mappa di Artin ammette $\mathfrak{M}$ come divisore, cioè tale che $P^{\mathfrak{M},1} \subseteq \mathrm{Ker}(\cdot, L/K)$. Consideriamo la successione

$$(\mathcal{O}_K/\mathfrak{p}^{\mathfrak{M}(\mathfrak{p})})^* \hookrightarrow K^{\mathfrak{M}}/K^{\mathfrak{M},1} \xrightarrow{i} I^{\mathfrak{M}}/P^{\mathfrak{M},1} \xrightarrow{(\cdot,L/K)} \mathrm{Gal}(L/K). \tag{2.4}$$

Per ogni primo $\mathfrak{p}$ di K esiste chiaramente il minimo intero $f(\mathfrak{p}) \leq \mathfrak{M}(\mathfrak{p})$ tale che la composizione delle mappe si fattorizzi attraverso $(\mathcal{O}_K/\mathfrak{p}^{f(\mathfrak{p})})^*$. Questo implica che la mappa di Artin si fattorizza attraverso il ray class group $I^{\mathfrak{M}}/P^{\mathfrak{M},1}$, dove $\mathfrak{M} = \mathfrak{M}_\infty \prod \mathfrak{p}^{f(\mathfrak{p})}$.

Definizione 2.20 (Conduttore)**.** Sia L un'estensione abeliana finita di un campo di numeri K. Chiamiamo *conduttore* dell'estensione L/K e lo indichiamo con $\mathfrak{f}(L/K)$ il minimo divisore di K tale che la mappa di Artin $(\cdot, L/K)$ si fattorizza attraverso il ray class group $I^{\mathfrak{M}}/P^{\mathfrak{M},1}$.

2.5 Fattorizzazione degli ideali

In questa sezione ci occupiamo della fattorizzazione degli ideali di un campo di numeri K in un'estensione abeliana finita L. Per la legge di reciprocità (teorema 2.14) L ammette un divisore di definizione $\mathfrak{M}$ e dalla corrispondenza del corollario 2.19 al campo L è associato un sottogruppo $H_L^{\mathfrak{M}}$ del gruppo I_K. La struttura della fattorizzazione in L di un ideale primo $\mathfrak{p}$ di K non ramificato in L è particolarmente semplice ed è un tipico risultato di class field theory, dal momento che collega queste informazioni con questioni relative al gruppo degli ideali.

Teorema 2.21 (Legge di decomposizione)**.** *Sia L/K un'estensione abeliana finita di campi di numeri di grado n e sia $\mathfrak{p}$ un ideale primo di K che non si ramifica in L. Siano inoltre $\mathfrak{M}$ un divisore di definizione di L non divisibile per $\mathfrak{p}$ e $H_L^{\mathfrak{M}}$ il sottogruppo di congruenza modulo $\mathfrak{M}$ associato a L. Se f è l'ordine di $\mathfrak{p}$ mod $H_L^{\mathfrak{M}}$ nel gruppo $I^{\mathfrak{M}}/H_L^{\mathfrak{M}}$, cioè il minimo numero naturale tale che $\mathfrak{p}^f \in H_L^{\mathfrak{M}}$, allora $\mathfrak{p}$ si spezza in L in un prodotto*

$$\mathfrak{p} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r$$

di $r = n/f$ ideali primi distinti $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, aventi tutti lo stesso grado di inezia f su $\mathfrak{p}$.

Dimostrazione. Sia $\mathfrak{p} = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r$ la fattorizzazione in ideali primi di $\mathfrak{p}$ in L. Dal momento che l'estensione L/K è di Galois e $\mathfrak{p}$ è non ramificato, gli ideali primi $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ sono tutti distinti e hanno lo stesso grado di inerzia $f(\mathfrak{P}|\mathfrak{p})$. Per la legge di reciprocità (teorema 2.14) sappiamo che $I^{\mathfrak{M}}/H_L^{\mathfrak{M}} \cong \mathrm{Gal}(L/K)$ e quindi

l'ordine di $\mathfrak{p}$ mod $H_L^{\mathfrak{M}}$ nel gruppo $I^{\mathfrak{M}}/H_L^{\mathfrak{M}}$ è uguale all'ordine dell'automorfismo di Frobenius $(\mathfrak{p}, L/K)$. Quest'ordine, dato che $\mathfrak{p}$ è non ramificato in L, è uguale alla cardinalità del gruppo di decomposizione $D(\mathfrak{P}_i|\mathfrak{p})$, che è proprio il grado di inerzia $f(\mathfrak{P}_i|\mathfrak{p})$. □

Il teorema appena dimostrato ci permette di fare la seguente osservazione.

Osservazione 2.22. *Gli ideali primi di un campo di numeri K che si spezzano completamente in un'estensione abeliana finita L con divisore di definizione $\mathfrak{M}$ sono precisamente gli ideali primi contenuti nel sottogruppo di congruenza $H_L^{\mathfrak{M}}$.*

2.6 Hilbert class field

Una delle più studiate estensioni abeliane di campi di numeri è l'Hilbert class field.

Definizione 2.23 (Hilbert class field)**.** Sia K un campo di numeri. Definiamo *Hilbert class field* di K il ray class field modulo 1 di K e lo indichiamo con K^1.

Nell'osservazione 2.3 abbiamo notato che il ray class group modulo 1 è il gruppo delle classi di ideali; pertanto, se nel teorema di esistenza (teorema 2.17) poniamo $\mathfrak{M} = 1$ e $H = P$, otteniamo l'Hilbert class field K^1 di K. Lo stesso teorema ci dice che K^1 è un'estensione abeliana non ramificata e che $\mathrm{Gal}(K^1/K) \cong I/P$. Dal momento che ogni estensione abeliana non ramificata ha conduttore $\mathfrak{f} = 1$, il corollario 2.19 implica che ogni estensione abeliana non ramificata è contenuta nell'Hilbert class field. Abbiamo perciò dimostrato il seguente teorema.

Teorema 2.24. *Sia K un campo di numeri. La massima estensione abeliana non ramificata di K è l'Hilbert class field K^1 di K e la mappa di Artin induce un isomorfismo*

$$\mathrm{Gal}(K^1/K) \cong \mathrm{Cl}(K).$$

Se ora consideriamo l'Hilbert class field K^1 di un campo di numeri K e ricordiamo che il suo sottogruppo di congruenza modulo 1 è P, dall'osservazione 2.22 otteniamo un interessante corollario.

Corollario 2.25. *Gli ideali primi di K che si spezzano completamente nell'Hilbert class field K^1 sono precisamente tutti gli ideali primi principali.*

L'Hilbert class field ha anche un'altra notevole proprietà, congetturata da Hilbert intorno al 1900.

Teorema 2.26 (Teorema dell'ideale principale)**.** *Sia K un campo di numeri. Ogni ideale I di K diventa principale nell'Hilbert class field K^1 di K.*

Non riportiamo qui l'intera dimostrazione di questo teorema, ne presentiamo però le idee fondamentali.

Dato un gruppo G indichiamo con G' il sottogruppo dei commutatori di G. Poniamo inoltre $G^{ab} = G/G'$ il massimo quoziente abeliano di G. Se H è un sottogruppo di G, esiste allora un'importante mappa da G^{ab} a H^{ab}.

Definizione 2.27 (Verlagerung)**.** Siano G un gruppo e H un sottogruppo di G di indice finito. Chiamiamo *Verlagerung* (*transfer*) l'omomorfismo canonico

$$\mathrm{Ver} : G/G' \to H/H',$$

definito nel seguente modo. Sia $R = \{r_1, \ldots, r_n\}$ un insieme di rappresentanti per le classi laterali sinistre di H in G; quindi

$$G = r_1 H \cup \ldots \cup r_n H.$$

Dato $g \in G$, per ogni $r \in R$ troviamo $g_r \in G$ e $r' \in R$ tali che $gr = r' g_r$. Allora

$$\mathrm{Ver}(g \bmod G') = \prod_{r \in R} g_r \bmod H'.$$

Questa definizione è indipendente dalla scelta del sistema di rappresentanti per le classi laterali sinistre di H in G.

Sia L/K un'estensione finita di Galois non necessariamente abeliana e sia K' un campo intermedio. Dato S un insieme finito di primi di K, l'estensione $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{K'}$, dove $\mathfrak{a}$ è un ideale di K, genera un omomorfismo $I_K^S \to I_{K'}^S$.

Proposizione 2.28. *Siano $K \subseteq K' \subseteq L$ campi di numeri con L/K estensione di Galois. Vale allora il seguente diagramma commutativo:*

$$\begin{array}{ccc} I_K^S & \xrightarrow{(\cdot, L/K)} & \mathrm{Gal}(L/K)^{ab} \\ \downarrow & & \downarrow \mathrm{Ver} \\ I_{K'}^S & \xrightarrow{(\cdot, L/K')} & \mathrm{Gal}(L/K')^{ab} \end{array}$$

Proposizione 2.29. *Sia K^1 l'Hilbert class field di K e K^2 l'Hilbert class field di K^1. Allora K^2 è un'estensione normale di K, K^1 è la massima estensione abeliana di K contenuta in K^2 e quindi*

$$\mathrm{Gal}(K^2/K)^{ab} \cong \mathrm{Gal}(K^1/K).$$

Dimostrazione. Ogni coniugato di K^2 su K è un'estensione abeliana non ramificata di K^1 e perciò contenuta in K^2; questo implica che K^2 è un'estensione normale di K. K^1 è invece la massima estensione abeliana di K contenuta in K^2 poiché ogni estensione abeliana di K contenuta in K^2 è non ramificata su K ed è dunque contenuta in K^1. □

Applicando la proposizione 2.28 con $S = \{\}$, $K = K$, $K' = K^1$ e $L = K^2$ e ricordando che, per la proposizione 2.29, $\mathrm{Gal}(K^2/K)^{ab} \cong \mathrm{Gal}(K^1/K)$, otteniamo il seguente diagramma commutativo:

$$\begin{array}{ccc} \mathrm{Cl}(K) \cong \mathrm{Gal}(K^1/K) \\ \Big\downarrow \qquad\qquad \Big\downarrow \mathrm{Ver} \\ \mathrm{Cl}(K^1) \cong \mathrm{Gal}(K^2/K^1) \end{array}$$

Per dimostrare il teorema dell'ideale principale (teorema 2.26) è quindi sufficiente mostrare che l'omomorfismo Verlagerung

$$\mathrm{Ver} : \mathrm{Gal}(K^1/K) \to \mathrm{Gal}(K^2/K^1)$$

è l'omomorfismo banale. Notiamo che se poniamo $G = \mathrm{Gal}(K^2/K)$, allora per la proposizione 2.29 $\mathrm{Gal}(K^1/K) = G/G'$ e $\mathrm{Gal}(K^2/K^1) = G'$. Il seguente teorema, congetturato da Emil Artin e dimostrato da Furtwängler nel 1930, mostra che il risultato riguarda esclusivamente questioni di teoria dei gruppi.

Teorema 2.30. *Sia G un gruppo finitamente generato, tale che il suo sottogruppo dei commutatori G' sia di indice finito. Allora l'omomorfismo*

$$\mathrm{Ver} : G/G' \to G'/G''$$

è l'omomorfismo banale.

Non riportiamo qui la dimostrazione del teorema, che può essere facilmente trovata in [22], dove viene proposta una dimostrazione di Witt più semplice di quella originale di Furtwängler.

2.7 Hilbert p-class field

Quando si lavora con un gruppo, spesso è conveniente studiare i suoi sottogruppi di Sylow. Nel caso del gruppo delle classi di ideali $\mathrm{Cl}(K)$ di un campo di numeri K indichiamo con $\mathrm{Cl}_p(K)$ il suo p-sottogruppo di Sylow.

Definizione 2.31 (p-estensione)**.** Sia K/F un'estensione di campi di numeri. Diciamo che K è una *p-estensione* di F se K/F è un'estensione normale e il gruppo di Galois $\mathrm{Gal}(K/F)$ è un p-gruppo.

Definizione 2.32 (Hilbert p-class field)**.** Sia K un campo di numeri. Chiamiamo *Hilbert p-class field* di K la massima p-estensione abeliana non ramificata di K e la indichiamo con $K^1_{(p)}$.

Per definizione l'Hilbert p-class field è contenuto nell'Hilbert class field, inoltre, per il teorema 2.24 di class field theory, abbiamo che

$$\mathrm{Gal}(K^1_{(p)}/K) \cong \mathrm{Cl}_p(K).$$

Definizione 2.33 (Hilbert p-class field tower)**.** Sia K un campo di numeri. Fissato un numero primo p, poniamo $K^0_{(p)} = K$ e indichiamo con $K^i_{(p)}$ l'Hilbert p-class field of $K^{i-1}_{(p)}$, dove $i \geq 1$. Abbiamo allora la successione di campi

$$K = K^0_{(p)} \subseteq K^1_{(p)} \subseteq \ldots \subseteq K^\infty_{(p)} = \bigcup_{i=0}^{\infty} K^i_{(p)},$$

che chiamiamo *Hilbert p-class field tower* di K.

La successione dei campi $K^i_{(p)}$ che definisce l'Hilbert p-class field tower può stabilizzarsi. Diciamo che l'Hilbert p-class field tower è finita se $K^\infty_{(p)}$ è un'estensione finita di K ed infinita altrimenti. Nel primo caso definiamo lunghezza dell'Hilbert p-class field tower il più piccolo intero non negativo i tale che $K^i_{(p)} = K^{i+1}_{(p)}$ e la indichiamo con il simbolo $L_p(K)$.

Capitolo 3

Campi ciclotomici

Siano n un intero positivo e ζ_n una radice n-esima primitiva dell'unità. Il campo di numeri $\mathbb{Q}(\zeta_n)$ è detto n-esimo campo ciclotomico.

In questo capitolo riportiamo alcuni risultati generali riguardanti i campi ciclotomici, che utilizziamo poi nel caso particolare del campo $K = \mathbb{Q}(\zeta_{29})$ per costruirne esplicitamente l'Hilbert class field K^1. Di quest'ultimo campo calcoliamo inoltre il gruppo di Galois $\mathrm{Gal}(K^1/\mathbb{Q})$.

Le dimostrazioni dei risultati delle prime sezioni possono essere trovate nel libro di Marcus [20] o in quello di Washington [29].

3.1 Risultati di base

Il primo risultato riguarda il polinomio minimo di ζ_n su $\mathbb{Q}$.

Teorema 3.1. *Sia ζ_n una radice n-esima primitiva dell'unità. Le radici dell'unità ζ_n^k, con $1 \leq k \leq n$ e $(k, n) = 1$, sono anch'esse radici n-esime primitive dell'unità e sono coniugate a ζ_n.*

Dal teorema 3.1 ricaviamo immediatamente i seguenti due corollari.

Corollario 3.2. *Il grado dell'estensione $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ è $\phi(n)$.*

Corollario 3.3. *Il gruppo di Galois di $\mathbb{Q}(\zeta_n)$ su $\mathbb{Q}$ è isomorfo al gruppo moltiplicativo degli interi modulo n. L'isomorfismo*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

associa ad ogni $k \mod n$ l'automorfismo $\zeta_n \mapsto \zeta_n^k$.

