Università di Pisa

Dipartimento di Matematica
Corso di Laurea Triennale in Matematica

Primi della forma $x^2 + ny^2$

Candidato
Davide Pierrat

Relatore
Davide Lombardo

Anno Accademico 2023/2024

Indice

Indice **1**

Introduzione **4**

1 Preliminari **5**
1.1 Anelli degli interi 5
1.2 Estensione di ideali primi, ramificazione ed inerzia 5
1.3 Discriminante 7
1.4 Fattorizzazione e Teorema di Dedekind 7
1.5 Campi quadratici 8

2 Ordini in campi di numeri **9**
2.1 Definizioni e prime proprietà 9
2.2 Ideali invertibili e gruppo delle classi 10
2.3 Ideali coprimi con l'indice 12

3 Class Field Theory **17**
3.1 Primi non ramificati e simbolo di Artin 17
3.2 Gruppo di Galois di estensioni ciclotomiche 19
3.3 Legge di reciprocità quadratica 19
3.4 Class Field Theory 21
3.5 Class Field Theory per $K = \mathbf{Q}$ 24
3.6 Hilbert Class Field 25
3.7 Ring Class Field 26

4 Soluzione di $p = x^2 + ny^2$ **29**
4.1 Soluzione del problema 29
4.2 Qualche esempio 32
4.3 Condizioni di congruenza 33

Bibliografia **35**

Introduzione

In questa tesi studiamo il seguente problema. Fissato un intero $n > 0$, vogliamo capire quali numeri primi p possono essere espressi nella forma

$$p = x^2 + ny^2, \text{ con } x, y \in \mathbf{Z}.$$

Questo problema ha una storia molto lunga, ed è stato affrontato (almeno per valori particolari di n) da matematici illustri tra i quali Fermat, Eulero, Lagrande, Legendre e Gauss. Il caso di $n = 1$ è il più famoso, e la sua dimostrazione è dovuta a Fermat:

$$p = x^2 + y^2 \iff p = 2, \text{ oppure } p \equiv 1 \mod 4.$$

Osserviamo che se $p = x^2 + ny^2$, allora p deve ammettere $-n$ come residuo quadratico. Infatti

$$p = x^2 + ny^2 \implies \left(\frac{x}{y}\right)^2 \equiv -n \mod p.$$

Se per $n = 1$ questa condizione necessaria è anche sufficiente, ci si accorge presto che questo non si generalizza. Ad esempio, prendendo $n = 5$ e $p = 7$, abbiamo che $\left(\frac{-5}{7}\right) = 1$, ma 7 non è esprimibile come $x^2 + 5y^2$. Scopriremo nell'ultimo capitolo che

$$p = x^2 + 5y^2 \iff p = 5, \text{ oppure } p \equiv 1, 9 \mod 20.$$

Osserviamo che in questo caso, come per $n = 1$, essere esprimibile nella forma $x^2 + ny^2$ equivale a chiedere che p soddisfi una condizione di congruenza.

Vedremo anche che se $p \neq 2, 23$, allora

$$p = x^2 + 23y^2 \iff \begin{cases} \left(\frac{-23}{p}\right) = 1 \\ x^3 - x + 1 \text{ ha una radice modulo } p. \end{cases}$$

Si può dimostrare che non esiste un sistema lineare di congruenze che individua esattamente questi primi (anche ammettendo finite eccezioni). Questa forma di soluzione è generale. Dimostreremo infatti il seguente teorema.

Teorema *Per ogni intero $n > 0$ esiste un polinomio monico $f(x)$ a coefficienti interi tale che, se p è coprimo con 2, con n, e con il discriminante di $f(x)$, allora*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \\ f(x) \textit{ ha una radice modulo } p. \end{cases}$$

La dimostrazione di questo teorema farà uso di alcuni strumenti molto potenti, che vengono dalla Class Field Theory. Questa teoria studia e classifica le estensioni abeliane, ossia con gruppo di Galois abeliano, di campi locali e globali. Noi saremo interessati ai campi globali di caratteristica 0, ovvero le estensioni finite di $\mathbf{Q}$, anche chiamati campi di numeri.

Il caso più semplice è quello di $\mathbf{Q}$, per il quale i risultati ottenibili tramite la Class Field Theory sono essenzialmente equivalenti al teorema di Kronecker-Weber. Questo teorema afferma che ogni estensione abeliana di $\mathbf{Q}$ è contenuta in un campo ciclotomico $\mathbf{Q}(\zeta_n)$. Per gli altri campi di numeri, la descrizione delle estensioni abeliane è più complicata e più astratta: corrisponderanno a certi gruppi di ideali frazionari dell'anello degli interi del campo base.

Il campo di numeri a cui applicheremo i teoremi della Class Field Theory è $\mathbf{Q}(\sqrt{-n})$, nel quale $x^2 + ny^2$ si fattorizza come $(x + \sqrt{-n}y)(x - \sqrt{-n}y)$. Costruiremo una sua estensione abeliana L, il Ring Class Field dell'anello $\mathbf{Z}[\sqrt{-n}]$, le cui proprietà saranno essenziali per dimostrare il teorema di cui sopra.

La fonte principale da cui questa esposizione attinge è il testo *Primes of the form* $x^2 + ny^2$, di David A. Cox ([Cox22]).

Chapter 1

Preliminari

In questo capitolo richiamiamo alcuni strumenti e risultati che stanno alla base della teoria algebrica dei numeri, i quali verranno utilizzati nel seguito.

1.1 Anelli degli interi

Un **campo di numeri** è un'estensione di $\mathbf{Q}$ di grado finito.

Se K è un campo di numeri, il suo **anello degli interi** è la chiusura integrale di $\mathbf{Z}$ in K, e viene indicato con $\mathcal{O}_K$. In altre parole, $\mathcal{O}_K$ è il sottoanello di K formato dagli elementi di K il cui polinomio minimo su $\mathbf{Q}$ ha coefficienti in $\mathbf{Z}$.

Si può dimostrare che $\mathcal{O}_K$ è un **dominio di Dedekind** ([Mar18, Thm 14]). In altre parole, è un dominio noetheriano, di dimensione 1 (quindi gli $\mathcal{O}_K$-ideali primi non nulli sono massimali), ed è integralmente chiuso. Le due conseguenze principali sono che:

- le sue localizzazioni $(\mathcal{O}_K)_{\mathfrak{p}}$ sono anelli di valutazione discreta (o "DVR") per ogni $\mathfrak{p}$ ideale primo non nullo,
- ogni ideale non nullo di $\mathcal{O}_K$ si fattorizza unicamente come prodotto di ideali primi ([Mar18, Thm 16]).

Si può mostrare che $\mathcal{O}_K \cong \mathbf{Z}^{[K:\mathbf{Q}]}$ come $\mathbf{Z}$-modulo.

Inoltre se I è un ideale di $\mathcal{O}_K$, l'indice $[\mathcal{O}_K : I]$ è finito, ed è chiamato **norma** di I. Viene anche indicato con $\mathrm{N}(I)$.

In particolare se $\mathfrak{p}$ è un ideale primo, $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ è un campo finito, detto **campo residuo** del primo $\mathfrak{p}$.

Un **primo di** K è un ideale primo non nullo di $\mathcal{O}_K$.

Dati due ideali I, J di un dominio A, diremo che I **divide** J (e scriveremo $I|J$) se esiste un ideale H tale che $J = IH$.

1.2 Estensione di ideali primi, ramificazione ed inerzia

Sia ora L/K un'estensione di campi di numeri. Abbiamo un'inclusione $\mathcal{O}_K \subseteq \mathcal{O}_L$, e possiamo considerare la fattorizzazione di $\mathfrak{p}\mathcal{O}_L$ come ideale di $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}.$$

Proposizione 1.2.1 *[Mar18, Thm 19]*
Siano $\mathfrak{p}$ e $\mathfrak{P}$ primi di K e di L rispettivamente. Allora sono equivalenti:

- $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$
- *$\mathfrak{P}$ appare nella fattorizzazione di $\mathfrak{p}\mathcal{O}_L$*
- $\mathfrak{P} \supseteq \mathfrak{p}$
- $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

In tale caso, scriviamo $\mathfrak{P} \mid \mathfrak{p}$, e diremo che "$\mathfrak{P}$ sta sopra $\mathfrak{p}$", o che "$\mathfrak{p}$ sta sotto $\mathfrak{P}$".

Definiamo l'**indice di ramificazione** di $\mathfrak{P}_i|\mathfrak{p}$ tramite la formula $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$. In altre parole, è l'esponente con cui $\mathfrak{P}_i$ appare nella fattorizzazione dell'estensione di $\mathfrak{p}$.
Se $\mathfrak{P} \mid \mathfrak{p}$, poiché $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, abbiamo un'estensione $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ dei campi residui. Definiamo il **grado d'inerzia**, indicato con $f(\mathfrak{P}|\mathfrak{p})$, come il grado di questa estensione.

Proposizione 1.2.2 *[Mar18, Thm 21]*
Sia $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}$ come sopra. Allora

$$[L : K] = \sum_{i=1}^{r} e_i f_i,$$

dove e_i ed f_i sono gli indici di ramificazione e i gradi di inerzia.