Sappiamo dal teorema 1.5 che per ogni campo di numeri K l'anello degli interi $\mathcal{O}_K$ di K è un gruppo libero abeliano di ordine n, cioè $\mathcal{O}_K \cong \mathbb{Z}^n$. Nel caso dei campi ciclotomici è però possibile migliorare questo risultato: l'anello degli interi è infatti monogenico.

Teorema 3.4. *L'anello degli interi algebrici $\mathcal{O}_n$ di $\mathbb{Q}(\zeta_n)$ è $\mathbb{Z}[\zeta_n]$.*

Dal precedente teorema 3.4 sappiamo quindi che una base di $\mathcal{O}_n$ su $\mathbb{Z}$ è data dalle potenze $1, \zeta_n, \ldots, \zeta_n^{\phi(n)-1}$. Abbiamo quindi un modo particolamente semplice per rappresentare gli interi di un campo ciclotomico.

Per quanto riguarda invece la struttura della fattorizzazione dei primi di $\mathbb{Q}$ in $\mathbb{Q}(\zeta_n)$ possiamo osservare che, per i primi p tali che $p \nmid n$, questa dipende soltanto dalla congruenza $p \mod n$.

Teorema 3.5. *Sia p un primo tale che $p \nmid n$ e sia f l'ordine moltiplicativo di $p \mod n$. Il primo p si spezza allora in $\mathbb{Q}(\zeta_n)$ nel prodotto di $\phi(n)/f$ ideali primi distinti, ciascuno di inerzia f.*

Per i primi p che dividono m vale invece il seguente teorema.

Teorema 3.6. *Sia p un primo tale che $p \mid n$, dove $n = p^k m$ e $(m, p) = 1$. Allora ogni ideale primo sopra p compare nella fattorizzazione di p con indice di ramificazione $e = \phi(p^k)$ e con grado di inerzia f uguale all'ordine moltiplicativo di p modulo m.*

3.2 Campi CM

Un tipo speciale di campi di numeri sono i campi CM, dei quali i campi ciclotomici sono un caso particolare.

Definizione 3.7 (Campo totalmente reale e campo totalmente immaginario)**.** Un campo di numeri è un *campo totalmente reale* se tutte le sue immersioni in $\mathbb{C}$ sono contenute in $\mathbb{R}$, mentre è un *campo totalmente immaginario* se non esiste alcuna sua immersione in $\mathbb{C}$ che sia contenuta in $\mathbb{R}$.

Definizione 3.8 (Campo CM)**.** Un campo di numeri è un *campo* CM se è un'estensione quadratica totalmente immaginaria di un campo di numeri totalmente reale.

Per poter dimostrare alcune proprietà dei campi CM è utile ricordare un'importante proposizione sul numero delle classi.

Proposizione 3.9. *Sia L/K un'estensione di campi di numeri tale che non esiste alcuna sottoestensione abeliana non ramificata su K. Allora il numero delle classi h_K di K divide il numero delle classi h_L di L.*

Dimostrazione. Sia K^1 l'Hilbert class field di K. Dal teorema 2.24 abbiamo che

$$\mathrm{Gal}(K^1/K) \cong \mathrm{Cl}(K).$$

Poiché K^1 è abeliana e non ramificata su K, dalle ipotesi otteniamo che $K^1 \cap L = K$ e quindi $[LK^1 : L] = [K^1 : K]$. L'estensione LK^1/L è non ramificata e abeliana e dunque è contenuta nell'Hilbert class field L^1 di L. Troviamo pertanto che $h_K = [LK^1 : L]$ divide $h_L = [L^1 : L]$. □

Un'estensione di campi di numeri totalmente ramificata su un primo è un caso particolare di estensione che soddisfa le ipotesi della proposizione 3.9 e dunque vale la prossima osservazione.

Osservazione 3.10. *Se L/K è un'estensione di campi di numeri totalmente ramificata su un primo, allora h_K divide h_L.*

Dalla precedente osservazione, notando che un campo CM è un'estensione totalmente ramificata all'infinito del proprio sottocampo reale massimale, ricaviamo il seguente risultato sul numero delle classi dei campi CM.

Teorema 3.11. *Sia K un campo* CM *e sia K^+ il suo massimo sottocampo reale. Se indichiamo con h e h^+ i numeri delle classi rispettivamente di K e di K^+, allora h^+ divide h.*

Definizione 3.12 (Numero delle classi relativo)**.** Chiamiamo *numero delle classi relativo* il quoziente $h^- = h/h^+$.

Per i campi ciclotomici vale un risultato ancora più forte.

Teorema 3.13. *Siano* $\mathrm{Cl}(\mathbb{Q}(\zeta_n))$ *e* $\mathrm{Cl}(\mathbb{Q}(\zeta_n)^+)$ *i gruppi delle classi di ideali rispettivamente di $\mathbb{Q}(\zeta_n)$ e del suo sottocampo reale $\mathbb{Q}(\zeta_n)^+$. Allora la mappa naturale di estensione* $\mathrm{Cl}(\mathbb{Q}(\zeta_n)^+) \to \mathrm{Cl}(\mathbb{Q}(\zeta_n))$ *è iniettiva.*

Per quanto riguarda le unità vale il seguente teorema.

Teorema 3.14. *Siano K un campo* CM*, K^+ il massimo sottocampo reale di K ed E e E^+ i rispettivi gruppi delle unità. Sia inoltre Ω_K il gruppo delle radici dell'unità contenute in K. Allora $E : \Omega_K E^+$ è uguale ad* 1 *o a* 2*.*

Corollario 3.15. *Sia $K = \mathbb{Q}(\zeta_n)$. Allora $E : \Omega_K E^+$ è uguale ad* 1 *se n è la potenza di numero primo, mentre $E : \Omega_K E^+$ è uguale ad* 2 *se n non è potenza di un primo.*

3.3 Gruppo delle unità

La struttura del gruppo delle unità di campo di numeri è ben nota grazie al teorema di Dirichlet.

Teorema 3.16 (Dirichlet)**.** *Sia E_K il gruppo delle unità dell'anello degli interi $\mathcal{O}_K$ di un campo di numeri K e siano r e $2s$ i numeri rispettivamente delle immersioni reali e delle immersioni complesse di K in $\mathbb{C}$. Allora E_K è il prodotto diretto $\Omega_K \times V$, dove Ω_K è il gruppo ciclico finito delle radici dell'unità contenute in K e V è un gruppo libero abeliano di rango $r + s - 1$.*

Il teorema di Dirichlet non ci fornisce però esplicitamente dei generatori del gruppo delle unità di un campo di numeri. Per questo motivo è particolarmente utile conoscere un sottogruppo di indice finito nel gruppo delle unità del quale siano noti con precisione i generatori; nel caso dei campi ciclotomici e delle loro massime sottoestensioni reali un gruppo di questo tipo è il gruppo delle unità ciclotomiche.

Definizione 3.17 (Unità ciclotomiche)**.** Sia $n \neq 2 \mod 4$ e sia E_n il gruppo delle unità di $\mathbb{Q}(\zeta_n)$. Indichiamo inoltre con V_n il gruppo moltiplicativo generato da $\{\pm\zeta_n, 1 - \zeta_n^a | 1 < a < n\}$. Definiamo gruppo delle *unità ciclotomiche* di $\mathbb{Q}(\zeta_n)$ il gruppo moltiplicativo $C_n = V_n \cap E_n$, mentre chiamiamo gruppo delle *unità ciclotomiche* di $\mathbb{Q}(\zeta_n)^+$ il gruppo moltiplicativo $C_n^+ = E_n^+ \cap C_n$.

Il prossimo lemma esplicita i generatori del gruppo delle unità ciclotomiche.

Lemma 3.18. *Siano p un primo e m un intero positivo. Valgono le seguenti due affermazioni:*

(a) il gruppo $C_{p^m}^+$ delle unità ciclotomiche di $\mathbb{Q}(\zeta_{p^m})^+$ è generato da -1 e dalle unità

$$\xi_a = \zeta_{p^m}^{\frac{1-a}{2}} \frac{1 - \zeta_{p^m}^a}{1 - \zeta_{p^m}}, \quad 1 < a < \frac{p^m}{2}, (a, p) = 1;$$

(b) il gruppo C_{p^m} delle unità ciclotomiche di $\mathbb{Q}(\zeta_n)$ è generato da ζ_{p^m} e da $C_{p^m}^+$.

Come abbiamo anticipato sopra, il gruppo delle unità ciclotomiche è di indice finito nel gruppo delle unità.

Teorema 3.19. *Siano p un primo e m un intero positivo. Il gruppo $C_{p^m}^+$ delle unità ciclotomiche di $\mathbb{Q}(\zeta_{p^m})^+$ è di indice finito nel gruppo delle unità $E_{p^m}^+$ e, se $h_{p^m}^+$ è il numero delle classi di $\mathbb{Q}(\zeta_{p^m})^+$, vale inoltre la relazione*

$$h_{p^m}^+ = [E_{p^m}^+ : C_{p^m}^+].$$

Utilizzando quanto ricordato finora sul gruppo delle unità di un campo ciclotomico e i risultati di van der Linden [28] sul numero delle classi h^+ della massima estensione reale di un campo ciclotomico, siamo in grado di esibire un sistema completo di generatori del gruppo delle unità del campo $\mathbb{Q}(\zeta_{29})$.

Teorema 3.20. *Un sistema di generatori per E_{29} è costituito dagli elementi $-\zeta_{29}, \eta_1, \ldots, \eta_{13}$, dove $\eta_j = \frac{1-\zeta_{29}^j}{1-\zeta_{29}}$.*

Dimostrazione. Dato che $h_n^+ = 1$ per $n \leq 70$ [28], allora $E_{29}^+ = C_{29}^+$ e quindi, per il corollario 3.15, $E_{29} = \Omega_{29} C_{29}^+$. Grazie al lemma 3.18 ricaviamo la tesi. □

3.4 Gruppo delle classi di ideali

Il gruppo delle classi di ideali $\mathrm{Cl}(\mathbb{Q}(\zeta_n))$, per il teorema 3.13, si divide naturalmente in due parti, che danno luogo alla successione esatta

$$0 \to \mathrm{Cl}(\mathbb{Q}(\zeta_n))^+ \to \mathrm{Cl}(\mathbb{Q}(\zeta_n)) \to \mathrm{Cl}(\mathbb{Q}(\zeta_n))^- \to 0.$$

Non si conosce molto sui gruppi $\mathrm{Cl}(\mathbb{Q}(\zeta_n))^+$, visto che già soltanto i numeri delle classi h_n^+ dei campi reali ciclotomici $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ sono difficili da calcolare, ma per $n \leq 70$ sono sicuramente banali [28]. Invece per h_n^- esiste una formula esplicita, facilmente calcolabile, già usata da Kummer verso la metà del 1800 per ricavarne i valori con $n < 100$ primo.

Chiaramente, se h_n^- è libero da quadrati, allora $\mathrm{Cl}(\mathbb{Q}(\zeta_n))^-$ è ciclico, ma in generale non è possibile individuare esattamente il gruppo $\mathrm{Cl}(\mathbb{Q}(\zeta_n))^-$ conoscendo esclusivamente h_n^-. Sorge quindi naturalmente il problema di determinare la struttura del gruppo $\mathrm{Cl}(\mathbb{Q}(\zeta_n))^-$.

Nell'articolo [18] del 1853 Kummer risolve il caso $n = 29$, trovando che il gruppo $\mathrm{Cl}(\mathbb{Q}(\zeta_{29}))$ è abeliano di tipo $(2, 2, 2)$, mentre nel 1870 dimostra che $\mathrm{Cl}(\mathbb{Q}(\zeta_{31}))^-$ è ciclico [17]. Successivamente il problema è stato affrontato da Iwasawa, che in [14] giustifica rigorosamente il risultato di Kummer secondo il quale $\mathrm{Cl}(\mathbb{Q}(\zeta_n))^-$ è un gruppo ciclico per $n < 100$ primo e $n \neq 29,\ 41$. Gerth dimostra in [7] che $\mathrm{Cl}(\mathbb{Q}(\zeta_{68}))$ è ciclico di ordine 8, mentre in [27] Tateyama determina, salvo alcune eccezioni, la struttura del gruppo $\mathrm{Cl}(\mathbb{Q}(\zeta_n))$ per $h_n < 10^4$. Infine Horie in [10] ha fornito un elenco completo di tutti i gruppi $\mathrm{Cl}(\mathbb{Q}(\zeta_n))$ che sono 2-gruppi.

Torniamo ad occuparci del campo $\mathbb{Q}(\zeta_{29})$ e vediamo come è possibile individuare la struttura del gruppo delle classi di $\mathbb{Q}(\zeta_{29})$, sapendo che $h_{29} = 8$.

Teorema 3.21. *Il gruppo delle classi di ideali di $\mathbb{Q}(\zeta_{29})$ è un 2-gruppo abeliano elementare di ordine 8, cioè*

$$\mathrm{Cl}(\mathbb{Q}(\zeta_{29})) \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

Dimostrazione. Dalla corrispondenza di Galois sappiamo che esiste un'unica sottoestensione di $\mathbb{Q}(\zeta_{29})$ di grado 4 su $\mathbb{Q}$. Chiamiamo L_4 questa estensione e sia σ un generatore di $\mathrm{Gal}(\mathbb{Q}(\zeta_{29})/L_4)$, che è un gruppo ciclico di ordine 7. Possiamo

agevolmente dimostrare che il campo L_4 è a fattorizzatione unica, ad esempio applicando il teorema 13 in [9] all'estensione di campi $L_4/\mathbb{Q}(\sqrt{29})$ oppure verificando esplicitamente che sono principali tutti gli ideali di norma minore o uguale al limite di Minkowski, che in questo vale circa $23,7$.

Poniamo ora

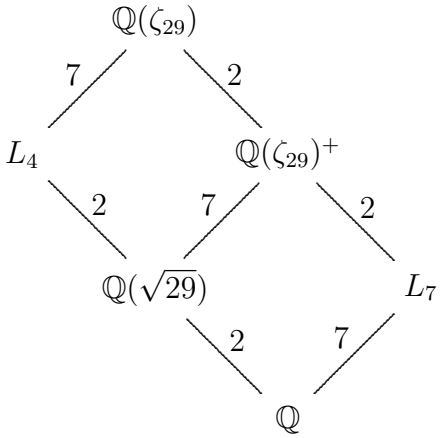
$$B_K = \{I \in \mathrm{Cl}(K) | I^2 = 1\},$$
$$A_K = \{I \in B_K | I^\sigma = I\}.$$

Dal momento che, se $I \in A_K$, allora

$$I = I^7 = I^{1+\sigma+\sigma^2+\sigma^3+\sigma^4+\sigma^5+\sigma^6} = 1,$$

ricaviamo che $|A_K| = 1$. D'altra parte $|B_K| \neq 1$, poiché $|\mathrm{Cl}(K)| = 8$. Pertanto σ è un'automorfismo di B_K di grado 7 e quindi $|B_K| = |\mathrm{Cl}(K)| = 8$. □

Prima di cercare dei generatori espliciti del gruppo delle classi di ideali di $\mathbb{Q}(\zeta_{29})$, riportiamo il diagramma delle sottoestensioni di $\mathbb{Q}(\zeta_{29})$ ottenuto grazie alla corrispondenza di Galois.



Il problema di trovare dei generatori espliciti del gruppo delle classi di ideali è essenzialmente di tipo computazionale. D'altra parte se consideriamo un ideale primo $\mathfrak{P}$ di $\mathbb{Q}(\zeta_{29})$ sopra un primo p di $\mathbb{Q}$ che non si spezza completamente in $\mathbb{Q}(\zeta_{29})$, allora il suo campo di decomposizione è un sottocampo proprio di $\mathbb{Q}(\zeta_{29})$. Questo sottocampo è a fattorizzazione unica poiché abbiamo visto che lo sono sia L_4 sia $\mathbb{Q}(\zeta_{29})^+$ e inoltre ogni loro sottoestensione lo è, dal momento che possiamo applicare l'osservazione 3.10 in quanto 29 è totalmente ramificato in $\mathbb{Q}(\zeta_{29})$. Tutto ciò implica che $\mathfrak{P}$ è principale e dunque i generatori di $\mathrm{Cl}(\mathbb{Q}(\zeta_{29}))$ vanno cercati tra gli ideali che stanno sopra i primi p di $\mathbb{Q}$ che si spezzano completamente in $\mathbb{Q}(\zeta_{29})$; per il teorema 3.5 questi sono i primi $p \equiv 1 \mod 29$. Osserviamo immediatamente che il più piccolo primo che soddisfa l'ultima congruenza è 59 ed infatti, cercando tra i primi sopra 59, troviamo che un sistema di generatori di $\mathrm{Cl}(\mathbb{Q}(\zeta_{29}))$ è composto dai tre ideali $(59, 54 + \zeta_n)$, $(59, 55 + \zeta_n)$ e $(59, 56 + \zeta_n)$.

3.5 Estensioni non ramificate

In questa sezione riportiamo un teorema che permette di costruire facilmente estensioni non ramificate di grado ℓ primo di un campo di numeri contenente le radici ℓ-esime dell'unità.

Definizione 3.22 (Primary, hyperprimary e singular primary)**.** Sia p un numero primo e sia K un campo di numeri contenente ζ_p. Poniamo $\pi = \zeta_p - 1$ e $\mathcal{P} = \prod_{\wp|p} \wp$. Sia inoltre $\alpha \in K^* \backslash (K^*)^p$ relativamente primo con p. Diciamo allora che α è

- *primary* se la congruenza $x^p \equiv \alpha \mod p\pi$ ha soluzione in K^*;
- *hyperprimary* se la congruenza $x^p \equiv \alpha \mod p\pi\mathcal{P}$ ha soluzione;
- *singular primary* se è primary ed inoltre esiste un ideale I di K tale che $I^p = (\alpha)$.

Teorema 3.23. *Sia p un numero primo e sia K un campo contenente ζ_p. Sia inoltre $\alpha \in K^* \backslash (K^*)^p$ relativamente primo con p. Valgono allora le seguenti tre equivalenze.*

(a) α è hyperprimary se e solo tutti i primi sopra p si spezzano completamente nell'estensione $K(\alpha^{\frac{1}{p}})/K$.

(b) α è primary se e solo l'estensione $K(\alpha^{\frac{1}{p}})/K$ è non ramificata per tutti i primi sopra p.

(c) α è singular primary se e solo l'estensione $K(\alpha^{\frac{1}{p}})/K$ è non ramificata per tutti i primi di K, fatta eccezione per il caso $p = 2$ in cui potrebbe esserci ramificazione per i primi infiniti.

3.6 Costruzione dell'Hilbert class field di $\mathbb{Q}(\zeta_{29})$

Ci occupiamo ora di costruire esplicitamente l'Hilbert class field del campo $K = \mathbb{Q}(\zeta_{29})$. Visto che per il teorema 3.21 il gruppo $\mathrm{Cl}(K)$ è abeliano elementare di esponente 2 e per il teorema 2.24 il gruppo di Galois $\mathrm{Gal}(K^1/K)$ è isomorfo a $\mathrm{Cl}(K)$, allora sappiamo che esistono 7 estensioni linearmente disgiunte a due a due non ramificate di grado 2 su K e che per ottenere l'Hilbert class field K^1 di K è sufficiente comporre tre di queste estensioni.
Utilizzando il punto (c) del teorema 3.23 e considerando il fatto che K non è un campo reale, possiamo ricondurre il problema di costruire estensioni non ramificate di K di grado 2 a quello equivalente di cercare elementi $\alpha \in K^* \backslash (K^*)^2$ singular

primary. Affinché α sia singular primary deve perciò esistere un ideale I di K tale che $I^2 = (\alpha)$ e deve inoltre avere soluzione la congruenza $x^2 \equiv \alpha \mod 4$.
Dimentichiamoci per un momento della congruenza e studiamo invece le estensioni $K(\sqrt{\alpha})$, dove $\alpha \in K^* \backslash (K^*)^2$ ed esiste un ideale I tale che $I^2 = (\alpha)$. Se fissiamo un ideale I, sappiamo che i possibili generatori di I^2 differiscono tra loro per la moltiplicazione per un'unità, cioè se $(\alpha) = (\alpha') = I^2$ allora $\alpha = \epsilon\alpha'$ con $\epsilon \in E_K$.

Lemma 3.24. *Sia I un ideale non principale di un campo di numeri K tale che I^2 è principale. Le estensioni di grado 2 che otteniamo aggiungendo a K una radice quadrata di un generatore di I^2 sono in corrispondenza biunivoca con gli elementi del gruppo E_K/E_K^2.*

Dimostrazione. È sufficiente osservare che, per la teoria di Kummer o, più elementarmente, per verifica diretta, le radici quadrate di due elementi α e α' di K danno luogo alla stessa estensione se e soltanto se $\alpha/\alpha' \in (K^*)^2$. □

Nel nostro caso dal teorema 3.16 otteniamo subito che $E_{29}/E_{29}^2 \cong (\mathbb{Z}/2\mathbb{Z})^{14}$ e dunque per ogni ideale I di $\mathbb{Q}(\zeta_{29})$ non principale esistono 2^{14} estensioni distinte di grado 2 di $\mathbb{Q}(\zeta_{29})$ ottenute aggiungendo una radice quadrata di un generatore di I^2.

Grazie al seguente lemma scopriamo che in realtà possiamo limitarci a considerare solo un numero finito di ideali I, per la precisione un numero pari alla cardinalità degli elementi di ordine 2 di $\mathrm{Cl}(K)$, cioè 7 e quindi ridurci ad un numero finito di estensioni.

Lemma 3.25. *Siano I e J due ideali appartenenti alla stessa classe. Per ogni $\alpha \in K$ tale che $I^2 = (\alpha)$ esiste $\beta \in K$ tale che $J^2 = (\beta)$ e $K(\sqrt{\alpha}) = K(\sqrt{\beta})$.*

Dimostrazione. Dato che I e J sono due ideali appartenenti alla stessa classe, esiste $\gamma \in K$ tale che $J/I = (\gamma)$ e quindi ricaviamo immediatamente che $J^2 = I^2(\gamma)^2 = (\alpha\gamma^2)$. Poniamo dunque $\beta = \alpha\gamma^2$ e otteniamo la tesi, visto che $\sqrt{\beta}/\sqrt{\alpha} \in K$. □

Fissiamo dunque dei generatori per il gruppo $\mathrm{Cl}(K)$, in particolare prendiamo i tre ideali

$$I_1 = (59, 54 + \zeta_n),\ I_2 = (59, 55 + \zeta_n),\ I_3(59, 56 + \zeta_n)$$

e scegliamo come generatori per i loro quadrati i numeri

$$\alpha_1 = \zeta_n^{14} - \zeta_n^{15} + \zeta_n^{24},\ \alpha_2 = -1 - \zeta_n + \zeta_n^3,\ \alpha_3 = -\zeta_n^6 - \zeta_n^{13} + \zeta_n^{20} + \zeta_n^{21},$$

dove $(\alpha_i) = I_i^2$. Definiamo inoltre gli insiemi

$$B = \{-1, \eta_1, \ldots, \eta_{13}, \alpha_1, \alpha_2, \alpha_3\},$$
$$C = \{(-1)^{c_0}(\eta_1)^{c_1} \ldots (\eta_{13})^{c_{13}}(\alpha_1)^{c_{14}}(\alpha_2)^{c_{15}}(\alpha_3)^{c_{16}} | c_i \in \{0, 1\}\}.$$

Per i lemmi 3.24 e 3.25 ogni estensione $K(\sqrt{\alpha})$ con $(\alpha) = I^2$ e I ideale di K può essere ottenuta aggiungendo a K una radice di un elemento di C. Per costruire l'Hilbert class field K^1 di K è pertanto sufficiente trovare per quali γ tra i $2^{17} = 131072$ elementi di C esiste una soluzione $x \in K$ alla congruenza $x^2 \equiv \gamma \mod 4$. Dato che $\gamma \in \mathcal{O}_K$ possiamo supporre che anche $x \in \mathcal{O}_K$. Per il teorema 3.4 abbiamo che $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ e quindi l'insieme

$$R = \left\{ \sum_{i=0}^{27} a_i \zeta_{29}^i | a_i \in \{0,1,2,3\} \right\}$$

è un sistema di rappresentanti per $\mathcal{O}_K/4\mathcal{O}_K$. A questo punto basterebbe testare la congruenza $\rho^2 \equiv \gamma \mod 4$ per ogni $\gamma \in C$ e per ogni rappresentante $\rho \in R$, ma il numero di tentativi è troppo elevato. Sia dunque $\rho = \sum_{i=0}^{27} a_i \zeta_{29}^i$ con $a_i \in \{0,1,2,3\}$ un elemento di R e osserviamo che se $y \in \mathcal{O}_K$ allora $\rho^2 \equiv (\rho + 2y)^2 \mod 4$. Possiamo così ridurci a considerare solo i $\rho = \sum_{i=0}^{27} a_i \zeta_{29}^i$ con $a_i \in \{0,1\}$. Calcolando esplicitamente il prodotto ρ^2, abbiamo che

$$\begin{aligned}
\left(\sum_{i=0}^{27} a_i \zeta_{29}^i \right)^2 &= \sum_{i=0}^{27} a_i^2 \zeta_{29}^{2i} + 2w = \sum_{i=0}^{13} a_i^2 \zeta_{29}^{2i} + a_{14}^2 \zeta_{29}^{28} + \sum_{i=15}^{27} a_i^2 \zeta_{29}^{2i-29} + 2w \\
&= \sum_{i=0}^{13} a_i^2 \zeta_{29}^{2i} + \sum_{i=15}^{27} a_i^2 \zeta_{29}^{2i-29} - \sum_{i=0}^{27} a_{14}^2 \zeta_{29}^{2i} + 2w \\
&= \sum_{i=0}^{13} (a_i^2 - a_{14}^2) \zeta_{29}^{2i} + \sum_{i=15}^{27} (a_i^2 - a_{14}^2) \zeta_{29}^{2i-29} - a_{14}^2 \zeta_{29}^{27} + 2w,
\end{aligned}$$

dove $w \in \mathcal{O}_K$. In questo modo notiamo che, una volta dato $\gamma \in C$ e supposto che la congruenza $\rho^2 \equiv \gamma \mod 2$ abbia soluzione, la parità di ciascun a_i risulta fissata da γ. D'altra parte, poiché $a_i \in \{0,1\}$, abbiamo da testare un solo candidato ρ per ogni γ; tutto questo può essere fatto in poche frazioni di secondo da un calcolatore. Come risultato otteniamo i quadrati dei generatori delle 7 estensioni quadratiche non ramificate e precisamente:

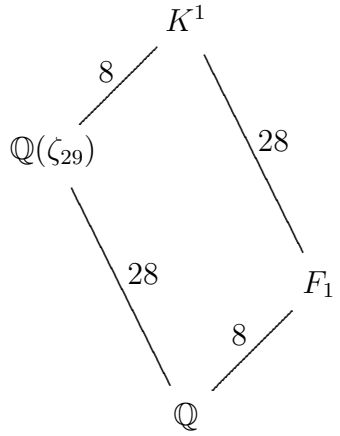
$$\begin{aligned}
\rho_1 &= \eta_{12}\eta_{11}\eta_{10}\eta_8\eta_7\eta_6\eta_2, \\
\rho_2 &= \eta_{13}\eta_{11}\eta_9\eta_6\eta_5\eta_3\eta_2, \\
\rho_3 &= \eta_{13}\eta_{12}\eta_{10}\eta_9\eta_8\eta_7\eta_5\eta_3, \\
\rho_4 &= -\eta_9\eta_8\eta_7\eta_6\eta_4\eta_3\eta_2\eta_1, \\
\rho_5 &= -\eta_{12}\eta_{11}\eta_{10}\eta_9\eta_4\eta_3\eta_1, \\
\rho_6 &= -\eta_{13}\eta_{11}\eta_8\eta_7\eta_5\eta_4\eta_1, \\
\rho_7 &= -\eta_{13}\eta_{12}\eta_{10}\eta_6\eta_5\eta_4\eta_2\eta_1.
\end{aligned}$$

3.7 Gruppo di Galois dell'Hilbert class field di $\mathbb{Q}(\zeta_{29})$ su $\mathbb{Q}$

L'Hilbert class field K^1 di $\mathbb{Q}(\zeta_{29})$ è un'estensione normale di $\mathbb{Q}$; sorge quindi naturalmente il problema di calcolare il gruppo di Galois $\mathrm{Gal}(K^1/\mathbb{Q})$. Per prima cosa osserviamo lo spezzamento del primo 29. Per il teorema 3.6 sappiamo che 29 ramifica totalmente in K; in particolare vale che $(29)\mathcal{O}_K = (1-\zeta_{29})^{28}\mathcal{O}_K$. Dato che, per il corollario 2.25, tutti gli ideali primi principali di un campo si spezzano completamente nell'Hilbert Class Field, avremo che $(1-\zeta_{29})\mathcal{O}_{K^1} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4\mathfrak{P}_5\mathfrak{P}_6\mathfrak{P}_7\mathfrak{P}_8$ e dunque

$$(29)\mathcal{O}_{K^1} = \prod_{i=1}^{8} \mathfrak{P}_i^{28}\mathcal{O}_{K^1}.$$

Possiamo quindi fissare un ideale $\mathfrak{P}_1$ di K^1 sopra 29 e considerarne il campo di decomposizione F_1 che, in questo caso, coincide con il campo di inerzia, dal momento che $f(\mathfrak{P}_1|29) = 1$. Inoltre, essendo $e(\mathfrak{P}_1|29) = 28$, F_1 è un'estensione di $\mathbb{Q}$ di grado 8 ed è linearmente disgiunta da K, in quanto 29 ramifica completamente in K, mentre l'indice di ramificazione di $\mathfrak{P}_1 \cap \mathcal{O}_{F_1}$ su 29 è 1. Pertanto, confrontando i gradi delle estensioni e ricordando che l'indice di ramificazione ed il grado d'inerzia sono moltiplicativi nelle torri di estensioni, otteniamo che $K^1 = KF_1$.