Proposizione 1.2.3 *[Mar18, Ch 6]*
Sia L/K un'estensione di Galois. Allora, con la notazione della proposizione precedente, gli e_i sono tutti uguali ad un certo e, e gli f_i sono tutti uguali ad un certo f. In particolare,

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

Proposizione 1.2.4 (Moltiplicatività nelle torri di e ed f) *Sia $L/F/K$ una torre di estensioni di campi di numeri, e siano $\mathfrak{P}, P, \mathfrak{p}$ primi di L, F e K rispettivamente, tali che $\mathfrak{P} \mid P$ e $P \mid \mathfrak{p}$. Allora*

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

Diremo che un primo $\mathfrak{p}$ di K:

- è **ramificato** in L se $e_i > 1$ per qualche i,
- è **totalmente ramificato** in L se $e_i = [L : K]$ (equivalentemente, se c'è un solo primo sopra $\mathfrak{p}$ e il suo grado d'inerzia è 1)
- **spezza completamente** in L se $e_i = f_i = 1$ per ogni i (equivalentemente, ci sono $[L : K]$ primi sopra $\mathfrak{p}$).

Un corollario della moltiplicatività nelle torri è il seguente.

Proposizione 1.2.5 *Se $L/F/K$ è una torre di estensioni, e $\mathfrak{p}$ è un primo di K, allora*

- *$\mathfrak{p}$ non ramifica in $L \implies \mathfrak{p}$ non ramifica in F,*
- *$\mathfrak{p}$ è totalmente ramificato in $L \implies \mathfrak{p}$ è totalmente ramificato in F,*

- $\mathfrak{p}$ *spezza completamente in* $L \implies \mathfrak{p}$ *spezza completamente in* F.

La seguente proposizione è più difficile da dimostrare.
($\star$ teo 31 pg 76 marcus)

Proposizione 1.2.6 *[Mar18, Thm 31]*
Siano F_1, F_2 *due estensioni di* K. *Se un primo* $\mathfrak{p}$ *di* K *non ramifica in* F_1 *e in* F_2, *allora non ramifica nel composto* F_1F_2.

1.3 Discriminante

Dato $\alpha \in K$, la moltiplicazione per α è una mappa $\mathbf{Q}$-lineare da K in sé. Definiamo la **traccia** di α, indicata con $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha)$, come la traccia di questa mappa. Si mostra facilmente che se $\alpha \in \mathcal{O}_K$, allora $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) \in \mathbf{Z}$.

Definiamo il **discriminante** dell'anello $\mathcal{O}_K$ nel modo seguente. Se $\{e_1, \dots, e_n\}$ è una $\mathbf{Z}$-base di $\mathcal{O}_K$, allora

$$\mathrm{disc}(\mathcal{O}_K) = \det((\mathrm{Tr}_{K/\mathbf{Q}}(e_i e_j))_{i,j}) \in \mathbf{Z}.$$

Si può mostrare che questo intero non dipende dalla base scelta, ed è non nullo. ($\star$ Marcus teo 7 pg 18)

Se $A \subseteq \mathcal{O}_K$ è un sottogruppo anch'esso isomorfo a $\mathbf{Z}^{[K:\mathbf{Q}]}$, definiamo il suo discriminante allo stesso modo, usando questa volta una $\mathbf{Z}$-base di A. Il discriminante di A è legato a quello di $\mathcal{O}_K$ dalla formula

$$\mathrm{disc}(A) = [\mathcal{O}_K : A]^2 \mathrm{disc}(\mathcal{O}_K).$$

Con $\mathrm{disc}(K)$ si intende $\mathrm{disc}(\mathcal{O}_K)$.

Proposizione 1.3.1 (Criterio per la ramificazione) *[Mar18, Thm 24, Thm 34]*
Un primo di $\mathbf{Q}$ *ramifica in* K *se e solo se divide il discriminante* $\mathrm{disc}(K)$.

Corollario 1.3.2 *Sia* $K = \mathbf{Q}(\alpha)$, *dove* $\alpha \in \mathcal{O}_K$ *ha polinomio minimo* $f(x)$. *Allora se* p *è un primo che non divide* $\mathrm{disc}(f(x))$ *(o equivalentemente se le radici di* $f(x)$, *le quali appartengono a un'estensione* L *di* K, *sono distinte modulo* $p\mathcal{O}_L$*), allora* p *non ramifica in* K.

Dimostrazione. Si può mostrare che a meno di segno, $\mathrm{disc}(f(x)) = \mathrm{disc}(\mathbf{Z}[\alpha])$. Siccome $\mathrm{disc}(K)$ divide $\mathrm{disc}(\mathbf{Z}[\alpha])$, la tesi segue. □

1.4 Fattorizzazione e Teorema di Dedekind

Il seguente teorema ci dice che fattorizzare le estensioni degli ideali primi è quasi equivalente a fattorizzare polinomi.

Teorema 1.4.1 (Dedekind) *[Mar18, Thm 27]*
Sia $L = K(\alpha)$ *con* α *intero. Sia* $\mu_\alpha(x)$ *il polinomio minimo di* α *su* K. *Sia* $\mathfrak{p}$ *un primo di* K *che non divide l'indice* $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$.

Siano $p_i(x) \in \mathcal{O}_K[x]$ *polinomi monici tali che* $\mu_\alpha(x) \equiv p_1(x)^{e_1} \dots p_r(x)^{e_r} \mod \mathfrak{p}$ *sia la fattorizzazione di* $\mu_\alpha(x)$ *in* $(\mathcal{O}_K/\mathfrak{p})[x]$.

Allora detto $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + p_i(\alpha)$, *abbiamo che i* $\mathfrak{P}_i$ *sono primi che dividono* $\mathfrak{p}$, *vale* $f(\mathfrak{P}|\mathfrak{p}) = \deg p_i(x)$, *ed abbiamo la fattorizzazione*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}.$$

Proposizione 1.4.2 *Nel teorema appena enunciato, se $K = \mathbf{Q}$ e $p \nmid \mathrm{disc}(\mu_\alpha(x))$, allora l'ipotesi sull'indice è soddisfatta.*

Dimostrazione. A meno di segno abbiamo $\mathrm{disc}(\mu_\alpha(x)) = \mathrm{disc}(\mathbf{Z}[\alpha]) = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \mathrm{disc}(K)$, quindi p non divide l'indice. □

1.5 Campi quadratici

Un **campo quadratico** è un'estensione K di $\mathbf{Q}$, dove $[K : \mathbf{Q}] = 2$.

La classificazione dei campi quadratici è elementare ed è la seguente:

$$\{d : d \in \mathbf{Z}, d \neq 1, d \text{ libero da quadrati}\} \leftrightarrow \{K : K \text{ è un campo quadratico}\}$$
$$d \mapsto \mathbf{Q}(\sqrt{d}).$$

Se $d > 0$ allora $\mathbf{Q}(\sqrt{d})$ è un sottocampo di $\mathbf{R}$, e quindi si dice **campo quadratico reale**. Altrimenti, si parla di **campo quadratico immaginario**.

Se $K = \mathbf{Q}(\sqrt{d})$ dove d è come sopra, allora

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{d}] & \text{se } d \equiv 2, 3 \mod 4 \\ \mathbf{Z}[\frac{1+\sqrt{d}}{2}] & \text{se } d \equiv 1 \mod 4. \end{cases}$$

Da questo si può calcolare facilmente il discriminante.

$$\mathrm{disc}(K) = \begin{cases} 4d & \text{se } d \equiv 2, 3 \mod 4 \\ d & \text{se } d \equiv 1 \mod 4. \end{cases}$$

Chapter 2

Ordini in campi di numeri

Ogni campo di numeri K ha un sottoanello speciale, ovvero il suo anello degli interi $\mathcal{O}_K$. Un fatto fondamentale per la teoria algebrica dei numeri è che $\mathcal{O}_K$ è un dominio di Dedekind. Questo si traduce in proprietà algebriche molto buone.

Come vedremo, ai fini di studiare i primi della forma $x^2 + ny^2$, sarà essenziale considerare l'anello $\mathcal{O} = \mathbf{Z}[\sqrt{-n}]$. Questo è un sottoanello di $\mathcal{O}_K$, dove $K = \mathbf{Q}(\sqrt{-n})$, ma per molti n abbiamo $\mathcal{O} \subsetneq \mathcal{O}_K$. Definiamo quindi una classe più grande di anelli rispetto a quella dei soli anelli degli interi, ossia quella degli ordini. Questi anelli non sono sempre domini di Dedekind (anzi, lo saranno solo gli ordini della forma $\mathcal{O}_K$), e quindi avranno meno proprietà degli anelli degli interi, e lavorare con essi sarà più delicato.

2.1 Definizioni e prime proprietà

Definizione 2.1.1 *Un **ordine** del campo di numeri K è un sottoanello $\mathcal{O} \subseteq \mathcal{O}_K$ che contiene una $\mathbf{Q}$-base di K.*

Motiviamo la definizione appena data: vogliamo considerare anelli più generali degli anelli degli interi, ma vogliamo conservare molte delle loro proprietà. Le due proposizioni seguenti mostrano che le richieste che abbiamo fatto sono ragionevoli.