Per il corollario 3.3 sappiamo che l'estensione $K/\mathbb{Q}$ è di Galois ed inoltre che $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/28\mathbb{Z}$. Dato che il gruppo $\mathrm{Gal}(K^1/F_1)$ si immerge iniettivamente nel gruppo $\mathrm{Gal}(K/\mathbb{Q})$ e i gradi delle estensioni K^1/F_1 e $K/\mathbb{Q}$ sono entrambi uguali a 28, ricaviamo che $\mathrm{Gal}(K^1/F_1) \cong (\mathbb{Z}/28\mathbb{Z})$. Grazie ai teoremi 2.24 e 3.21 ricaviamo che $\mathrm{Gal}(K^1/K) \cong \mathrm{Cl}(K) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Lemma 3.26. *La funzione*

$$\psi : \mathrm{Gal}(K^1/K) \times \mathrm{Gal}(K^1/F_1) \to \mathrm{Gal}(K^1/\mathbb{Q})$$

tale che $\psi(\sigma,\tau)=\sigma\tau$ *è biunivoca.*

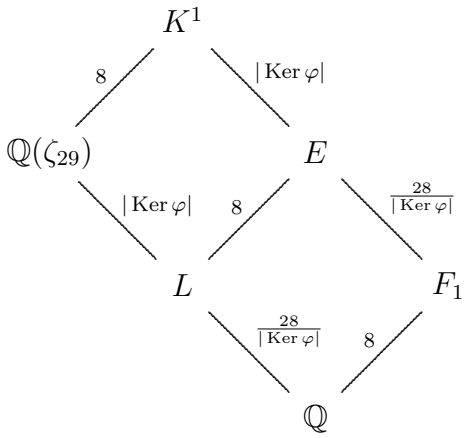
Dimostrazione. Dal momento che $[K^1:\mathbb{Q}(\zeta_{29})][K^1:F_1]=28\cdot 8=[K^1:\mathbb{Q}]$, allora $\mathrm{Gal}(K^1/K)\times\mathrm{Gal}(K^1/F_1)$ e $\mathrm{Gal}(K^1/\mathbb{Q})$ hanno la stessa cardinalità. Per ottenere la tesi possiamo quindi limitarci a dimostrare che ψ è iniettiva. Supponiamo che $\sigma_1\tau_1=\sigma_2\tau_2$ con $\sigma_1,\sigma_2\in\mathrm{Gal}(K^1/K)$ e $\tau_1,\tau_2\in\mathrm{Gal}(K^1/F_1)$. Allora l'elemento $\sigma_2^{-1}\sigma_1=\tau_2\tau_1^{-1}$ di $\mathrm{Gal}(K^1/\mathbb{Q})$ appartiene sia a $\mathrm{Gal}(K^1/K)$ sia a $\mathrm{Gal}(K^1/F_1)$ e quindi, poiché K^1 è il composto di K e F_1, è l'identità. Perciò $\sigma_1=\sigma_2$ e $\tau_1=\tau_2$ e dunque la mappa ψ è iniettiva. □

Per poter dire che $\mathrm{Gal}(K^1/\mathbb{Q})$ è un prodotto semidiretto tra $\mathrm{Gal}(K^1/K)$ e $\mathrm{Gal}(K^1/F_1)$ è necessario dimostrare che uno di questi ultimi 2 gruppi è un sottogruppo normale di $\mathrm{Gal}(K^1/\mathbb{Q})$, ma questo è immediato, in quanto abbiamo appena ricordato che l'estensione $K/\mathbb{Q}$ è di Galois e dunque $\mathrm{Gal}(K^1/K)$ è un sottogruppo normale di $\mathrm{Gal}(K^1/\mathbb{Q})$. Perciò

$$\mathrm{Gal}(K^1/\mathbb{Q})\cong(\mathbb{Z}/2\mathbb{Z})^3\rtimes_\varphi\mathbb{Z}/28\mathbb{Z},$$

dove $\varphi:\mathbb{Z}/28\mathbb{Z}\to\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^3)$.

Per descrivere, a meno di isomorfismi, il gruppo di Galois di K^1 su $\mathbb{Q}$, è ora necessario studiare la mappa φ. Il gruppo $(\mathbb{Z}/2\mathbb{Z})^3$ contiene 7 elementi di ordine 2 e quindi qualunque automorfismo $\psi\in\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^3)$ fissa l'identità e permuta tra loro gli altri 7 elementi; ciò significa che è possibile vedere $\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^3)$ come sottogruppo di S_7. Poiché in S_7 non esistono elementi di ordine 14 né, a maggior ragione, di ordine 28, possiamo allora concludere che $\mathrm{Ker}\,\varphi$ è diverso da $\{e\}$ e da $\mathbb{Z}/2\mathbb{Z}$.
Vogliamo ora dimostrare che $\mathrm{Ker}\,\varphi\cong\mathbb{Z}/4\mathbb{Z}$. Supponiamo quindi, per assurdo, che $\mathrm{Ker}\,\varphi$ sia isomorfo ad uno degli altri tre gruppi possibili: $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$ e $\mathbb{Z}/28\mathbb{Z}$. Indichiamo con g_i, dove $1\le i\le|\mathrm{Ker}\,\varphi|$, gli elementi di $\mathrm{Gal}(K^1/F_1)$ che appartengono a $\mathrm{Ker}\,\varphi$ e osserviamo che l'insieme $G=\{(0,g_i)|1\le i\le|\mathrm{Ker}\,\varphi|\}$ è un sottogruppo di $\mathrm{Gal}(K^1/\mathbb{Q})$. Possiamo facilmente verificare che il gruppo G è isomorfo a $\mathrm{Ker}\,\varphi$ e che G è contenuto nel centro di $\mathrm{Gal}(K^1/\mathbb{Q})$. Pertando G è un sottogruppo normale di $\mathrm{Gal}(K^1/\mathbb{Q})$ ed esiste allora un'estensione di Galois $E/\mathbb{Q}$ tale che $\mathrm{Gal}(E/\mathbb{Q})\cong\mathrm{Gal}(K^1/\mathbb{Q})/\mathrm{Ker}\,\varphi$. Dalla teoria di Galois sappiamo che E contiene F_1 ed inoltre la sottoestensione L di K di grado $28/|\mathrm{Ker}\,\varphi|$ su $\mathbb{Q}$.



Notiamo immediatamente che E/L è non ramificata al finito e di grado 8, in quanto la fattorizzazione in E dell'unico primo da considerare, l'intero 29, contiene necessariamente 8 primi distinti, poiché E è un'estensione normale di $\mathbb{Q}$ e c'è un primo sopra 29 che ha indice di ramificazione e d'inerzia uguale a 1 in F_1. Per concludere dobbiamo quindi dimostrare che L_4, $\mathbb{Q}(\sqrt{29})$ e $\mathbb{Q}$ non hanno estensioni non ramificate al finito di grado 8. Grazie alla legge di reciprocità (teorema 2.14) e al teorema 2.4 abbiamo che

$$[E : L] = |\operatorname{Gal}(E/L)| \leq I_L^{\mathfrak{M}_\infty}/P_L^{\mathfrak{M}_\infty,1} = h_{\mathfrak{M}} \leq h_L \cdot 2^{r_0}, \tag{3.1}$$

dove $\mathfrak{M}_\infty$ è il prodotto di tutti gli r_0 primi reali di L. Ora L_4, $\mathbb{Q}(\sqrt{29})$ e $\mathbb{Q}$ sono tutti campi con gruppo delle classi banali e dunque $h_L = 1$. Inoltre L_4 è un'estensione normale complessa e perciò non ha primi reali, $\mathbb{Q}(\sqrt{29})$ ne ha 2 e $\mathbb{Q}$ solo 1. La disuguaglianza 3.1 implica pertanto che $8 = [E : L] \leq 4$, cioè un assurdo. Abbiamo così dimostrato che

$$\operatorname{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/7\mathbb{Z},$$

dove φ ha immagine non banale.

In generale queste informazioni non sono sufficienti a individuare, a meno di isomorfismi, il gruppo, ma in questo caso, grazie al seguente lemma, dimostriamo che il gruppo è univocamente determinato.

Lemma 3.27. *Siano N e M due gruppi e φ e φ' due omomorfismi da M in* $\operatorname{Aut}(N)$*. Se M è ciclico e il sottogruppo $\varphi(M)$ è coniugato a $\varphi'(M)$, allora*

$$N \rtimes_\varphi M \cong N \rtimes_{\varphi'} M.$$

Dimostrazione. Sia m un generatore di M. Dato che M è ciclico e $\varphi(M)$ è coniugato a $\varphi'(M)$, allora esiste un intero i e un automorfismo $\alpha \in \operatorname{Aut}(N)$ tali che

$$\varphi'(m^i) = \alpha\varphi(m)\alpha^{-1}.$$

È quindi immediato verificare che un isomorfismo tra $N \rtimes_\varphi M$ e $N \rtimes_{\varphi'} M$ è dato dalla funzione $(n, m^j) \mapsto (n, m^{ij})$. □

Possiamo facilmente calcolare che la cardinalità del gruppo $\mathrm{Aut}(N)$ è uguale a $168 = 2^3 \cdot 3 \cdot 7$ e dunque, per il secondo teorema di Sylow, tutti i sottogruppi di 7 elementi di $\mathrm{Aut}(N)$ sono coniugati tra loro. Applicando il lemma 3.27 con $N = (\mathbb{Z}/2\mathbb{Z})^3$ e $M = \mathbb{Z}/7\mathbb{Z}$ otteniamo che il prodotto semidiretto $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/7\mathbb{Z}$ è unico, a meno di isomorfismi, se, come nel nostro caso, φ ha nucleo banale. Perciò, osservando che K^1 è il composto di E e L_4, possiamo concludere che è univocamente determinato anche il gruppo

$$\mathrm{Gal}(K^1/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \times ((\mathbb{Z}/2\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/7\mathbb{Z}),$$

dove l'omomorfismo $\varphi : \mathbb{Z}/7\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^3)$ ha nucleo banale.

Capitolo 4

Teoria dei nodi

Nella prima parte di questo capitolo esponiamo la teoria dei nodi di Scholz [24], seguendo in parte l'articolo di Jehne [15]. Presentiamo poi alcuni interessanti risultati.

4.1 Il quadrato fondamentale

Sia K un campo di numeri. Direttamente dalla definizione di gruppo delle classi di ideali abbiamo la successione esatta

$$1 \to P_K \to I_K \to \mathrm{Cl}(K) \to 1.$$

Immergendo invece K^* nel gruppo degli ideli J_K ricaviamo la successione esatta

$$1 \to K^* \to J_K \to \mathcal{C}(K) \to 1,$$

dove, per definizione, $\mathcal{C}(K) = J_K/K^*$ è il gruppo delle classi degli ideli. L'omomorfismo canonico surgettivo

$$J_K \to I_K, \quad \alpha = (\alpha_\mathfrak{p}) \mapsto \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})},$$

ha per nucleo precisamente tutti gli ideli α tali che $v_\mathfrak{p}(\alpha_\mathfrak{p}) = 0$ o, equivalentemente, $\alpha_\mathfrak{p} \in U_\mathfrak{p}$ per ogni $\mathfrak{p} \nmid \infty$. Chiamiamo gruppo delle unità degli ideli il nucleo di questa applicazione e lo indichiamo con U_K. Otteniamo così un'altra successione esatta:

$$1 \to U_K \to J_K \to I_K \to 1.$$

Osserviamo poi che dall'omomorfismo surgettivo $K^* \to P_K$, che manda ogni elemento di K^* nell'ideale generato dall'elemento stesso, ricaviamo immediatamente un'ulteriore successione esatta:

$$1 \to E_K \to K^* \to P_K \to 1.$$

Immergiamo E_K in U_K e definiamo gruppo delle classi delle unità degli ideli il quoziente $\mathcal{E}_K = U_K/E_K$. In questo modo riusciamo a costruire il seguente quadrato fondamentale di successioni esatte corte.

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & E_K & \longrightarrow & K^* & \longrightarrow & P_K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U_K & \longrightarrow & J_K & \longrightarrow & I_K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathcal{E}_K & \longrightarrow & \mathcal{C}(K) & \longrightarrow & \mathrm{Cl}(K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Tutti i gruppi del diagramma dipendono dal campo di numeri K e quindi possiamo definire dei funtori $E, U, J, ^*, \ldots$ dalla categoria dei campi di numeri in quella dei gruppi abeliani che associano ad un campo di numeri K rispettivamente i gruppi $E_K, U_K, J_K, K^*, \ldots$ Per ogni estensione L/K la norma N_K^L induce degli omomorfismi $F_L \to F_K$ per i funtori $F = E, U, J, ^*$ e quindi, prendendo i quozienti, anche per tutti gli altri. Per ogni funtore F definito a partire dal quadrato fondamentale poniamo quindi

$$F_{\#}(L/K) := \mathrm{Ker}(N_K^L : F_L \to F_K), \quad F^{\#}(L/K) := \mathrm{Coker}(N_K^L : F_L \to F_K).$$

Osserviamo che possiamo considerare il nucleo e il conucleo della norma come funtori della categoria delle estensioni algebriche di campi di numeri. Una qualunque successione esatta corta

$$1 \to A \to B \to C \to 1$$

di funtori ottenuta dal quadrato fondamentale è compatibile con la norma, vale cioè il seguente diagramma:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A_L & \longrightarrow & B_L & \longrightarrow & C_L & \longrightarrow & 1 \\
 & & \mathrm{N}\downarrow & & \mathrm{N}\downarrow & & \mathrm{N}\downarrow & & \\
1 & \longrightarrow & A_K & \longrightarrow & B_K & \longrightarrow & C_K & \longrightarrow & 1
\end{array} \tag{4.1}$$

4.2 Nodi in un'estensione algebrica

Per poter definire i nodi, è utile prima ricordiare il seguente importante lemma sui diagrammi commutativi.