Proposizione 2.1.1 *Sia $\mathcal{O}$ un sottoanello di K. Allora $\mathcal{O}$ è uno $\mathbf{Z}$-modulo finitamente generato se e solo se $\mathcal{O} \subseteq \mathcal{O}_K$.*

Proposizione 2.1.2 *Sia $\mathcal{O}$ un sottoanello di $\mathcal{O}_K$. Allora sono equivalenti:*

- *$\mathcal{O}$ contiene una $\mathbf{Q}$-base di K*
- *il campo delle frazioni di $\mathcal{O}$ è K*
- *$\mathcal{O}$ è isomorfo a $\mathbf{Z}^{[K:\mathbf{Q}]}$ come $\mathbf{Z}$-modulo*
- *l'indice $f = [\mathcal{O}_K : \mathcal{O}]$ è finito.*

Da quest'ultima proposizione abbiamo che ogni ordine è contenuto in esattamente un anello degli interi che ha lo stesso campo delle frazioni K. Gli anelli degli interi sono banalmente degli ordini, e vengono chiamati **ordini massimali**. Invece, gli ordini per cui $\mathcal{O} \subsetneq \mathcal{O}_K$ vengono chiamati **ordini non massimali**.

Definizione 2.1.2 *Un **ideale frazionario** di $\mathcal{O}$ è un $\mathcal{O}$-sottomodulo (non nullo) finitamente generato di K. Diciamo che l'ideale frazionario I è **invertibile** se esiste un ideale frazionario J tale che $IJ = \mathcal{O}$.*

Proposizione 2.1.3 *[Mar18, Thm 15]*
Sia $\mathcal{O}_K$ un ordine massimale. Allora tutti i suoi ideali frazionari non nulli sono invertibili.

Le proprietà più importanti che gli ordini hanno in comune con gli ordini massimali sono le seguenti: sono domini noetheriani, hanno dimensione di Krull uguale a 1, e i loro ideali hanno indice finito.

Invece, se l'ordine in considerazione è non massimale, gli ideali frazionari non sono tutti invertibili, e perdiamo necessariamente la fattorizzazione unica in ideali primi, proprietà che invece i domini di Dedekind hanno.

Esempio 2.1.1 *Sia $\mathcal{O} = \mathbf{Z}[\sqrt{5}] \subseteq \mathbf{Q}(\sqrt{5})$, e consideriamo l'ideale di $\mathcal{O}$ dato da $I = 2\mathcal{O} + (1 + \sqrt{5})\mathcal{O}$. Allora I non è invertibile.*

Dimostrazione. Calcoliamo il quadrato di I:

$$I^2 = (4, 6 + 2\sqrt{5}, 2 + 2\sqrt{5}) = (2)I.$$

Se per assurdo I fosse invertibile, detto J il suo inverso, moltiplicando per J avremmo che $I = 2\mathcal{O}$. Si vede però facilmente che $[\mathcal{O} : I] = 2$, mentre $[\mathcal{O} : 2\mathcal{O}] = 4$. □

Da questo esempio notiamo inoltre che l'indice degli ideali di $\mathcal{O}$ non è moltiplicativo. Vedremo nella prossima sezione che questo non accade se ci restringiamo agli ideali invertibili.

2.2 Ideali invertibili e gruppo delle classi

Fissiamo la seguente notazione: dato un ordine $\mathcal{O}$, sia $\mathcal{I}(\mathcal{O})$ il gruppo degli ideali frazionari invertibili, e sia $\mathcal{P}(\mathcal{O})$ il sottogruppo degli ideali frazionari principali (è banale che questi siano invertibili). Quando consideriamo l'ordine massimale di K, scriviamo alternativamente $\mathcal{I}_K$ e $\mathcal{P}_K$ al posto di $\mathcal{I}(\mathcal{O}_K)$ e $\mathcal{P}(\mathcal{O}_K)$.

Possiamo allora generalizzare il gruppo delle classi $\mathrm{Cl}(K) = \mathcal{I}_K/\mathcal{P}_K$ a un invariante più fine. Il gruppo delle classi dipende infatti solo dal campo di numeri che consideriamo, ed è definito come $\mathcal{I}_K/\mathcal{P}_K$. Sarebbe più corretto pensarlo come assegnato ad $\mathcal{O}_K$, e indicato quindi con $\mathrm{Cl}(\mathcal{O}_K)$. Più in generale per un ordine $\mathcal{O}$, possiamo quindi definire il suo **gruppo delle classi** come

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

In questa sezione studiamo più da vicino l'invertibilità degli ideali, e otteniamo una descrizione del gruppo delle classi che ci sarà utile nel seguito.

Definizione 2.2.1 *Un primo $\mathfrak{p}$ di $\mathcal{O}$ si dice **regolare** se $\mathcal{O}_\mathfrak{p}$ è integralmente chiuso, ossia se $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{p}$. Altrimenti diremo che $\mathfrak{p}$ è un primo **non regolare**.*

La nozione di **norma** di un ideale è analoga a quella degli ordini massimali. Dato I ideale intero di $\mathcal{O}$, poniamo $\mathrm{N}(I) = |\mathcal{O}/I|$. Chiaramente, se $I \subseteq J$ sono due ideali, abbiamo la divisibilità $\mathrm{N}(J)\big|\mathrm{N}(I)$.

Proposizione 2.2.1 *Sia $\mathfrak{p}$ un primo dell'ordine $\mathcal{O}$, e sia $f = [\mathcal{O}_K : \mathcal{O}]$. Allora le seguenti proprietà sono equivalenti.*

1. $\mathfrak{p}$ *è coprimo con* $f\mathcal{O}$
2. $f\mathcal{O} \nsubseteq \mathfrak{p}$
3. $\mathfrak{p} \cap \mathbf{Z}$ *è coprimo con* f
4. $\mathrm{N}(\mathfrak{p})$ *è coprimo con* f

Dimostrazione. (1 $\iff$ 2). Siccome $\mathfrak{p}$ è massimale, è vera esattamente una tra $f\mathcal{O} \subseteq \mathfrak{p}$ e $\mathfrak{p} + f\mathcal{O} = \mathcal{O}$, che è quello che volevamo.

(2 $\iff$ 3). Se $\mathfrak{p} \cap \mathbf{Z} = (p)$, abbiamo una mappa $\mathbf{Z}/p \to \mathcal{O}/\mathfrak{p}$, e quindi $\mathcal{O}/\mathfrak{p}$ è un campo di caratteristica p. Allora $f\mathcal{O} \subseteq \mathfrak{p}$ se e solo se la moltiplicazione per f annulla questo anello, che accade se e solo se p divide f.

(3 $\iff$ 4). Come già detto, $\mathcal{O}/\mathfrak{p}$ è un campo di caratteristica p, e quindi la sua cardinalità $\mathrm{N}(\mathfrak{p})$ è potenza di p. La tesi ora è ovvia.

□

Proposizione 2.2.2 *Sia* $\mathfrak{p}$ *un primo dell'ordine* $\mathcal{O}$ *che soddisfa una delle proprietà equivalenti della Proposizione 2.2.1. Allora* $\mathfrak{p}$ *è regolare. In particolare, esistono finiti primi non regolari.*

Dimostrazione. Stiamo supponendo che p ed f siano coprimi, da cui gli indici $[\mathcal{O}_K : p\mathcal{O}_K]$ e $[\mathcal{O}_K : \mathcal{O}]$ sono coprimi. Otteniamo quindi $\mathcal{O}_K = \mathcal{O} + p\mathcal{O}_K$, e localizzando abbiamo $(\mathcal{O}_K)_\mathfrak{p} = \mathcal{O}_\mathfrak{p} + p(\mathcal{O}_K)_\mathfrak{p}$. Siccome $p \subseteq \mathfrak{p}$, per il lemma di Nakayama abbiamo $(\mathcal{O}_K)_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$.

I primi non regolari devono necessariamente contenere $f\mathcal{O}$, e corrispondono quindi ad alcuni primi di $\mathcal{O}/f\mathcal{O}$ che è un anello finito, e quindi sono in numero finito.

□

Enunciamo due lemmi di algebra commutativa che ci permetteranno di caratterizzare gli ideali invertibili.

Lemma 2.2.3 *[Sut, Thm 3.2]*
Sia A *un dominio noetheriano. Allora un* A*-ideale frazionario* I *è invertibile se e solo se la localizzazione* $I_\mathfrak{p}$ *è un* $A_\mathfrak{p}$*-ideale frazionario invertibile per ogni* $\mathfrak{p}$ *ideale massimale di* A*.*

Lemma 2.2.4 *[Bou, Ch II, §5, Prop 5]*
Sia A *un dominio semilocale (cioè con finiti ideali massimali). Allora un* A*-ideale frazionario è invertibile se e solo se è principale.*

Proposizione 2.2.5 *Sia* $\mathcal{O}$ *un ordine ed* I *un suo ideale frazionario. Allora le seguenti proprietà sono equivalenti.*

1. I *è invertibile*
2. $I_\mathfrak{p}$ *è un* $\mathcal{O}_\mathfrak{p}$*-ideale frazionario principale per ogni primo* $\mathfrak{p}$ *di* $\mathcal{O}$*.*
3. $I_\mathfrak{p}$ *è un* $\mathcal{O}_\mathfrak{p}$*-ideale frazionario principale per ogni primo non regolare* $\mathfrak{p}$ *di* $\mathcal{O}$*.*

Dimostrazione. (1 $\iff$ 2). Si ottiene facilmente combinando i Lemmi 2.2.3 e 2.2.4.