Lemma 4.1 (Lemma del serpente)**.** *Sia dato un diagramma commutativo con le righe esatte nella categoria dei gruppi abeliani:*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 1 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

Vale allora la seguente successione esatta:

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & \operatorname{Ker} f & \longrightarrow & \operatorname{Ker} a & \longrightarrow & \operatorname{Ker} b & \longrightarrow & \operatorname{Ker} c & & \\ & & & & & & & & \downarrow{\scriptstyle d} & & \\ 1 & \longleftarrow & \operatorname{Coker} g' & \longleftarrow & \operatorname{Coker} c & \longleftarrow & \operatorname{Coker} b & \longleftarrow & \operatorname{Coker} a & & \end{array}$$

Nel lemma del serpente è centrale l'esistenza dell'omomorfismo di collegamento d. Poiché utilizzeremo più volte questo lemma, ricordiamo la definizione di d. Fissiamo un elemento γ in $\operatorname{Ker} c$, che è anche un elemento di C. Dal momento che l'omomorfismo g è surgettivo, esiste un elemento β in B tale che $g(\beta) = \gamma$. Il diagramma è commutativo e dunque $1 = c(\beta) = c(g(\beta)) = g'(b(\beta))$, cioè $b(\beta)$ appartiene a $\operatorname{Ker} g'$. Dall'esattezza della seconda riga troviamo un elemento α' in A' tale che $f'(\alpha') = b(\beta)$. Definiamo pertanto $d(\gamma) = \alpha' + \operatorname{Im} a$.

Applicando questo lemma al diagramma 4.1, otteniamo la successione esatta

$$\begin{array}{ccccccc} 1 & \longrightarrow & A_{\#} & \longrightarrow & B_{\#} & \longrightarrow & C_{\#} \\ & & & & & & \downarrow{\scriptstyle d} \\ 1 & \longleftarrow & C^{\#} & \longleftarrow & B^{\#} & \longleftarrow & A^{\#} \end{array} \tag{4.2}$$

Definizione 4.2 (Nodo)**.** Definiamo *nodo* di A in B in un'estensione finita L/K e lo indichiamo con $[A, B]_{L/K}$ l'immagine dell'omomorfismo di collegamento d, cioè

$$[A, B]_{L/K} = A_K \cap N_K^L B_L / N_K^L A_L.$$

Il nodo di A in B misura in un certo senso quanto distano dall'essere esatte la sequenza dei nuclei della norma e quella dei conuclei della norma. Dalla definizione di nodo riusciamo infatti a spezzare la successione 4.2 nelle seguenti due successioni esatte:

$$1 \to A_{\#} \to B_{\#} \to C_{\#} \to [A, B] \to 1, \tag{4.3}$$

$$1 \to [A, B] \to A^{\#} \to B^{\#} \to C^{\#} \to 1. \tag{4.4}$$

Per ognuna delle sei successioni esatte corte del quadrato fondamentale possiamo chiaramente definire il rispettivo nodo associato. In questo modo otteniamo sei nodi, ma uno di questi è banale; vale infatti il seguente lemma.

Lemma 4.3. *Il nodo delle unità degli ideli negli ideli è banale, cioè* $[U, J] = 1$.

Dimostrazione. Dobbiamo dimostrare che $U_K \cup N_K^L J_L = N_K^L U_L$. Considerando una componente degli ideli alla volta, è sufficiente provare che per ogni $\mathfrak{P}|\mathfrak{p}$ in L/K vale l'uguaglianza

$$U_\mathfrak{p} \cup N_{K_\mathfrak{p}}^{L_\mathfrak{P}} L_\mathfrak{P}^* = N_{K_\mathfrak{p}}^{L_\mathfrak{P}} U_\mathfrak{P}.$$

Il caso in cui $K_\mathfrak{p}$ è archimedeo è di verifica immediata: infatti se $\mathfrak{p}$ e $\mathfrak{P}$ sono entrambi reali o entrambi complessi l'uguaglianza è ovvia, mentre se $\mathfrak{p}$ è reale e $\mathfrak{P}$ è complesso otteniamo

$$\mathbb{R} \cap N_\mathbb{R}^\mathbb{C} \mathbb{C}^* = \mathbb{R}^+ = N_\mathbb{R}^\mathbb{C} \mathbb{C}^*.$$

Sia perciò $\mathfrak{p}$ un ideale primo di K e siano π_K e π_L elementi primi rispettivamente di $K_\mathfrak{p}$ e $L_\mathfrak{P}$. Per ogni elemento $a \in K_\mathfrak{P}$ possiamo scrivere $a = \pi_L^\nu u$, dove $u \in U_\mathfrak{P}$, e quindi $N(a) = \pi_K^{\nu f} \eta N(u)$ con $\eta \in U_\mathfrak{p}$. La condizione $N(a) \in U_\mathfrak{p}$ implica $\nu = 0$ e dunque $a \in U_\mathfrak{P}$, da cui la tesi. □

Il lemma appena dimostrato ci permette di fare la seguente osservazione.

Osservazione 4.4. *Per ogni estensione di campi di numeri* L/K *vale* $E_K \cap NL^* \subseteq E_K \cap NU_L$ *e quindi*

$$[E, M] \leq [E, U],$$

dove con M *indichiamo il funtore che ad un campo di numeri* K *associa il gruppo moltiplicativo* K^*.

Rimangono perciò cinque nodi, ai quali diamo i seguenti nomi:

1. number knot $\nu = \nu_{L/K} = [K^*, J_K]$;
2. first unit knot $\omega = \omega_{L/K} = [E_K, K^*]$;
3. second unit knot $\omega' = \omega'_{L/K} = [E_K, U_K]$;
4. ideal knot $\delta = \delta_{L/K} = [P_K, I_K]$;
5. idele knot $\gamma = \gamma_{L/K} = [\mathcal{E}_K, \mathcal{C}(K)]$.

4.3 Successione fondamentale di nodi

Applichiamo la successione esatta corta 4.3 alle ultime due righe del quadrato fondamentale e, ricordando il lemma 4.3, otteniamo il seguente diagramma commutativo esatto:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & U_\# & \longrightarrow & J_\# & \longrightarrow & I_\# & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathcal{E}_\# & \longrightarrow & \mathcal{C}_\# & \longrightarrow & \mathrm{Cl}_\# & \longrightarrow & [\mathcal{E}, \mathcal{C}] \longrightarrow 1
\end{array}$$

Utilizzando ora il lemma 4.1 del serpente, ricaviamo la successione esatta

$$\begin{array}{ccccccccc} & & 1 & \longrightarrow & E_{\#} & \longrightarrow & M_{\#} & \longrightarrow & P_{\#} \\ & & & & & & & & \downarrow \\ 1 & \longleftarrow & \gamma & \longleftarrow & \delta & \longleftarrow & \nu & \longleftarrow & \omega' \end{array}$$

Se spezziamo quest'ultima successione esatta in ω', troviamo la successione esatta fondamentale di nodi.

Teorema 4.5 (Successione fondamentale di nodi (Fundamental knot sequence))**.** *Sia L/K una qualunque estensione normale di campi di numeri. Allora è esatta la successione*

$$1 \longrightarrow \omega \longrightarrow \omega' \xrightarrow{\psi} \nu \xrightarrow{\varphi} \delta \longrightarrow \gamma \longrightarrow 1.$$

Dimostrazione. Poiché l'osservazione 4.4 implica che $\omega \hookrightarrow \omega'$, per ricavare la tesi è sufficiente dimostrare che la successione in esame è esatta in ω'. Per comodità identifichiamo ω con la sua immagine in ω'. Ora $\omega \subseteq \operatorname{Ker}\psi$ in quanto $\omega \subseteq NL^*/NE_L$. D'altra parte osserviamo che un elemento di ω' che appartiene a $\operatorname{Ker}\psi$ deve appartenere a $E_K \cap NL^*/NE_L$, cioè a ω. □

A. Scholz considera altri due nodi oltre a ν:

1. Scholz's unit knot $\omega^0 = \omega'/\omega$;
2. Scholz's divisor knot $\delta^0 = \operatorname{Im}(\varphi)$.

Grazie a queste nuove definizioni possiamo riscrivere la successione fondamentale.

Teorema 4.6 (Scholz's knot sequence)**.** *Vale la seguente successione esatta:*

$$1 \longrightarrow \omega^0_{L/K} \longrightarrow \nu_{L/K} \longrightarrow \delta^0_{L/K} \longrightarrow 1.$$

Come corollario del teorema 4.5 ricaviamo un risultato di Furuta ([5], Teorema 5).

Corollario 4.7. *Sia L/K un'estensione di campi di numeri tale che il numero delle classi $h_L = h$ di L sia relativamente primo con il grado n dell'estensione. Allora*

$$\omega'_{L/K} \cong \nu_{L/K}$$

Dimostrazione. Se dimostriamo che $\omega_{L/K} = \delta_{L/K} = 1$, allora il teorema 4.5 fornisce l'isomorfismo che cerchiamo. Per definizione abbiamo

$$\delta_{L/K} = P_K \cap NI_L/NP_L$$

e dunque vogliamo mostrare che $P_K \cap NI_L = NP_L$. Chiaramente $P_K \cap NI_L \supseteq NP_L$ e quindi rimane da provare l'altro contenimento. Consideriamo perciò un ideale A di L tale che $NA = (k)$, con $k \in K$. Elevando alla h ricaviamo che $NA^h = (k)^h$. Poiché, per definizione, h è la cardinalità del gruppo delle classi di ideali di L, esiste un elemento $l \in L$ tale che $A^h = (l)$. Inoltre, per il teorema cinese del resto, esistono due interi a e b tali che $ah + bn = 1$ e pertanto possiamo scrivere

$$(k) = (k)^{ah+bn} = N((l)^a(k)^b),$$

da cui $(k) \in NP_L$. Quanto al fatto che $\omega_{L/K} = 1$, cioè che $E_K \cap NL^* = NE_L$, osserviamo che anche in questo caso un contenimento è banale, in particolare $E_K \cap NL^* \supseteq NE_L$. Sia perciò ε un elemento di $E_K \cap NL^*$ e siano l e m due interi di L tali che $N(l/m) = \varepsilon$. Fattorizziamo (l) in L in modo da avere

$$(l) = \mathfrak{P}_1^{f_1} \cdots \mathfrak{P}_r^{f_r},$$

con $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ ideali primi distinti di L. Eleviamo alla h e notiamo che possiamo scomporre l^h nel prodotto di interi l_i di L tali che $(l_i) = (\mathfrak{P}_i^{f_i})^h$, così che possiamo scrivere $l^h = \eta l_1 \cdots l_r$, con $\eta \in E_L$. Ragionando allo stesso modo per m, troviamo $m^h = \vartheta m_1 \cdots m_s$, con $\vartheta \in E_L$. Poiché $N(l/m) \in E_k$, gli ideali primi in cui si fattorizza (l) sono, a meno di coniugati, gli stessi in cui si fattorizza (m). Possiamo pertanto supporre, eventualmente sostituendo qualche m_i con un suo coniugato, che questi due insiemi di ideali siano uguali, dato che la norma di due elementi coniugati è uguale. Da ciò segue che esiste un elemento $\eta \in E_L$ tale che $N\eta = \varepsilon^h$. Utilizzando gli interi a e b dati dal teorema cinese del resto ottenuti sopra, abbiamo

$$\varepsilon = \varepsilon^{ah+bn} = N(\eta^a \varepsilon^b),$$

da cui $\varepsilon \in NE_L$. □

4.4 Estensioni centrali

Definizione 4.8 (Estensione di un gruppo)**.** Sia G un gruppo. Definiamo *estensione del gruppo* G una qualunque sequenza esatta corta di gruppi

$$1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1.$$

Definizione 4.9 (Estensione centrale e ricoprimento)**.** Consideriamo un'estensione di gruppi X:

$$1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1.$$

Definiamo l'estensione di gruppi X *centrale* se A è contenuto in $Z(G)$, mentre diciamo che è un *ricoprimento* se $A \subseteq \Gamma'$.

Schur ha dimostrato in [25] che l'ordine dei gruppi A nelle estensioni centrali che sono ricoprimenti è limitato. Inoltre i gruppi A che appartengono ad un qualunque ricomprimento centrale massimale sono isomorfi. Possiamo perciò dare un nome a questa classe di isomorfismo.

Definizione 4.10 (Moltiplicatore di Schur)**.** Definiamo *moltiplicatore di Schur* di un gruppo finito G e lo indichiamo con $\mathcal{M}(G)$ la classe di isomorfismo del gruppo A in un qualunque ricoprimento centrale massimale X:

$$1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1.$$

Chiamiamo inoltre gruppo di ricoprimento di G ogni gruppo Γ in un ricoprimento centrale massimale.

Sempre in [25] Schur ha determinato la struttura di $\mathcal{M}(G)$ per gruppi abeliani G, dimostrando la seguente proposizione.

Proposizione 4.11. *Sia G un p-gruppo abeliano. Grazie alla decomposizione di Kronecker (teorema 5.1) possiamo scrivere*

$$G = \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p^{n_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_m}\mathbb{Z},$$

con $n_1 \geq n_2 \geq \cdots \geq n_m$. Abbiamo allora che

$$\mathcal{M}(G) \cong \mathbb{Z}/p^{n_2}\mathbb{Z} \oplus (\mathbb{Z}/p^{n_3}\mathbb{Z})^2 \oplus \cdots \oplus (\mathbb{Z}/p^{n_m}\mathbb{Z})^{m-1}.$$

In particolare $\operatorname{rank}_p(\mathcal{M}(G)) = \binom{m}{2}$.

Per un'esposizione completa delle proprietà del moltiplicatore di Schur di un gruppo rimandiamo a [16].

Definizione 4.12 (Torre ed estensione centrale)**.** Sia $L/K/F$ una torre di estensioni di campi di numeri. Diciamo che la torre $L/K/F$ è una *torre centrale* se lo è l'estensione di gruppi di Galois associata

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/F) \longrightarrow \mathrm{Gal}(K/F) \longrightarrow 1.$$

In questo caso chiamiamo L un'*estensione centrale* di K rispetto a F.

Definizione 4.13 (Central class field)**.** Sia K/F un'estensione normale di campi di numeri. Chiamiamo *central class field* di K rispetto a F la massima estensione centrale non ramificata di K rispetto a F e la indichiamo con K_c qualora sia evidente il campo F cui facciamo riferimento.

Come conseguenza dei risultati sui nodi delle sezioni precedenti e di quelli di class field theory è possibile dimostrare i seguenti isomorfismi di genus theory. Per la dimostrazione rimandiamo a [15]. L'ultimo isomorfismo era stato scoperto da Scholz [24] e riscoperto da Furuta [5].

Teorema 4.14. *Sia L/K un'estensione di campi di numeri e sia H^1 l'Hilbert class field di K. Valgono allora i seguenti tre isomorfismi:*

$$\begin{aligned} \delta^0 &\cong \mathrm{Gal}(L_c/L_g); \\ \delta &\cong \mathrm{Gal}(L_c/H^1 L); \\ \gamma &\cong \mathrm{Gal}(L_g/H^1 L). \end{aligned}$$

Il seguente teorema è un risultato di Schur [24] e Tate.

Teorema 4.15. *Sia L/K un'estensione normale di campi di numeri con gruppo di Galois G. Siano inoltre $G_{\mathfrak{P}}$ i gruppi di Galois delle estensioni $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, dove con $L_{\mathfrak{P}}$ e $K_{\mathfrak{p}}$ indichiamo i completamenti di L e K rispetto agli ideali primi $\mathfrak{P}$ e $\mathfrak{p}$, con $\mathfrak{P}|\mathfrak{p}$. Vale allora la sequenza esatta*

$$\coprod_{\mathfrak{P}} \mathcal{M}(G_{\mathfrak{P}})\hat{} \to \mathcal{M}(G)\hat{} \to \nu_{L/K} \to 1.$$

Dimostrazione. Riportiamo brevemente i passaggi principali della dimostrazione, rimandando a [2] per le definizioni e le proprietà dei gruppi di coomologia e per ulteriori dettagli.