(2 $\iff$ 3). Sia J un ideale frazionario (anche non invertibile) di $\mathcal{O}$, e sia $\mathfrak{p}$ un primo regolare di $\mathcal{O}$. Poiché $\mathcal{O}_\mathfrak{p}$ è un DVR, ogni suo ideale frazionario è principale. In particolare, $J_\mathfrak{p}$ è principale.

□

Corollario 2.2.6 *La norma per gli ideali (interi) invertibili di un ordine* $\mathcal{O}$ *è moltiplicativa.*

Dimostrazione. Se A è un gruppo abeliano finito di cardinalità $p^k m$ con p ed m coprimi, allora la localizzazione $A_{(p)}$ ha cardinalità p^k. In particolare, $|A| = \prod_p |A_{(p)}|$.

In particolare se I è un ideale di $\mathcal{O}$, allora

$$N(I) = |\mathcal{O}/I| = \prod_p |(\mathcal{O}/I)_{(p)}| = \prod_p |\mathcal{O}_{(p)}/I_{(p)}|,$$

dove le localizzazioni sono fatte rispetto alla parte moltiplicativa $\mathbf{Z} \setminus (p)$.

Siano I e J due ideali invertibili di $\mathcal{O}$. Dimostreremo che

$$|\mathcal{O}_{(p)}/I_{(p)}J_{(p)}| = |\mathcal{O}_{(p)}/I_{(p)}|\,|\mathcal{O}_{(p)}/J_{(p)}|.$$

Questo implicherà la tesi, poiché moltiplicando questa relazione su tutti i p primi otteniamo proprio $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

Siccome $\mathcal{O}_{(p)}$ è un dominio semilocale ed $I_{(p)}$ è un suo ideale invertibile, esso è principale per la Proposizione 2.2.4. Gli $\mathcal{O}_{(p)}$-moduli $\mathcal{O}_{(p)}/J_{(p)}$ e $I_{(p)}/I_{(p)}J_{(p)}$ sono isomorfi, dove un isomorfismo è dato dalla moltiplicazione per un generatore di $I_{(p)}$. Abbiamo quindi

$$|\mathcal{O}_{(p)}/I_{(p)}J_{(p)}| = |\mathcal{O}_{(p)}/I_{(p)}|\,|I_{(p)}/I_{(p)}J_{(p)}| = |\mathcal{O}_{(p)}/I_{(p)}|\,|\mathcal{O}_{(p)}/J_{(p)}|.$$

□

2.3 Ideali coprimi con l'indice

Come appena visto, gli ideali invertibili si comportano meglio dell'intero insieme di ideali di un ordine. Esploriamo ora un loro sottoinsieme che ha proprietà ancor migliori.

Dato un ordine $\mathcal{O}$ di K, consideriamo gli ideali di $\mathcal{O}$ coprimi con $f\mathcal{O}$, dove $f = [\mathcal{O}_K : \mathcal{O}]$ è l'indice dell'ordine. In altre parole stiamo guardando gli ideali I per cui

$$I + f\mathcal{O} = \mathcal{O}.$$

Proposizione 2.3.1 *Gli ideali di $\mathcal{O}$ coprimi con $f\mathcal{O}$ sono invertibili.*

Dimostrazione. Sia I tale che $I + f\mathcal{O} = \mathcal{O}$ Prendiamo un primo non regolare $\mathfrak{p} \subseteq \mathcal{O}$. Per la Proposizione 2.2.2 abbiamo $f\mathcal{O} \subseteq \mathfrak{p}$, per cui a maggior ragione $I + \mathfrak{p} = \mathcal{O}$. Localizzando otteniamo $I_\mathfrak{p} + \mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$, che per il lemma di Nakayama implica $I_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$, che è principale. Per la Proposizione 2.2.5 abbiamo la tesi. □

Proposizione 2.3.2 *Sia I un ideale di $\mathcal{O}$. Allora*

$$I \text{ è coprimo con } f\mathcal{O} \iff \mathrm{N}(I) \text{ è coprimo con } f.$$

Dimostrazione. Supponiamo $\mathrm{N}(I)$ ed f coprimi. Allora $I + f\mathcal{O} = \mathcal{O}$, poiché la norma del primo membro divide sia $\mathrm{N}(I)$, sia $\mathrm{N}(f\mathcal{O}) = f^{[K:\mathbf{Q}]}$.

Per l'altra freccia, supponiamo che $\mathrm{N}(I)$ ed f non siamo coprimi. Esisterà quindi p primo razionale che li divide entrambi. Siccome $p \,|\, |\mathcal{O}/I|$, esisterà un sottogruppo $M \subseteq \mathcal{O}$ tale che $I \subseteq M$ e $p = [\mathcal{O} : M]$. Allora è chiaro che $I + f\mathcal{O} \subseteq M \subsetneq \mathcal{O}$.

□

Proposizione 2.3.3 *L'insieme degli ideali coprimi con $f\mathcal{O}$ è chiuso per moltiplicazione.*

Dimostrazione. Siano I e J due ideali coprimi con $f\mathcal{O}$. Abbiamo allora la catena di inclusioni

$$\mathcal{O} = \mathcal{O} \cdot \mathcal{O} = (I + f\mathcal{O})(J + f\mathcal{O}) \subseteq IJ + f\mathcal{O} \subseteq \mathcal{O}$$

che dimostra la tesi. □

Indichiamo con $\mathcal{I}(\mathcal{O}, f)$ il sottogruppo di $\mathcal{I}(\mathcal{O})$ generato dagli ideali di $\mathcal{O}$ coprimi con $f\mathcal{O}$. Similmente sia $\mathcal{I}_K(f)$ il sottogruppo di $\mathcal{I}_K$ generato dagli ideali di $\mathcal{O}_K$ coprimi con $f\mathcal{O}_K$.

Con la prossima proposizione mostriamo che, se ci interessa il gruppo delle classi $\mathrm{Cl}(\mathcal{O})$, è sufficiente studiare il sottogruppo $\mathcal{I}(\mathcal{O}, f)$ anziché l'intero gruppo $\mathcal{I}(\mathcal{O})$.

Proposizione 2.3.4 *[Con, Thm 5.2]*
Ogni elemento di $\mathrm{Cl}(\mathcal{O})$ *è rappresentato da un ideale di* $\mathcal{I}(\mathcal{O}, f)$*, dove* $f = [\mathcal{O}_K : \mathcal{O}]$.

Dimostrazione. Sia $I \in \mathcal{I}(\mathcal{O})$, e sia J il suo inverso. Basta trovare un x per cui $xI \in \mathcal{I}(\mathcal{O}, f)$. Per ogni primo $\mathfrak{p}$ di $\mathcal{O}$, abbiamo che $\mathfrak{p}J \subsetneq J$. Questo è ovvio se $\mathfrak{p}$ è invertibile, ma è vero in generale per il lemma di Nakayama, dopo aver localizzato al primo $\mathfrak{p}$. Sia quindi $\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ l'insieme dei primi non regolari. Per il Teorema Cinese del Resto esiste x tale che $x \in J \setminus \mathfrak{p}_i J$ per ogni $1 \leq i \leq k$.

Ora basta dimostrare che

$$xI + f\mathcal{O} = \mathcal{O}.$$

Il primo membro è un sottoinsieme del secondo poiché $x \in J$. Rimane da mostrare che nessun primo di $\mathcal{O}$ contiene il primo membro. I primi regolari non contengono $f\mathcal{O}$ per la Proposizione 2.2.2. Se $\mathfrak{p}_i$ è un primo non regolare, moltiplicando per I la relazione $x \notin \mathfrak{p}_i J$ otteniamo $xI \nsubseteq \mathfrak{p}_i$. □

Abbiamo dunque ottenuto

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}) = \mathcal{I}(\mathcal{O}, f)/(\mathcal{P}(\mathcal{O}) \cap \mathcal{I}(\mathcal{O}, f)).$$

Sia $\mathcal{P}(\mathcal{O}, f)$ il gruppo generato dagli ideali principali di $\mathcal{O}$ coprimi con $f\mathcal{O}$. Non è difficile mostrare che l'inclusione $\mathcal{P}(\mathcal{O}, f) \subseteq \mathcal{P}(\mathcal{O}) \cap \mathcal{I}(\mathcal{O}, f)$ è in realtà un'uguaglianza.