Per un primo $\mathfrak{P}$ di L sopra un primo $\mathfrak{p}$ di K poniamo $G_{\mathfrak{p}} = \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Consideriamo la successione esatta:

$$H^{-1}(G, J_L) \to H^{-1}(G, \mathcal{C}_L) \to \nu \to 1.$$

Da un risultato di class field theory sappiamo che

$$H^{-1}(G, J_L) \cong \coprod_{\mathfrak{p}} H^{-1}(G_{\mathfrak{p}}, L^*_{\mathfrak{P}}).$$

Dalla reciprocità di Tate abbiamo gli isomorfismi

$$\begin{aligned} H^{-1}(G_{\mathfrak{p}}, L^*_{\mathfrak{P}}) &\cong H^{-3}(G_{\mathfrak{p}}, \mathbb{Z}), \\ H^{-1}(G, \mathcal{C}_L) &\cong H^{-3}(G, \mathbb{Z}). \end{aligned}$$

Dal teorema di dualità della coomologia di gruppi finiti ricaviamo

$$\begin{aligned} H^{-3}(G, \mathbb{Z}) &\cong H^2(G, \mathbb{Q}/\mathbb{Z})\hat{} \\ H^{-3}(G_{\mathfrak{p}}, \mathbb{Z}) &\cong H^2(G_{\mathfrak{p}}, \mathbb{Q}/\mathbb{Z})\hat{} \end{aligned}$$

e dunque, ricordando che il moltiplicatore di Schur $\mathcal{M}(G)$ è isomorfo al gruppo $H^2(G, \mathbb{Q}/\mathbb{Z})$, otteniamo la tesi. □

Teorema 4.16 (Hasse norm theorem)**.** *Sia L/K un'estensione ciclica di campi di numeri. Allora un elemento di K è una norma di L/K se e solo se è una norma di $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ per ogni valutazione $\mathfrak{P}$ di L, vale cioè*

$$\nu_{L/K} = 1.$$

Dimostrazione. Consideriamo la sequenza esatta del teorema 4.15

$$\coprod_{\mathfrak{P}} \mathcal{M}(G_{\mathfrak{P}})\hat{} \longrightarrow \mathcal{M}(G)\hat{} \longrightarrow \nu_{L/K} \longrightarrow 1.$$

Poiché il moltiplicatore di Schur di un gruppo ciclico è banale, possiamo concludere che $\nu_{L/K} = 1$. □

Corollario 4.17. *Sia L/K un'estensione normale non ramificata di campi di numeri con gruppo di Galois G. Allora*

$$\nu_{L/K} \cong \mathcal{M}(G).$$

Dimostrazione. Poiché L/K è non ramificata, allora anche $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ è non ramificata per ogni valutazione $\mathfrak{P}$ di L. Dato che le estensioni non ramificate di campi locali sono cicliche, allora abbiamo che $\mathcal{M}(G_{\mathfrak{P}}) = 1$ per ogni valutazione $\mathfrak{P}$ di L. Utilizzando ora la successione esatta del teorema 4.15, ricaviamo la tesi. □

Corollario 4.18. *Sia L/K un'estensione normale, finita e non ramificata con gruppo di Galois $G = \mathrm{Gal}(L/K)$. Vale allora la seguente successione esatta:*

$$1 \longrightarrow E_K/E_K \cap NL^* \longrightarrow \mathcal{M}(G)\hat{} \longrightarrow \mathrm{Gal}(L_c/L_g) \longrightarrow 1.$$

Dimostrazione. Consideriamo la succesione esatta del teorema 4.6

$$1 \longrightarrow \omega^0_{L/K} \longrightarrow \nu_{L/K} \longrightarrow \delta^0_{L/K} \longrightarrow 1.$$

Per ipotesi l'estensione L/K è non ramificata e quindi ogni unità in E_K è una norma locale, cioè $E_K \cap NU_L = E_K$. Abbiamo perciò che $\omega^0_{L/K} \cong E_K/E_K \cap NL^*$. Applicando ora il corollario 4.17 e il teorema 4.14 otteniamo la tesi. □

La seguente proposizione è dovuta a Iwasawa [13].

Proposizione 4.19. *Sia K un campo di numeri tale che la sua p-Hilbert class field tower termini con L. Allora*

$$E_K/NE_L \cong \mathcal{M}(\mathrm{Gal}(L/K)).$$

Presentiamo infine come corollario un risultato di Bond [1], che useremo nel prossimo capitolo.

Corollario 4.20. *Sia E_K il gruppo delle unità di un campo di numeri K e sia r l'ℓ-rango di E/E^ℓ. Se l'Hilbert ℓ-class field tower di K è abeliana, cioè se $L_\ell(K) \leq 1$, allora*

$$\operatorname{rank} \mathrm{Cl}_\ell(K) \leq \frac{1+\sqrt{1+8r}}{2}.$$

Dimostrazione. Supponiamo che l'Hilbert ℓ-class field tower termini con K^1. Allora, per la proposizione 4.19,

$$\mathcal{M} = \mathcal{M}(\mathrm{Gal}(K^1/K)) \cong E_K/N_K^{K^1} E_{K^1}$$

e dunque $\mathcal{M}$ ha ℓ-rango minore o uguale a r. D'altra parte, per la proposizione 4.11, l'ℓ-rango di $\mathcal{M}$ è esattamente $\binom{s}{2}$, dove s è l'ℓ-rango di $\mathrm{Cl}_\ell(K)$. Perciò

$$\frac{s(s-1)}{2} \leq r,$$

cioè $(2s-1)^2 \leq 1+8r$, da cui, estraendo le radici quadrate, otteniamo la tesi. □

Capitolo 5

Estensioni assolute cicliche di grado ℓ

Oggetto di studio di questo capitolo sono le estensioni assolute cicliche di grado primo dispari ℓ, cioè le estensioni algebriche di $\mathbb{Q}$ di grado ℓ con gruppo di Galois ciclico.

5.1 Gruppi abeliani

La struttura dei gruppi abeliani è ben nota, in particolare vale il seguente teorema.

Teorema 5.1 (Decomposizione di Kronecker)**.** *Ogni gruppo abeliano finito G può essere scritto come somma diretta di gruppi ciclici di ordine potenza di un numero primo, cioè*

$$G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{n_r}\mathbb{Z},$$

con $p_1, \ldots, p_r$ primi e $r, n_1, \ldots, n_r$ naturali.

Definizione 5.2 (Gruppo Duale)**.** Sia G un gruppo abeliano finito. Definiamo *gruppo duale* di G e lo indichiamo con $G\widehat{\ }$ il gruppo moltiplicativo degli omomorfismi da G in $\mathbb{C}^*$.

Teorema 5.3. *Sia G un gruppo abeliano finito. Allora il gruppo duale $G\widehat{\ }$ è isomorfo, in modo non canonico, a G.*

Ricordiamo ora la definizione di p^n-rango di un gruppo abeliano finitamente generato.

Definizione 5.4 (p^n-rango)**.** Sia G un gruppo abeliano finitamente generato. Per ogni numero primo p e per ogni intero positivo n, definiamo *p^n-rango* di G e lo indichiamo con $\mathrm{rank}_{p^n}(G)$ il numero di addendi di ordine multiplo di p^n nella decomposizione di Kronecker di G.

Esistono altre definizioni equivalenti per il rango. Riportiamo qui quella di Gerth [6].

Osservazione 5.5. *Sia G un gruppo abeliano finito e sia S il suo p-sottogruppo di Sylow. Allora*

$$\mathrm{rank}_p\, S = \dim_{F_p}(S \otimes_{\mathbb{Z}_p} F_p),$$

dove F_p è il campo finito di p elementi e $\mathbb{Z}_p$ è l'anello degli interi p-adici.

Definizione 5.6 (Gruppo abeliano elementare)**.** Un *gruppo abeliano elementare* è un gruppo abeliano finito nel quale tutti gli elementi diversi dall'identità hanno lo stesso ordine.

Notiamo immediatamente che in un gruppo abeliano elementare l'ordine di ogni elemento diverso dall'identità deve essere un numero primo p e quindi ogni gruppo abeliano elementare è un p-gruppo. Inoltre possiamo considerare ogni p-gruppo abeliano elementare come uno spazio vettoriale su F_p. In particolare, se G è un gruppo abeliano finitamente generato, allora G/pG è un gruppo abeliano elementare, in quanto l'ordine di ogni elemento di G/pG è un divisore di p.

Osservazione 5.7. *Sia G un gruppo abeliano finitamente generato. Allora* $\mathrm{rank}_p(G)$ *è la dimensione dello spazio vettoriale G/pG su F_p e dunque*

$$\mathrm{rank}_p(G) = \log_p(|G/pG|).$$

5.2 G-moduli

In questa sezione studiamo l'azione di un gruppo ciclico G di ordine un primo dispari ℓ su un gruppo abeliano A con l'intento di ricavare delle informazioni sull'ℓ-rango di A. L'idea è di applicare poi questi risultati con G gruppo di Galois di un'estensione algebrica K di $\mathbb{Q}$ e con A gruppo delle classi di ideali di K.

I risultati qui esposti sono dovuti a Gras [8], Cornell [3] e Inaba [11].

Lemma 5.8. *Sia $G =< \sigma >$ un gruppo ciclico di ordine un primo dispari ℓ e sia A un G-modulo tale che l'elemento norma $N = 1 + \sigma + \ldots + \sigma^{\ell-1}$ appartenga all'annullatore di A, cioè tale che $NA = 0$. Allora*

$$A^\ell = A^{(1-\sigma)^{\ell-1}},$$

dove abbiamo posto $A^\ell = \{x^\ell | x \in A\}$ e $A^{(1-\sigma)^{\ell-1}} = \{x^{(1-\sigma)^{\ell-1}} | x \in A\}$.

Dimostrazione. A è un G-modulo e quindi anche un modulo su $\mathbb{Z}[G]$. Dal momento che N annulla A, possiamo considerare A come un $\mathbb{Z}[G]/N$-modulo, cioè come un modulo su $\mathbb{Z}[\zeta_\ell]$, dove ζ_ℓ è una radice ℓ-esima primitiva dell'unità; infatti $1 + \zeta_\ell + \ldots + \zeta_\ell^{\ell-1} = 0$. In $\mathbb{Z}[\zeta_\ell]$ l'ideale (ℓ) è uguale all'ideale $(1 - \zeta_\ell)^{\ell-1}$ e quindi, poiché σ agisce su A esattamente come agisce ζ_ℓ, otteniamo la tesi. □

Sia A un G-modulo e sia $x \in A^{(1-\sigma)^i}$. Consideriamo l'applicazione

$$1-\sigma : A^{(1-\sigma)^{i-1}} \to A^{(1-\sigma)^i}$$

tale che $x \mapsto x^{1-\sigma}$. Passando a quoziente otteniamo una mappa

$$1-\sigma : A^{(1-\sigma)^{i-1}}/A^{(1-\sigma)^i} \to A^{(1-\sigma)^i}/A^{(1-\sigma)^{i+1}},$$

dato che $(A^{(1-\sigma)^i})^{1-\sigma} = A^{(1-\sigma)^{i+1}}$. Notiamo inoltre che, per lo stesso motivo, questa mappa è surgettiva. Abbiamo perciò costruito una successione di funzioni surgettive:

$$A/A^{1-\sigma} \to A^{1-\sigma}/A^{(1-\sigma)^2} \to \cdots \to A^{(1-\sigma)^{\ell-2}}/A^{(1-\sigma)^{\ell-1}} \to \cdots .$$

Nel caso in cui A sia un ℓ-gruppo abeliano finito, possiamo concludere la successione con 1:

$$A/A^{1-\sigma} \to A^{1-\sigma}/A^{(1-\sigma)^2} \to \cdots \to A^{(1-\sigma)^{\ell-2}}/A^{(1-\sigma)^{\ell-1}} \to \cdots \to 1,$$

visto che

$$(1-\sigma)^\ell \equiv 0 \mod \ell\mathbb{Z}[G]$$

e dunque $1 = A^{(1-\sigma)^i}$ se i è sufficientemente grande.

Proposizione 5.9. *Sia G un gruppo ciclico di ordine un primo dispari ℓ, sia σ un generatore di G e sia A un G-modulo. Allora*

(i) $\operatorname{rank}_\ell A \leq \ell \operatorname{rank}_\ell(A/A^{1-\sigma})$.

(ii) Se la norma appartiene all'annullatore di A, allora

$$\operatorname{rank}_\ell(A) \leq (\ell-1)\operatorname{rank}_\ell(A/A^{1-\sigma}).$$

(iii) Supponendo che la norma appartenga all'annullatore di A e che inoltre A contenga un elemento di ordine ℓ^2, allora $\operatorname{rank}_\ell(A) \geq \ell - 1$.

Dimostrazione. Consideriamo, come abbiamo visto prima, la successione di funzioni surgettive

$$A/A^{1-\sigma} \to A^{1-\sigma}/A^{(1-\sigma)^2} \to \cdots \to A^{(1-\sigma)^{\ell-2}}/A^{(1-\sigma)^{\ell-1}} \to \cdots . \tag{5.1}$$

La surgettività implica che, per ogni $i \geq 0$,

$$|A/A^{1-\sigma}| \geq |A^{(1-\sigma)^i}/A^{(1-\sigma)^{i+1}}|.$$

Se la norma appartiene all'annullatore di A, dal lemma 5.8 ricaviamo che

$$A^\ell = A^{(1-\sigma)^{\ell-1}}.$$

Vale pertanto la seguente successione di inclusioni:

$$A^\ell = A^{(1-\sigma)^{\ell-1}} \subseteq A^{(1-\sigma)^{\ell-2}} \subseteq \cdots A^{1-\sigma} \subseteq A.$$

Ora A/A^ℓ è un gruppo abeliano elementare e quindi, per $0 \leq i \leq \ell - 1$, anche $A^{(1-\sigma)^i}/A^{(1-\sigma)^{i+1}}$ è un gruppo abeliano elementare visto che è un sottogruppo di A/A^ℓ. Dal fatto che $\operatorname{rank}_\ell A = \log_\ell |A/A^\ell|$ e che

$$|A/A^\ell| = |A/A^{1-\sigma}||A^{1-\sigma}/A^{(1-\sigma)^2}| \cdots |A^{(1-\sigma)^{\ell-2}}/A^{(1-\sigma)^{\ell-1}}|,$$

segue che

$$\operatorname{rank}_\ell A = \operatorname{rank}_\ell(A/A^{1-\sigma}) + \cdots + \operatorname{rank}_\ell(A^{(1-\sigma)^{\ell-2}}/A^{(1-\sigma)^{\ell-1}})$$

e quindi il punto (ii).