Abbiamo quindi la descrizione del gruppo delle classi come

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O}, f)/\mathcal{P}(\mathcal{O}, f).$$

Un motivo per cui è molto conveniente considerare $\mathcal{I}(\mathcal{O}, f)$ è che questi ideali frazionari si relazionano molto bene ad alcuni ideali frazionari dell'ordine massimale $\mathcal{O}_K$. Abbiamo infatti la corrispondenza seguente.

Proposizione 2.3.5 *[Con, Thm 3.8]*
L'estensione e contrazione di ideali dà una bigezione tra gli $\mathcal{O}$*-ideali interi coprimi con* $f\mathcal{O}$ *e gli* $\mathcal{O}_K$*-ideali interi coprimi con* $f\mathcal{O}_K$*:*

$$\begin{aligned} I &\mapsto I\mathcal{O}_K \\ J \cap \mathcal{O} &\hookleftarrow J. \end{aligned}$$

Inoltre, questa bigezione preserva la norma.

Dimostrazione. Per prima cosa, mostriamo che la coprimalità è conservata nella mappa.

- Se I è tale che $I + f\mathcal{O} = \mathcal{O}$, moltiplicando per $\mathcal{O}_K$ otteniamo $I\mathcal{O}_K + f\mathcal{O}_K = \mathcal{O}_K$.

- Se J è tale che $J + f\mathcal{O}_K = \mathcal{O}_K$, la sua norma $\mathrm{N}(J)$ è coprima con f. Siccome la mappa $\mathcal{O}/(J \cap \mathcal{O}) \to \mathcal{O}_K/J$ è iniettiva, anche $\mathrm{N}(J \cap \mathcal{O})$ è coprima con f, e per la Proposizione 2.3.2 abbiamo concluso.

Mostriamo ora che, dati I e J come sopra, le mappe $\mathcal{O}/(J \cap \mathcal{O}) \to \mathcal{O}_K/J$ e $\mathcal{O}/I \to \mathcal{O}_K/I\mathcal{O}_K$ sono isomorfismi.

- Consideriamo la mappa $\mathcal{O}/(J \cap \mathcal{O}) \to \mathcal{O}_K/J$. Abbiamo già osservato che è iniettiva. Inoltre, è surgettiva se e solo se $\mathcal{O} + J = \mathcal{O}_K$, ma questo è ovvio poiché gli indici di $\mathcal{O}$ e di J in $\mathcal{O}_K$ sono coprimi.
- Consideriamo $\mathcal{O}/I \to \mathcal{O}_K/I\mathcal{O}_K$. La surgettività segue anche qui dal fatto che $\mathcal{O}$ e $I\mathcal{O}_K$ hanno indici coprimi in $\mathcal{O}_K$. Per l'iniettività va mostrato che $I\mathcal{O}_K \cap \mathcal{O} = I$. Questo è mostrato dalla catena di inclusioni

$$I \subseteq I\mathcal{O}_K \cap \mathcal{O} = (I\mathcal{O}_K \cap \mathcal{O}) \cdot (I + f\mathcal{O}) \subseteq \mathcal{O} \cdot I + I\mathcal{O}_K \cdot f\mathcal{O} \subseteq I,$$

  dove per l'ultima inclusione abbiamo usato che $f\mathcal{O}_K \subseteq \mathcal{O}$.

Rimane da dire che le due mappe sono inverse, ossia che $I\mathcal{O}_K \cap \mathcal{O} = I$ e $(J \cap \mathcal{O})\mathcal{O}_K = J$. La prima è già stata mostrata. Per quanto riguarda la seconda, un'inclusione è ovvia. Questa inclusione è un'uguaglianza per questioni di norma, in quanto

$$[\mathcal{O}_K : J] = [\mathcal{O} : J \cap \mathcal{O}] = [\mathcal{O}_K : (J \cap \mathcal{O})\mathcal{O}_K],$$

dove stiamo usando gli isomorfismi appena dimostrati.

□

Corollario 2.3.6 *La bigezione appena illustrata induce un isomorfismo*

$$\mathcal{I}(\mathcal{O}, f) = \mathcal{I}_K(f).$$

Dimostrazione. La bigezione è moltiplicativa perché lo è la mappa di estensione. Quindi, c'è un isomorfismo tra i gruppi generati, che per definizione sono $\mathcal{I}(\mathcal{O}, f)$ e $\mathcal{I}_K(f)$. □

Corollario 2.3.7 *La mappa naturale* $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K)$ *è suriettiva. In particolare il class number di un ordine è un multiplo del class number del corrispettivo ordine massimale.*

Dimostrazione. La composizione

$$\mathcal{I}(\mathcal{O}, f) \to \mathcal{I}_K(f) \to \mathcal{I}_K(f)/\mathcal{P}_K(f) = \mathrm{Cl}(\mathcal{O}_K)$$

è surgettiva. Inoltre, poiché l'estensione di un ideale principale è principale, la mappa passa al quoziente, e la tesi è dimostrata. □

Sia $H \subseteq \mathcal{I}_K(f)$ il sottogruppo che corrisponde a $\mathcal{P}(\mathcal{O}, f)$ tramite l'isomorfismo $\mathcal{I}(\mathcal{O}, f) = \mathcal{I}_K(f)$.

$$\begin{array}{ccc} \mathcal{I}(\mathcal{O}, f) & \longleftarrow & \mathcal{I}_K(f) \\ \uparrow & & \uparrow \\ \mathcal{P}(\mathcal{O}, f) & \longleftarrow & H \end{array}$$

Abbiamo chiaramente la seguente espressione per il gruppo delle classi di $\mathcal{O}$:

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O}, f)/\mathcal{P}(\mathcal{O}, f) = \mathcal{I}_K(f)/H.$$

Per rendere utile tutto ciò, vogliamo studiare il sottogruppo H. Intanto per come è costruito l'isomorfismo, H è generato dagli $\alpha\mathcal{O}_K$ per cui $\alpha \in \mathcal{O}$ è coprimo con $f\mathcal{O}$ (o equivalentemente, la norma $\mathrm{N}(\alpha)$ è coprima con f).

Dimostriamo una proprietà di H apparentemente insignificante, ma che come vedremo è estremamente utile dal punto di vista della Class Field Theory. In seguito diamo una descrizione esplicita di H nel caso particolare in cui K è un campo quadratico immaginario.

Proposizione 2.3.8 *Sia $\mathcal{P}_{K,1}(f) \subseteq \mathcal{P}_K(f)$ il sottogruppo generato dagli $\alpha\mathcal{O}_K$ dove $\alpha \equiv 1$ modulo $f\mathcal{O}_K$. Allora*

$$\mathcal{P}_{K,1}(f) \subseteq H.$$

Dimostrazione. Ricordiamo che

- $\mathcal{P}_{K,1}(f)$ è generato dagli ideali $\alpha\mathcal{O}_K$, dove $\alpha \in \mathcal{O}_K$ soddisfa $\alpha \equiv 1 \mod f\mathcal{O}_K$.
- H è generato dagli ideali $\alpha\mathcal{O}_K$, dove $\alpha \in \mathcal{O}$ soddisfa $\alpha\mathcal{O} + f\mathcal{O} = \mathcal{O}$.

Chiaramente basta mostrare che un α che soddisfa le condizioni del primo punto soddisfa anche quelle del secondo.

Se α soddisfa il primo punto, allora $\alpha \in 1 + f\mathcal{O}_K \subseteq 1 + \mathcal{O} = \mathcal{O}$.

Inoltre $\alpha\mathcal{O}_K$ e $f\mathcal{O}_K$ sono coprimi, poiché $1 \in \alpha + f\mathcal{O}_K$. Da questo otteniamo che $\mathrm{N}(\alpha) = [\mathcal{O}_K : \alpha\mathcal{O}_K] = [\mathcal{O} : \alpha\mathcal{O}]$ è coprimo con f, e abbiamo la tesi usando la Proposizione 2.3.2.

□

Proposizione 2.3.9 *Se $I \in H$ è un ideale intero, allora è della forma $\alpha\mathcal{O}_K$ con $\alpha \in \mathcal{O}$.*

Dimostrazione. Per definizione di H l'ideale I è della forma $\frac{x}{y}\mathcal{O}_K$, dove $x, y \in \mathcal{O}$ hanno norma coprima con f. Inoltre siccome stiamo supponendo che I sia intero, abbiamo $\frac{x}{y} \in \mathcal{O}_K$. Allora $\frac{x}{y} \in (\frac{1}{y}\mathcal{O}) \cap \mathcal{O}_K \subseteq (\frac{1}{\mathrm{N}(y)}\mathcal{O}) \cap \mathcal{O}_K \subseteq \mathcal{O}$, dove l'ultima inclusione viene dal fatto che $\mathrm{N}(y)$ è coprimo con l'indice $f = [\mathcal{O}_K : \mathcal{O}]$.

□

Lemma 2.3.10 *Sia $\alpha \in \mathcal{O}_K$ tale che*

$$\alpha \equiv a \mod f\mathcal{O}_K, \text{ dove } a \in \mathbf{Z} \text{ è coprimo con } f.$$

Allora $\alpha \in \mathcal{O}$, e la norma $\mathrm{N}(\alpha)$ è coprima con f. In particolare $\alpha\mathcal{O}_K \in \mathcal{I}_K(f)$.