L'esistenza di un elemento di A di ordine ℓ^2 implica che $A^{(1-\sigma)^{\ell-1}}/A^{(1-\sigma)^\ell} \neq 1$. Per la surgettività delle funzioni nella successione 5.1 abbiamo che, per $0 \leq i \leq \ell-1$,

$$|A^{(1-\sigma)^i}/A^{(1-\sigma)^{i+1}}| \geq |A^{(1-\sigma)^{\ell-1}}/A^{(1-\sigma)^\ell}| \geq \ell$$

e quindi (iii).

Per dimostrare il punto (i) osserviamo che il modulo $A^{(1-\sigma)^\ell}$ è annullato dalla norma, così che possiamo applicare il lemma precedente 5.8. Abbiamo allora che

$$A^{(1-\sigma)^\ell} = (A^{(1-\sigma)})^{(1-\sigma)^{(\ell-1)}} = (A^{(1-\sigma)})^\ell \subseteq A^\ell.$$

Esiste perciò una mappa surgettiva $A/A^{(1-\sigma)^\ell} \to A/A^\ell$. Dal momento che

$$\operatorname{rank}_\ell A \geq \operatorname{rank}_\ell(A/A^{(1-\sigma)^\ell}) \geq \operatorname{rank}_\ell(A/A^\ell) = \operatorname{rank}_\ell A,$$

ricaviamo l'uguaglianza $\operatorname{rank}_\ell = \operatorname{rank}_\ell(A/A^{(1-\sigma)^\ell})$. Il risultato segue ora dalla stessa dimostrazione del punto (ii), fatta eccezione per il fatto che la filtrazione è in questo caso di ℓ passi. □

5.3 Genus field

Un modo per studiare le proprietà dell'Hilbert class field è quello di considerare sottoestensioni più semplici come, ad esempio, il genus field.

Definizione 5.10 (Genus field, genus number e genus group)**.** Siano F e K due campi di numeri tali che $F \subset K$. Chiamiamo *genus field* di K rispetto a F e lo indichiamo con K_F^* o con K_g, qualora sia evidente il campo F cui facciamo riferimento, la massima estensione abeliana non ramificata di K che sia della forma KF^*, con F^* estensione abeliana di F. Definiamo inoltre *genus number* il grado dell'estensione $[K_F^*/K]$ e *genus group* il gruppo di Galois $\mathrm{Gal}(K_F^*/K)$. Nel caso in cui abbiamo $F = \mathbb{Q}$ parliamo rispettivamente di absolute genus field, absolute genus number e absolute genus group.

Determinare il genus field richiede spesso risultati di class field, come ad esempio in [12], ma in alcuni casi è sufficiente usare la teoria della ramificazione di Hilbert. La dimostrazione del prossimo teorema è di Zhang [30] e non usa argomenti di class field.

Teorema 5.11. *Sia K un'estensione assoluta abeliana di grado ℓ^s, con ℓ un primo dispari e $s \geq 1$. Allora il genus field di K è*

$$K_g = K \prod_{p \neq \ell} C_p = \prod_p C_p,$$

dove $p \in \mathbb{N}$ corre tra i primi che ramificano in K, $e(p)$ è l'indice di ramificazione di p in $K/\mathbb{Q}$, C_p, con $p \neq \ell$, è l'unico sottocampo di grado $e(p)$ di $\mathbb{Q}(\zeta_p)$ e C_ℓ è il sottocampo di grado $e(\ell)$ di $\mathbb{Q}(\zeta_{\ell^t})$ per qualche $t \in \mathbb{N}$ sufficientemente grande.

Dimostrazione. Il campo C_ℓ è ben definito in quanto $e(\ell)|\ell^s$. Osserviamo che anche il campo C_p, con $p \neq \ell$, è ben definito. Infatti, dal momento che K è un'estensione abeliana di $\mathbb{Q}$, per il teorema di Kronecker-Weber esiste $m \in \mathbb{N}$ tale che $K \subseteq \mathbb{Q}(\zeta_m)$. Se a è tale che $p^a \| m$, allora, per il teorema 3.6, l'indice di ramificazione di p in $\mathbb{Q}(\zeta_m)$ è $p^{a-1}(p-1)$ e dunque $e(p)|(p^{a-1}(p-1), l^s)$. Pertanto otteniamo che $e(p)|p-1$ e quindi il campo C_p è ben definito.

Sia K' il campo di inerzia di p, con $p \neq \ell$, in KC_p. Vogliamo dimostrare che

$$KC_p = K'C_p.$$

Siano perciò E e E_1 rispettivamente il gruppo di inerzia e il primo gruppo di ramificazione di p in KC_p. Sappiamo che E/E_1 è ciclico e che E_1 è un p-gruppo. Poiché però $|E_1|$ divide $[KC_p : \mathbb{Q}]$ che è una potenza di ℓ, abbiamo che $|E_1| = 1$ e quindi E è ciclico di ordine $|E| \geq |E_K| = e(p)$. D'altra parte osserviamo che la mappa di restrizione $\sigma \mapsto (\sigma_{C_p}, \sigma_K)$ definisce un'immersione $E \to E_{C_p} \times E_K$, dove con E_{C_p} e E_K indichiamo i gruppi di inerzia di p in C_p e in K. Perciò E non ha elementi di ordine maggiore di $e(p)$, da cui ricaviamo che $|E| = e(p)$. Dal momento che $K' \cap C_p = \mathbb{Q}$, segue che

$$[K'C_p : \mathbb{Q}] = [K' : \mathbb{Q}][C_p : \mathbb{Q}] = [K' : \mathbb{Q}]e(p) = [K' : \mathbb{Q}][KC_p : K'] = [KC_p : \mathbb{Q}]$$

e quindi $KC_p = K'C_p$. Osserviamo che p è chiaramente non ramificato in K' e che l'indice di ramificazione di ogni primo $q \neq p$ in K' è $e(q)$. Possiamo quindi procedere in maniera analoga per un primo $q \neq p, \ell$ ed il gruppo $K'C_q$ e ottenere $K'C_q = K''C_q$; dunque $KC_pC_q = K''C_pC_q$. Iterando su tutti i primi $p_i \neq \ell$ che ramificano in K ricaviamo

$$KC_{p_1}C_{p_2}\cdots C_{p_r} = K^{(r)}C_{p_1}C_{p_2}\cdots C_{p_r}, \tag{5.2}$$

dove ogni p_i è non ramificato in $K^{(r)}$. Per il teorema di Kronecker-Weber abbiamo allora che $K^{(r)} = C_\ell$. Notiamo che per trovare l'equazione 5.2 le uniche proprietà di K che abbiamo usato sono state il fatto che l'indice di ramificazione di p in K fosse $e(p)$ e che $[K : \mathbb{Q}]$ fosse una potenza di ℓ. Anche il genus field K_g di K soddisfa queste due proprietà in quanto K_g/K è un'estensione non ramificata. Infatti se un primo $q \neq \ell$ divide $[K_g : \mathbb{Q}]$, allora K_g ha un sottocampo di grado q. Consideriamo un primo p che ramifica in questo campo. Troviamo allora una contraddizione poiché $q|e(p)|l^s$. Pertanto, come nel caso di K, vale l'equazione

$$K_gC_{p_1}C_{p_2}\cdots C_{p_r} = C_\ell C_{p_1}C_{p_2}\cdots C_{p_r} = L, \tag{5.3}$$

dunque $K_g \subseteq L$. D'altra parte l'indice di ramificazione di p_i in $L/\mathbb{Q}$ è $[C_{p_i} : \mathbb{Q}] = e(p_i)$ e quindi L/K è un'estensione non ramificata al finito. Inoltre L/K è non ramificata anche all'infinito dato che $[L : \mathbb{Q}]$, essendo uguale ad una potenza di ℓ, è dispari e quindi $L \in \mathbb{R}$. Perciò $L \subseteq K_g$ ed abbiamo così la tesi. □

Corollario 5.12. *Sia K è un'estensione ciclica di $\mathbb{Q}$ di grado un primo dispari ℓ. Allora il genus field di K è*

$$K_g = C_\ell C_{p_1}\cdots C_{p_r} = KC_{p_1}\cdots C_{p_r},$$

dove C_{p_i} è l'unico sottocampo di grado ℓ di $\mathbb{Q}(\zeta_{p_i})$, C_ℓ è l'unico sottocampo di grado ℓ di $\mathbb{Q}(\zeta_\ell)$ se ℓ è ramificato, altrimenti $C_\ell = \mathbb{Q}$ e $p_1, \ldots, p_r$ sono tutti i primi diversi da ℓ che ramificano in K.

Dimostrazione. L'indice di ramificazione è necessariamente ℓ per ogni primo ramificato. Applicando il teorema 5.11 otteniamo immediatamente la tesi. □

Abbiamo appena visto che il genus field K_g di un'estensione ciclica $K/\mathbb{Q}$ di grado un primo dispari ℓ è il composto di estensioni cicliche di $\mathbb{Q}$ di grado ℓ. Possiamo quindi ricavare la struttura dei gruppi di Galois delle estensioni K_g/K e $K_g/\mathbb{Q}$.

Osservazione 5.13. *Sia K è un'estensione ciclica di $\mathbb{Q}$ di grado un primo dispari ℓ. Se t è il numero di primi che ramificano in K, abbiamo allora che*

$$\mathrm{Gal}(K_g/\mathbb{Q}) \cong (\mathbb{Z}/\ell\mathbb{Z})^t.$$

Inoltre, poiché tutti i sottogruppi di $(\mathbb{Z}/\ell\mathbb{Z})^t$ *di cardinalità* ℓ^{t-1} *sono isomorfi a* $(\mathbb{Z}/\ell\mathbb{Z})^{t-1}$,

$$\mathrm{Gal}(K_g/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^{t-1}$$

e dunque $\mathrm{rank}_\ell \mathrm{Gal}(K_g/K) = t-1$.

Sia K un'estensione ciclica di F e sia σ un generatore di $\mathrm{Gal}(K/F)$. Vale allora la successione esatta

$$1 \to \mathrm{Gal}(K^1/K) \to \mathrm{Gal}(K^1/F) \to \mathrm{Gal}(K/F) \to 1.$$

Sia z_σ un elemento del gruppo $\mathrm{Gal}(K^1/F)$ che si proietta su σ. Consideriamo la mappa $\psi : \mathrm{Gal}(K^1/K) \to \mathrm{Gal}(K^1/K)$ tale che

$$\psi(\mu) = z_\sigma \mu z_\sigma^{-1}, \quad \mu \in \mathrm{Gal}(K^1/K).$$

Osserviamo che questa mappa è indipendente dalla scelta di z_σ. Infatti, se $z_\sigma, \hat{z}_\sigma \in \mathrm{Gal}(K^1/F)$ si proiettano entrambi su σ, allora $\hat{z}_\sigma^{-1} z_\sigma$ e $z_\sigma^{-1}\hat{z}_\sigma$ sono automorfismi del gruppo $\mathrm{Gal}(K^1/K)$, in quanto appartengono al nucleo della proiezione di $\mathrm{Gal}(K^1/F)$ su $\mathrm{Gal}(K/F)$. D'altra parte, per definizione di Hilbert class field, il gruppo $\mathrm{Gal}(K^1/K)$ è abeliano e quindi

$$\hat{z}_\sigma^{-1} z_\sigma \mu z_\sigma^{-1} \hat{z}_\sigma = \hat{z}_\sigma^{-1} z_\sigma z_\sigma^{-1} \hat{z}_\sigma \mu = \mu,$$

cioè la mappa è indipendente dalla scelta del rappresentante z_σ:

$$z_\sigma \mu z_\sigma^{-1} = \hat{z}_\sigma \mu \hat{z}_\sigma^{-1}.$$

Quanto abbiamo appena dimostrato definisce chiaramente un'azione del gruppo $\mathrm{Gal}(K/F)$ su $\mathrm{Gal}(K^1/K)$ data dalla funzione $\sigma^i \mapsto \psi^i$, con $i \in \mathbb{N}$. Questa azione corrisponde all'azione naturale di $\mathrm{Gal}(K/F)$ su $\mathrm{Cl}(K)$, quando indentifichiamo $\mathrm{Cl}(K)$ con $\mathrm{Gal}(K^1/K)$.

Proposizione 5.14. *Sia* K/F *un'estensione normale di campi di numeri e sia* F^* *il campo fissato dal sottogruppo dei commutatori di* $\mathrm{Gal}(K^1/F)$. *Vale allora* $K_F^* = KF^*$.

Dimostrazione. Dato che F^* è il campo fissato dal sottogruppo dei commutatori di $\mathrm{Gal}(K^1/F)$, F^* contiene tutte le estensioni abeliane di F contenute in K^1. Inoltre, poiché $K \subseteq KF^* \subseteq K^1$, EF^* è non ramificata su K e quindi otteniamo la tesi. □

Proposizione 5.15. *Sia* K *un'estensione ciclica di* F *e sia* σ *un generatore di* $\mathrm{Gal}(K/F)$. *Allora grazie alla mappa di Artin otteniamo*

$$\mathrm{Gal}(K_F^*/K) \cong \mathrm{Cl}(K)/\mathrm{Cl}(K)^{1-\sigma}.$$

Dimostrazione. Per la proposizione 5.14 è sufficiente dimostrare che il sottogruppo dei commutatori di $\mathrm{Gal}(K^1/F)$ è isomorfo a $\mathrm{Cl}(K)^{1-\sigma}$. Dal momento che l'estensione K/F è ciclica e dunque abeliana, il sottogruppo dei commutatori di $\mathrm{Gal}(K^1/F)$ è contenuto in $\mathrm{Gal}(K^1/K)$. Per quando abbiamo appena dimostrato il gruppo $\mathrm{Gal}(K/F)$ agisce per coniugio su $\mathrm{Gal}(K^1/K)$. Consideriamo dunque un commutatore $aba^{-1}b^{-1} \in \mathrm{Gal}(K^1/F)$. Chiaramente esistono $\alpha, \beta \in \mathrm{Gal}(K^1/K)$ e $z_\sigma^i, z_\sigma^j \in \mathrm{Gal}(K^1/F)$ tali che $a = z_\sigma^i \alpha$ e $b = z_\sigma^j \beta$; perciò:

$$\begin{aligned} aba^{-1}b^{-1} &= z_\sigma^i \alpha z_\sigma^j \beta \alpha^{-1} (z_\sigma^i)^{-1} \beta^{-1} (z_\sigma^j)^{-1} \\ &= z_\sigma^i \alpha (z_\sigma^i)^{-1} z_\sigma^i z_\sigma^j \beta \alpha^{-1} (z_\sigma^i)^{-1} (z_\sigma^j)^{-1} z_\sigma^j \beta^{-1} (z_\sigma^j)^{-1} \\ &= \psi^i(\alpha) \psi^{i+j}(\beta\alpha^{-1}) \psi^j(\beta^{-1}). \end{aligned}$$

Per comodità usiamo la notazione esponenziale per indicare l'azione di $\mathrm{Gal}(K/F)$ su $\mathrm{Gal}(K^1/K)$:

$$\alpha^\sigma = z_\sigma \alpha z_\sigma^{-1} = \psi(\alpha).$$

Otteniamo così

$$aba^{-1}b^{-1} = \alpha^{\sigma^i} \beta^{\sigma^{i+j}} (\alpha^{-1})^{\sigma^{i+j}} (\beta^{-1})^{\sigma^j} = ((\alpha)^{\sigma^i})^{1-\sigma^j} ((\beta^{-1})^{\sigma^j})^{1-\sigma^i}.$$

Osserviamo ora che

$$(((\alpha)^{\sigma^i})^{1+\sigma+\cdots+\sigma^{j-1}})^{1-\sigma} = ((\alpha)^{\sigma^i})^{1-\sigma^j} = \alpha^{\sigma^i} \alpha^{-\sigma^{i+j}}$$

e che, analogamente,

$$(((\beta^{-1})^{\sigma^j})^{1+\sigma+\cdots+\sigma^{i-1}})^{1-\sigma} = ((\beta^{-1})^{\sigma^j})^{1-\sigma^i} = \beta^{-\sigma^j} \beta^{\sigma^{i+j}}.$$

Abbiamo così dimostrato che $aba^{-1}b^{-1} \in \mathrm{Cl}(K)^{1-\sigma}$, cioè $\mathrm{Gal}(K^1/F)' \subseteq \mathrm{Cl}(K)^{1-\sigma}$. Per dimostrare invece il contenimento inverso è sufficiente utilizzare la precedente relazione con $i = 1$, $j = 0$ e $\alpha = e$ e ottenere $(\beta^{-1})^{1-\sigma} = (\beta)^\sigma \beta^{-1} = z_\sigma \beta z_\sigma^{-1} \beta^{-1}$, cioè $\mathrm{Cl}(K)^{1-\sigma} \subseteq \mathrm{Gal}(K^1/F)'$. □

5.4 Disuguaglianze sul rango del gruppo delle classi

Il prossimo risultato è dovuto a Leopoldt [19] e a Moriya [21].

Proposizione 5.16. *Sia K un'estensione ciclica di $\mathbb{Q}$ di grado primo dispari ℓ. Se ramificano in K esattamente t primi, allora*

$$t - 1 \leq \operatorname{rank} \mathrm{Cl}_\ell(K) \leq (\ell - 1)(t - 1).$$

Dimostrazione. Sia G il gruppo di Galois dell'estensione $K/\mathbb{Q}$ e sia σ un suo generatore. L'azione naturale di G su $\mathrm{Cl}(K)$ rende $\mathrm{Cl}(K)$ un G-modulo. Inoltre, poiché $\mathrm{Cl}(\mathbb{Q}) = 1$, la norma N di un qualunque ideale di K è un ideale principale e quindi N appartiene all'annullatore di $\mathrm{Cl}(K)$. Siamo perciò nelle ipotesi della proposizione 5.9; applicandola dal punto (ii) otteniamo che

$$\mathrm{rank}_\ell(\mathrm{Cl}(K)) \leq (\ell - 1)\,\mathrm{rank}_\ell(\mathrm{Cl}(K)/\,\mathrm{Cl}(K)^{1-\sigma}).$$

Chiaramente $\mathrm{rank}_\ell(\mathrm{Cl}(K)) = \mathrm{rank}_\ell(\mathrm{Cl}_\ell(K))$. Dalla proposizione 5.15 sappiamo che

$$\mathrm{Gal}(K_g/K) \cong \mathrm{Cl}(K)/\,\mathrm{Cl}(K)^{1-\sigma},$$

mentre per l'osservazione 5.13 abbiamo che $\mathrm{rank}_\ell \mathrm{Gal}(K_g/K) = t - 1$. Ricaviamo pertanto che

$$\mathrm{rank}\,\mathrm{Cl}_\ell(K) \leq (\ell - 1)(t - 1).$$

L'altra parte della disuguaglianza segue dal fatto che, sempre per l'osservazione 5.13, $\mathrm{Gal}(K_g/K) \cong (\mathbb{Z}/\ell\mathbb{Z})^{t-1}$, cioè esiste un'estensione abeliana non ramificata di K con gruppo di Galois isomorfo a $(\mathbb{Z}/\ell\mathbb{Z})^{t-1}$ e quindi, per il teorema 2.24, $(\mathbb{Z}/\ell\mathbb{Z})^{t-1}$ è un sottogruppo di $\mathrm{Cl}(K)$. □

Vediamo ora come è possibile migliorare la stima sull'ℓ-rango del gruppo $\mathrm{Cl}_\ell(K)$ se assumiamo che $\mathrm{Cl}_\ell(K)$ contenga un elemento di ordine ℓ^2.

Proposizione 5.17. *Sia K un'estensione ciclica di $\mathbb{Q}$ di grado un primo dispari ℓ e sia $t \geq 2$. Se ramificano in K esattamente t primi e il gruppo $\mathrm{Cl}_\ell(K)$ contiene un elemento di ordine ℓ^2, allora*

$$\mathrm{rank}\,\mathrm{Cl}_\ell(K) \geq t + \ell - 3.$$

Dimostrazione. Per gli stessi motivi descritti nella dimostrazione della proposizione 5.16 osserviamo che

$$\mathrm{rank}_\ell(\mathrm{Cl}(K)/\,\mathrm{Cl}(K)^{1-\sigma}) = t - 1 \tag{5.4}$$

e che possiamo applicare anche qui la proposizione 5.9. Dal punto (iii) di quest'ultima proposizione ricaviamo che

$$\mathrm{rank}\,\mathrm{Cl}_\ell(K) \geq (\ell - 1).$$

Riguardando però la dimostrazione di questa disuguaglianza, notiamo che possiamo migliorare la stima. Conosciamo infatti con precisione il rango di $\mathrm{Cl}(K)/\,\mathrm{Cl}(K)^{1-\sigma}$, che è maggiore di 0 poiché $t \geq 2$ ed inoltre, dal fatto che $\mathrm{Cl}_\ell(K)$ contiene un elemento di ordine ℓ^2, sappiamo che, per $1 \leq i \leq \ell - 1$,

$$\mathrm{rank}(\mathrm{Cl}(K)^{(1-\sigma)^i}/\,\mathrm{Cl}(K)^{(1-\sigma)^{i+1}}) \geq 1.$$

Ricaviamo pertanto che

$$\operatorname{rank}_\ell \operatorname{Cl}(K) = \operatorname{rank} \operatorname{Cl}_\ell(K) \geq t - 1 + 1 \cdot (\ell - 2) = t - \ell - 3.$$

□

Siamo finalmente in grado di dare una nuova dimostrazione del teorema di Nomura [23].

Teorema 5.18. *Sia K un campo ciclico cubico tale che esattamente 3 primi razionali ramificano in K. Sono allora equivalenti le seguenti due condizioni:*

(i) la lunghezza dell'Hilbert class field tower di K è maggiore di 1, cioè $L_3(K) > 1$;

(ii) il numero delle classi di ideali del genus field K_g di K è divisibile per 3.

Dimostriamo separatamente le due implicazioni.

Dimostrazione $(i) \Rightarrow (ii)$. Per comodità consideriamo due casi differenti, a seconda che il genus field K_g coincida o no con l'Hilbert 3-class field K_3^1.

Se $K_g = K_3^1$, allora, per il teorema 2.24, sappiamo che $\operatorname{Gal}(K_3^2/K_3^1) \cong \operatorname{Cl}_3(K_3^1)$. Poiché, per ipotesi, l'Hilbert class field tower di K è strettamente maggiore di 1, allora K_3^2 è un'estensione abeliana non ramificata e non banale di K_3^1, cioè $|\operatorname{Gal}(K_3^2/K_3^1)| > 1$. Avendo supposto $K_g = K_3^1$, ricaviamo che $|\operatorname{Cl}_3(K_g)| > 1$ e dunque $3|\operatorname{Cl}_3(K_g)$.

Se $K_g \neq K_3^1$, allora, per definizione di Hilbert 3-class field, K_3^1 è la massima 3-estensione abeliana non ramificata di K. Dato che il genus field, per l'osservazione 5.13, è una 3-estensione abeliana non ramificata di K, allora $K \subseteq K_g \subsetneq K_3^1$, dove il secondo contenimento è stretto poiché abbiamo inoltre supposto $K_g \neq K_3^1$. K_3^1 è pertanto un'estensione abeliana non ramificata non banale di K, visto che lo è di K_g, e quindi $3|\operatorname{Cl}_3(K_g)$. □

Dimostrazione $(ii) \Rightarrow (i)$. Se $K_g = K_3^1$ la tesi è ovvia; possiamo pertanto supporre che $K_g \neq K_3^1$. Applicando la proposizione 5.16 con $\ell = 3$ e $t = 3$ otteniamo un'ottima stima sul 3-rango del gruppo delle classi, in particolare vale che

$$2 \leq \operatorname{rank} \operatorname{Cl}_3(K) \leq 4.$$

Osserviamo inoltre che, per il teorema 3.16 di Dirichlet, $E_K/E_K^3 \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Il corollario 4.20 pertanto afferma che se l'Hilbert 3-class field tower di K è abeliana, allora

$$\operatorname{rank} \operatorname{Cl}_3(K) \leq \frac{1 + \sqrt{1 + 8 \cdot 2}}{2} \approx 2,56,$$

cioè $\operatorname{rank} \mathrm{Cl}_3(K) \leq 2$, visto che che stiamo lavorando con numeri interi. Questo significa che il corollario 4.20 implica immediatamente la condizione (i) se $\operatorname{rank} \mathrm{Cl}_3(K) \geq 2$. Resta perciò da considerare soltanto il caso in cui $\operatorname{rank} \mathrm{Cl}_3(K)$ sia uguale a 2. Per ipotesi esattamente 3 primi razionali ramificano in K e dunque, per l'osservazione 5.13, sappiamo che

$$\mathrm{Gal}(K_g/K) \cong (\mathbb{Z}/3\mathbb{Z})^2,$$

dove σ è un generatore dell'estensione $K/\mathbb{Q}$. Poiché abbiamo supposto $K_g \neq K_3^1$, il gruppo di Galois di $\mathrm{Gal}(K_3^1/K) \cong \mathrm{Cl}_3(K)$ deve avere cardinalità maggiore o uguale a 27. Inoltre, dal momento che $\operatorname{rank} \mathrm{Cl}_3(K) = 2$, $\mathrm{Cl}_3(K)$ contiene un elemento di ordine almeno 9. Utilizzando allora la disuguaglianza della proposizione 5.17 ricaviamo che $\operatorname{rank} \mathrm{Cl}_3(K) \geq 3$ e dunque un assurdo. □

Osservazione 5.19. *La validità della condizione (ii) del teorema 5.18, grazie ai risultati di Cornell e Rosen [4], è facilmente verificabile in quanto dipende dal rango di una certa matrice* 3×3 *a coefficienti in* $\mathbb{Z}/3\mathbb{Z}$.

Bibliografia

[1] Robert J. Bond, *Unramified abelian extensions of number fields*, J. Number Theory **30** (1988), no. 1, 1–10.

[2] John W. S. Cassels and Albrecht Fröhlich (eds.), *Algebraic number theory*, London and New York, London Mathematical Society with the support of the International Mathematical Union, Academic Press, 1967.

[3] Gary Cornell, *Relative genus theory and the class group of l-extensions*, Trans. Amer. Math. Soc. **277** (1983), no. 1, 421–429.

[4] Gary Cornell and Michael Rosen, *The class group of an absolutely abelian l-extension*, Illinois J. Math. **32** (1988), no. 3, 453–461.

[5] Yoshiomi Furuta, *On class field towers and the rank of ideal class groups*, Nagoya Math. J. **48** (1972), 147–157.

[6] Frank Gerth, III, *On 3-class groups of cyclic cubic extensions of certain number fields*, J. Number Theory **8** (1976), no. 1, 84–98.

[7] ———, *The ideal class groups of two cyclotomic fields*, Proc. Amer. Math. Soc. **78** (1980), no. 3, 321–322.

[8] Georges Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l. I, II*, Ann. Inst. Fourier (Grenoble) **23** (1973), no. 3, 1–48; ibid. **23** (1973), no. 4, 1–44.

[9] Helmut Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil Ia: Beweise zu Teil I*, Jber. Deutsch. Math.-Verein. **36** (1927), no. 36, 233–311.

[10] Kuniaki Horie, *On the exponents of ideal class groups of cyclotomic fields*, Proc. Amer. Math. Soc. **119** (1993), no. 4, 1049–1052.

[11] Eizi Inaba, *Über die Struktur der l-Klassengruppe zyklischer Zahlkörper vom Primzahlgrad l*, J. Fac. Sci. Imp. Univ. Tokyo. Sect. I. **4** (1940), 61–115.

[12] Makoto Ishida, *The genus fields of algebraic number fields*, Springer-Verlag, Berlin, 1976, Lecture Notes in Mathematics, Vol. 555.

[13] Kenkichi Iwasawa, *A note on the group of units of an algebraic number field*, J. Math. Pures Appl. (9) **35** (1956), 189–192.

[14] ———, *A note on ideal class groups*, Nagoya Math. J. **27** (1966), 239–247.

[15] Wolfram Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. **311/312** (1979), 215–254, In memoriam Arnold Scholz.

[16] Gregory Karpilovsky, *The Schur multiplier*, London Mathematical Society Monographs. New Series, vol. 2, Oxford University Press, New York, 1987.

[17] E.E. Kummer, *Über die aus 31sten Wurzeln der Einheit gebildeten complexen Zahlen*, Monatsberichte der Kön. Preuß. Ak. der Wiss. zu Berlin (1870), 755–766.

[18] Ernst E. Kummer, *Über die Irregularität von Determinanten*, Monatsberichte der Kön. Preuß. Ak. der Wiss. zu Berlin (1853), 194–200.

[19] Heinrich W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9** (1953), 351–362.

[20] Daniel A. Marcus, *Number fields*, Springer-Verlag, New York, 1977, Universitext.

[21] Mikao Moriya, *Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrad*, Japanese J. Math. **10** (1933), 1–18.

[22] Jürgen Neukirch, *Class field theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 280, Springer-Verlag, Berlin, 1986.

[23] Akito Nomura, *A note on the 3-class field tower of a cyclic cubic field*, Proc. Japan Acad. Ser. A Math. Sci. **83** (2007), no. 2, 14–15.

[24] Arnold Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen. II*, J. Reine Angew. Math. **182** (1940), 217–234.

[25] Issai Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **132** (1907), 85–137.

[26] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[27] Koichi Tateyama, *On the ideal class groups of some cyclotomic fields*, Proc. Japan Acad. Ser. A Math. Sci. **58** (1982), no. 7, 333–335.

[28] Frank J. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), no. 160, 693–707.

[29] Lawrence C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982.

[30] Xian Ke Zhang, *A simple construction of genus fields of abelian number fields*, Proc. Amer. Math. Soc. **94** (1985), no. 3, 393–395.