Dimostrazione. Abbiamo che $\alpha \in a + f\mathcal{O}_K \subseteq a + \mathcal{O} = \mathcal{O}$. Inoltre, $\alpha\mathcal{O}_K + f\mathcal{O}_K = \mathcal{O}_K$, poiché contiene sia f che a, i quali sono coprimi. La tesi segue. □

Lemma 2.3.11 *Sia K un campo quadratico. Allora se $\alpha \in \mathcal{O}$ ha norma coprima con f, allora*

$$\alpha \equiv a \mod f\mathcal{O}_K \text{ dove } a \in \mathbf{Z} \text{ è coprimo con } f.$$

Dimostrazione. Sia $\{1, x\}$ una $\mathbf{Z}$-base di $\mathcal{O}_K$. L'ordine $\mathcal{O}$ è un sottogruppo di $\mathcal{O}_K$ che contiene 1. Poiché l'indice è f, necessariamente $\mathcal{O} = \mathbf{Z} \oplus fx\mathbf{Z}$. Questo rende chiaro che $\mathcal{O} = \mathbf{Z} + f\mathcal{O}_K$, e che quindi $\alpha \equiv a \mod f\mathcal{O}_K$ dove $a \in \mathbf{Z}$.

Inoltre poiché α ha norma coprima con f, abbiamo che $\alpha\mathcal{O}_K + f\mathcal{O}_K = \mathcal{O}_K$, da cui $a\mathcal{O}_K + f\mathcal{O}_K = \mathcal{O}_K$, e quindi a ed f sono coprimi.

□

Definiamo $\mathcal{P}_{K,\mathbf{Z}}(f) \subseteq \mathcal{I}_K(f)$ il sottogrupppo generato dagli ideali $\alpha\mathcal{O}_K$, dove α soddisfa le ipotesi del lemma 2.3.10.

Proposizione 2.3.12 *[Cox22, Prop 7.22]*
Sia K un campo quadratico, e sia H come sopra. Allora $H = \mathcal{P}_{K,\mathbf{Z}}(f)$.

Dimostrazione. Abbiamo definito questi due gruppi dando un insieme di generatori per ciascuno. I due lemmi precedenti dicono proprio che questo insieme è lo stesso, e la tesi è quindi ovvia. □

Chapter 3

Class Field Theory

La Class Field Theory è una branca della teoria dei numeri che studia e classifica le estensioni abeliane di campi locali e globali. A noi interesserà il caso globale di caratteristica 0, ossia il caso dei campi di numeri. Per capire quali primi sono esprimibili nella forma $x^2 + ny^2$, costruiremo grazie a questa teoria una specifica estensione abeliana di $\mathbf{Q}(\sqrt{-n})$ le cui proprietà saranno essenziali per risolvere il problema.

In questo capitolo, se non viene specificato diversamente, L/K è un'estensione di campi di numeri, mentre $\mathfrak{P}|\mathfrak{p}$ sono due primi, di L e di K rispettivamente.

3.1 Primi non ramificati e simbolo di Artin

Ci restringiamo alla situazione in cui L/K è un'estensione di Galois.

Preso $g \in \mathrm{Gal}(L/K)$, accade che $g(\mathcal{O}_L) = \mathcal{O}_L$, poiché interi vengono mandati in interi. Inoltre, $g(\mathfrak{P})$ è ancora un primo, e $g(\mathfrak{P}) \cap K = g(\mathfrak{P} \cap K) = g(\mathfrak{p}) = \mathfrak{p}$. In altre parole, G agisce sui primi di L che stanno sopra a $\mathfrak{p}$, e si può dimostrare che quest'azione è transitiva.

Chiamiamo $D(\mathfrak{P})$ lo stabilizzatore di $\mathfrak{P}$. L'azione di $D(\mathfrak{P})$ su $\mathcal{O}_L$ passa al quoziente modulo $\mathfrak{P}$, ed $\mathcal{O}_K$ è fissato puntualmente. Abbiamo quindi un omomorfismo

$$D(\mathfrak{P}) \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})),$$

dove $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$ e $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ sono i campi residui dei primi presi in considerazione.

Proposizione 3.1.1 *[Mar18, Ch 4, Cor 1]*

L'omomorfismo appena descritto è surgettivo. Inoltre, se $\mathfrak{p}$ non ramifica in L, è anche iniettivo.

Se $\mathbf{F}_{q^n}/\mathbf{F}_q$ è un'estensione di campi finiti, il suo gruppo di Galois è ciclico. Inoltre ha un generatore privilegiato, chiamato automorfismo di Frobenius, descritto da $x \mapsto x^q$.

Concludiamo che, nelle ipotesi della Proposizione 3.1.1, esiste un unico elemento $g \in \mathrm{Gal}(L/K)$ tale che

$$g(x) \equiv x^{\#\kappa(\mathfrak{p})} \mod \mathfrak{P} \text{ per ogni } x \in \mathcal{O}_L.$$

Questo automorfismo si chiama **elemento di Frobenius**, e viene indicato con il **simbolo di Artin** $\left(\frac{L/K}{\mathfrak{P}}\right)$.

Proposizione 3.1.2 *[Cox22, Ch 2, Cor 5.21]*

Come prima, L/K è un'estensione di Galois e $\mathfrak{p}$ non ramifica in L. Valgono allora le seguenti proprietà del simbolo di Artin.

1. *Fissato* $\mathfrak{p}$*, gli elementi* $\left(\frac{L/K}{\mathfrak{P}}\right)$ *(al variare di* $\mathfrak{P}|\mathfrak{p}$*) sono tutti coniugati in* $\mathrm{Gal}(L/K)$*. Più precisamente, se* $\mathfrak{P}' = g(\mathfrak{P})$ *è un altro primo sopra* $\mathfrak{p}$ *(ricordiamo che sono tutti di questa forma, poiché l'azione di* $\mathrm{Gal}(L/K)$ *sui primi sopra* $\mathfrak{p}$ *è transitiva) vale*

$$\left(\frac{L/K}{g(\mathfrak{P})}\right) = g\left(\frac{L/K}{\mathfrak{P}}\right)g^{-1}.$$

2. *L'ordine di* $\left(\frac{L/K}{\mathfrak{P}}\right)$ *è il grado di inerzia* $f(\mathfrak{P}|\mathfrak{p})$*.*

3. *Sia* F *un campo intermedio dell'estensione* L/K*, anch'esso di Galois su* K*, e sia* $P = \mathfrak{P}\cap F$*. Se* $\mathrm{res}_{L/F} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ *è l'omomorfismo di restrizione, vale*

$$\mathrm{res}_{L/F}\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) = \left(\frac{F/K}{P}\right).$$

Dimostrazione. 1. Per prima cosa, $\#\kappa(\mathfrak{P}) = \#\kappa(\mathfrak{g}(\mathfrak{P}))$. Dato $x \in \mathcal{O}_L$, abbiamo

$$\left(\frac{L/K}{\mathfrak{P}}\right)(g^{-1}x) \equiv (g^{-1}x)^{\#\kappa(\mathfrak{P})} = g^{-1}(x^{\#\kappa(\mathfrak{P})}) \mod \mathfrak{P}.$$

Se ora applichiamo g ad entrambi i membri otteniamo

$$g\left(\frac{L/K}{\mathfrak{P}}\right)g^{-1}(x) \equiv x^{\#\kappa(\mathfrak{P})} \mod g(\mathfrak{P}),$$

da cui segue la tesi poiché l'elemento che induce il Frobenius modulo $g(\mathfrak{P})$ è unico.

2. Tramite l'isomorfismo $D(\mathfrak{P}) \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$, poiché il Frobenius genera il gruppo di Galois dell'estensione residua, l'ordine cercato è $\#\,\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) = f(\mathfrak{P}|\mathfrak{p})$.

3. Per ogni $x \in \mathcal{O}_L$ vale $\left(\frac{L/K}{\mathfrak{P}}\right)(x) \equiv x^{\kappa(\mathfrak{p})} \mod \mathfrak{P}$. In particolare per ogni $x \in \mathcal{O}_F$ vale $\left(\frac{L/K}{\mathfrak{P}}\right)(x) - x^{\kappa(\mathfrak{p})} \in \mathfrak{P}\cap F = P$. Quindi $\mathrm{res}_{L/F}\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)$ soddisfa la proprietà che caratterizza $\left(\frac{F/K}{P}\right)$.

□

Facciamo un'osservazione molto importante. Nel caso in cui L/K sia un'estensione abeliana, per il punto 1 della proposizione appena dimostrata, abbiamo che $\left(\frac{L/K}{\mathfrak{P}}\right)$ non dipende davvero da $\mathfrak{P}$, ma solamente da $\mathfrak{p}$, il primo di K che gli sta sotto. Nel caso di un'estensione abeliana ha senso quindi la scrittura $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Notiamo inoltre, sempre nel caso abeliano, che se $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2\dots\mathfrak{P}_k$, dove i $\mathfrak{P}_i$ sono distinti in quanto $\mathfrak{p}$ è non ramificato, abbiamo $\left(\frac{L/K}{\mathfrak{p}}\right)(x) - x^{\#\kappa(\mathfrak{p})} \in \mathfrak{P}_i$ per ogni i e per ogni $x \in \mathcal{O}_L$, e quindi per il Teorema Cinese del Resto abbiamo anche

$$\left(\frac{L/K}{\mathfrak{p}}\right)(x) \equiv x^{\#\kappa(\mathfrak{p})} \text{ modulo } \mathfrak{p}\mathcal{O}_L \text{ per ogni } x \in \mathcal{O}_L.$$

3.2 Gruppo di Galois di estensioni ciclotomiche

Come prima applicazione dei concetti appena introdotti, calcoliamo il gruppo di Galois delle estensioni ciclotomiche $\mathbf{Q}(\zeta_n)/\mathbf{Q}$.

Proposizione 3.2.1 *Il gruppo di Galois* $G = \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ *è canonicamente isomorfo a* $(\mathbf{Z}/n)^\times$.

Dimostrazione. Dividiamo la dimostrazione in tre lemmi.

Lemma 3.2.2 *C'è un'immersione* $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/n)^\times$, *e in particolare l'estensione è abeliana.*

Dimostrazione. Fissiamo una radice n-esima primitiva dell'unità ζ_n. Ogni elemento $g \in G$ mappa ζ_n ad un'altra radice n-esima primitiva, ossia ad un ζ_n^a per qualche $a \in (\mathbf{Z}/n)^\times$. La mappa $g \mapsto a$ non dipende dalla radice primitiva scelta, è un omomorfismo, ed è iniettivo poiché ζ_n genera l'estensione di campi. Abbiamo quindi $i : G \hookrightarrow (\mathbf{Z}/n)^\times$. □

Notiamo che non abbiamo usato nulla di $\mathbf{Q}$, e che quindi lo stesso lemma vale per estensioni ciclotomiche di qualsiasi campo.

Lemma 3.2.3 *Dato* p *primo che non divide* n, *le radici* n*-esime dell'unità sono distinte modulo* p *(ossia, modulo* $p\mathcal{O}_K$, *con* $K = \mathbf{Q}(\zeta_n)$*). In particolare* p *non ramifica in* $\mathbf{Q}(\zeta_n)$.

Dimostrazione. I polinomi $x^n - 1$ e nx^{n-1} sono coprimi in $\mathbf{F}_p[x]$, perché non hanno radici comuni in $\overline{\mathbf{F}}_p$. Per il criterio della derivata abbiamo dimostrato la prima affermazione. Il fatto che p non ramifichi in $\mathbf{Q}(\zeta_n)$ segue ora dal Corollario 1.3.2. □

Lemma 3.2.4 *Dato* p *primo che non divide* n, *vale* $i\left(\left(\frac{\mathbf{Q}(\zeta_n)/\mathbf{Q}}{p}\right)\right) = p$. *In particolare* p *appartiene all'immagine* $i(G)$.

Dimostrazione. Consideriamo $\left(\frac{\mathbf{Q}(\zeta_n)/\mathbf{Q}}{p}\right)(\zeta_n) = \zeta$. Questa è una radice n-esima dell'unità, e per definizione abbiamo $\zeta \equiv \zeta_n^p$ modulo p. Dal lemma 3.2.3 otteniamo che necessariamente la congruenza è un'uguaglianza, ossia $\zeta = \zeta_n^p$, e che quindi $i\left(\left(\frac{\mathbf{Q}(\zeta_n)/\mathbf{Q}}{p}\right)\right) = p$.

□

Siccome i primi che non dividono n generano il gruppo $(\mathbf{Z}/n)^\times$ (perché basta fattorizzare un rappresentante in fattori primi), abbiamo $i(G) = (\mathbf{Z}/n)^\times$ che era la tesi.

□

3.3 Legge di reciprocità quadratica

In questa sezione dimostriamo la legge di reciprocità quadratica. La includiamo per i seguenti motivi.

- È un'altra applicazione del simbolo di Artin.
- Le leggi di reciprocità sono uno dei grandi temi della Class Field Theory, ed il tentativo di generalizzarle ha spinto lo sviluppo di questa teoria. La legge di reciprocità quadratica è la più semplice, trattabile anche in maniera elementare.

- Data un'estensione di campi di numeri L/K, un insieme molto rilevante è quello dei primi di K che spezzano completamente in L, che indichiamo con $\mathrm{Spl}(L/K)$. Poniamo quindi l'attenzione allo schema dimostrativo, che sarà lo stesso del teorema principale della tesi: per risolvere un problema che è frasato naturalmente su un campo di numeri K, scegliamo accuratamente una sua estensione L in modo che il problema si possa rifrasare in termini di $\mathrm{Spl}(L/K)$.

Ricordiamo cos'è il **simbolo di Legendre**: dato un primo p e un intero n non multiplo di p, poniamo $\left(\frac{n}{p}\right) = 1$ se n è un quadrato modulo p, o equivalentemente se il polinomio $X^2 - n$ ha radici modulo p. Altrimenti poniamo $\left(\frac{n}{p}\right) = -1$.

Introduciamo la seguente notazione. Dato p dispari, esattamente uno tra p e $-p$ è congruo a 1 modulo 4. Lo indichiamo con p^*. In altre parole, $p^* = (-1)^{\frac{p-1}{2}} p$.

Teorema 3.3.1 (reciprocità quadratica) *Siano $p \neq q$ primi dispari. Allora*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

o equivalentemente,

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

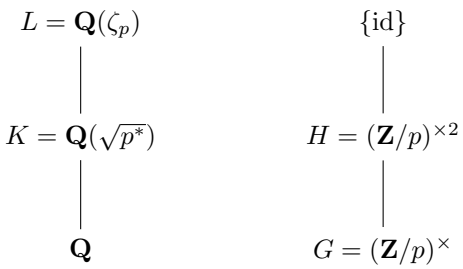
Dimostrazione. L'equivalenza delle due uguaglianze si mostra facilmente con il criterio di Eulero, il quale afferma che $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Dimostreremo quindi la seconda uguaglianza.

Consideriamo l'estensione ciclotomica $\mathbf{Q}(\zeta_p)/\mathbf{Q}$.

Lemma 3.3.2 *L'unico sottocampo quadratico del campo ciclotomico $\mathbf{Q}(\zeta_p)$ è $\mathbf{Q}(\sqrt{p^*})$.*

Dimostrazione. I sottocampi quadratici corrispondono, grazie alla teoria di Galois, ai sottogruppi di indice 2 del gruppo $\mathrm{Gal}(\mathbf{Q}(\zeta_p)) = (\mathbf{Z}/p)^\times$. Questo gruppo è ciclico di ordine $p-1$ che è pari. Quindi c'è un solo sottogruppo H di indice 2, costituito dai quadrati non multipli di p, e c'è un unico sottocampo quadratico K del campo ciclotomico. Abbiamo già visto nel Lemma 3.2.3 che i primi razionali diversi da p non ramificano in $\mathbf{Q}(\zeta_p)$. In particolare, i primi razionali diversi da p non ramificano in K. Dal calcolo dei discriminanti dei campi quadratici, sappiamo che l'unico campo quadratico per cui questo accade è $\mathbf{Q}(\sqrt{p^*})$, che è quindi uguale a K.

□



Lemma 3.3.3 *Il primo q spezza completamente in K se e solo se $\left(\frac{p^*}{q}\right) = 1$.*

Dimostrazione. Siccome $q \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt{p^*}]] = 2$, per il Teorema 1.4.1 fattorizzare $q\mathcal{O}_K$ equivale a fattorizzare $X^2 - p^*$ modulo q. In particolare, q spezza completamente in K se e solo se $X^2 - p^*$ si spezza modulo q, che equivale per definizione a $\left(\frac{p^*}{q}\right) = 1$.

□

Lemma 3.3.4 *Il primo q spezza completamente in K se e solo se $\left(\frac{q}{p}\right) = 1$.*

Dimostrazione. Nell'isomorfismo tra G e $(\mathbf{Z}/p)^\times$, abbiamo che $\left(\frac{\mathbf{Q}(\zeta_p)/\mathbf{Q}}{q}\right)$ corrisponde a q (ce lo dice il Lemma 3.2.4). Usando il punto 3 della Proposizione 3.1.2, abbiamo che $\left(\frac{K/\mathbf{Q}}{q}\right)$ corrisponde a $q \in G/H$. Per concludere,

$$
\begin{aligned}
q \text{ spezza completamente in } K &\iff \left(\frac{K/\mathbf{Q}}{q}\right) = \mathrm{id}_{G/H} && (3.1)\\
&\iff q = \mathrm{id}_{(\mathbf{Z}/p)^\times/(\mathbf{Z}/p)^{\times 2}} && (3.2)\\
&\iff q \in (\mathbf{Z}/p)^{\times 2} && (3.3)\\
&\iff \left(\frac{q}{p}\right) = 1, && (3.4)
\end{aligned}
$$

dove la prima equivalenza è data dal punto 2 della Proposizione 3.1.2.

□

La tesi è ovvia mettendo assieme gli ultimi due lemmi.

□

3.4 Class Field Theory

Sia K un campo di numeri. Stiamo per enunciare tre teoremi della Class Field Theory, i quali classificano completamente (sebbene la loro descrizione sia molto astratta e non facilmente utilizzabile) le estensioni abeliane di K. Prima è necessario introdurre un po' di nozioni. Parliamo quindi di primi infiniti, di moduli (i quali permetteranno di raffinare la solita relazione di congruenza), e di sottogruppi di congruenza.

Consideriamo le immersioni $K \to \mathbf{C}$, che sono tante quante il grado $[K : \mathbf{Q}]$. Queste immersioni si dividono in **immersioni reali** (le immersioni σ per cui $\sigma(K) \subseteq \mathbf{R}$) e **immersioni complesse** (le rimanenti).

Notiamo che le immersioni complesse sono naturalmente suddivise in coppie di immersioni coniugate.

Definizione 3.4.1 *Un **primo infinito** di K è una classe di equivalenza di immersioni $K \to \mathbf{C}$, dove due immersioni sono equivalenti se e solo se sono uguali o coniugate. Un **primo reale** è un primo infinito rappresentato da un'immersione reale. Un **primo complesso** è un primo infinito rappresentato da un'immersione complessa.*

Definizione 3.4.2 (Ramificazione per primi infiniti) *Sia L/K un'estensione di campi di numeri e σ un primo infinito di K. Diremo che σ **ramifica** in L se sono verificate entrambe le seguenti condizioni:*

- *σ è un primo reale,*

- *esiste Σ primo complesso tale che $\Sigma|_K = \sigma$ (notiamo che questa uguaglianza ha senso perché non dipende dal rappresentante della classe di equivalenza di Σ).*

Definizione 3.4.3 *Un **modulo** di K è un prodotto formale sui primi di K (finiti e infiniti)*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$$

dove gli esponenti soddisfano

- $\mathfrak{m}(\mathfrak{p}) \geq 0$*, ed al più finiti sono non nulli*
- $\mathfrak{m}(\mathfrak{p}) = 0$ *per i primi complessi*
- $\mathfrak{m}(\mathfrak{p}) \in \{0, 1\}$ *per i primi reali.*

Un modulo può essere scritto come prodotto $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, separando il contributo dei primi finiti e di quelli infiniti. Osserviamo che $\mathfrak{m}_0$ può essere considerato come un vero e proprio prodotto, ed è quindi un ideale di $\mathcal{O}_K$.

Dati due moduli $\mathfrak{m}$ ed $\mathfrak{n}$, diciamo che $\mathfrak{m}|\mathfrak{n}$ se $\mathfrak{m}(\mathfrak{p}) \leq \mathfrak{n}(\mathfrak{p})$ per ogni primo $\mathfrak{p}$.

La nozione di modulo, come il nome lascia intuire, serve a generalizzare il concetto di congruenza. Infatti dato un modulo $\mathfrak{m}$ di K e due elementi $a, b \in K^\times$, diciamo che

$$a \equiv b \mod \mathfrak{m}$$

se $a - b \in \mathfrak{m}_0$, e $\sigma(a/b) > 0$ per ogni σ primo reale che divide $\mathfrak{m}$. Questa è chiaramente una relazione di equivalenza.

Useremo le seguenti notazioni:

- $\mathcal{I}_K$: il gruppo degli ideali frazionari di $\mathcal{O}_K$
- $\mathcal{I}_K(\mathfrak{m}) \subseteq \mathcal{I}_K$: il sottogruppo generato dagli ideali (interi) coprimi con $\mathfrak{m}$, ossia (per definizione) con $\mathfrak{m}_0$
- $\mathcal{P}_K$: il gruppo degli ideali frazionari principali di $\mathcal{O}_K$
- $\mathcal{P}_K(\mathfrak{m}) \subseteq \mathcal{P}_K$: il sottogruppo generato dagli ideali principali (interi) coprimi con $\mathfrak{m}$ (ossia con $\mathfrak{m}_0$)
- $\mathcal{P}_{K,1}(\mathfrak{m}) \subseteq \mathcal{I}_K(\mathfrak{m})$: il sottogruppo degli ideali principali $\alpha\mathcal{O}_K$ in cui $\alpha \in K$ soddisfa $\alpha \equiv 1 \mod \mathfrak{m}$.

Tutto questo generalizza la notazione del capitolo 2, a meno di confondere $\mathcal{I}_K(f)$ con il più corretto $\mathcal{I}_K(f\mathcal{O}_K)$, e simili.

Notiamo inoltre che l'utilizzo che faremo di questi strumenti per risolvere il problema di $p = x^2 + ny^2$ sarà con il campo base $K = \mathbf{Q}(\sqrt{-n})$, il quale non ha primi reali. Per questa scelta di K, un modulo non sarà altro che un ideale di $\mathcal{O}_K$.

Definizione 3.4.4 *Un sottogruppo $H \subseteq \mathcal{I}_K(\mathfrak{m})$ si dice **sottogruppo di congruenza** per il modulo $\mathfrak{m}$ se*

$$\mathcal{P}_{K,1}(\mathfrak{m}) \subseteq H \subseteq \mathcal{I}_K(\mathfrak{m}).$$

In questo caso, il quoziente

$$\mathcal{I}_K(\mathfrak{m})/H$$

*è detto un **gruppo delle classi generalizzato** per il modulo $\mathfrak{m}$.*

Non è difficile dimostrare che $\mathcal{P}_{K,1}(\mathfrak{m})$ ha indice finito in $\mathcal{I}_K(\mathfrak{m})$. In particolare i gruppi delle classi generalizzati sono gruppi finiti.

Esempio 3.4.1 *Prendiamo il modulo banale $\mathfrak{m} = 1$. Il gruppo $\mathcal{P}_{K,1}(1)$ è banalmente un sottogruppo di congruenza per $\mathfrak{m}$, e il gruppo delle classi generalizzato relativo ad esso è*

$$\mathcal{I}_K(1)/\mathcal{P}_{K,1}(1) = \mathcal{I}_K/\mathcal{P}_K = \mathrm{Cl}(K),$$

e quindi il gruppo delle classi di K è un gruppo delle classi generalizzato.

Esempio 3.4.2 *Consideriamo un ordine $\mathcal{O}$ di K, e sia f il suo indice in $\mathcal{O}_K$.*

Sia $\mathfrak{m} = f\mathcal{O}_K$ ed H il sottogruppo della Proposizione 2.3.8. La stessa proposizione mostra che H è un sottogruppo di congruenza per $\mathfrak{m}$. Quindi

$$\mathcal{I}(\mathcal{O}, f)/\mathcal{P}(\mathcal{O}, f) = \mathcal{I}_K(f)/H = \mathrm{Cl}(\mathcal{O})$$

è un gruppo delle classi generalizzato.

Definiamo ora la **mappa di Artin**. Ricordiamo che, data L/K estensione abeliana di campi di numeri e $\mathfrak{p}$ un primo (finito) di K che non ramifica in L, abbiamo definito $\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$. Sia ora $\mathfrak{m}$ un modulo di K, divisibile per ogni primo (finito) che ramifica in L. Il gruppo $\mathcal{I}_K(\mathfrak{m})$ è uno $\mathbf{Z}$-modulo libero sui primi che non dividono $\mathfrak{m}$, sui quali $\left(\frac{L/K}{\cdot}\right)$ è ben definito. Possiamo quindi estendere moltiplicativamente il simbolo di Artin a una mappa

$$\Phi^{\mathfrak{m}}_{L/K} : \mathcal{I}_K(\mathfrak{m}) \to \mathrm{Gal}(L/K),$$

chiamata mappa di Artin.

Siamo pronti ad enunciare tre teoremi molto importanti della Class Field Theory.

Teorema 3.4.1 (**Reciprocità di Artin**) *[Cox22, Thm 8.2, Thm 8.5]*

Sia L/K abeliana, e sia $\mathfrak{m}$ un modulo divisibile per tutti i primi (finiti e infiniti) che ramificano in L. Allora:

- *La mappa di Artin $\Phi^{\mathfrak{m}}_{L/K}$ è suriettiva.*
- *Esiste un modulo $\mathfrak{f}$ (chiamato **conduttore** dell'estensione L/K), divisibile esattamente per i primi di K che ramificano in L, tale che*

$$\mathcal{P}_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi^{\mathfrak{m}}_{L/K}) \subseteq \mathcal{I}_K(\mathfrak{m}) \iff \mathfrak{f}|\mathfrak{m}.$$

  *In questo caso diciamo che L **ammette** $\mathfrak{m}$ come modulo.*

Mettendo assieme le due proposizioni otteniamo che se $\mathfrak{f}|\mathfrak{m}$,

$$\mathcal{I}_K(\mathfrak{m})/\ker(\Phi^{\mathfrak{m}}_{L/K}) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

è un gruppo delle classi generalizzato per il modulo $\mathfrak{m}$.

Teorema 3.4.2 (**di esistenza**) *[Cox22, Thm 8.6] Sia $\mathfrak{m}$ un modulo di K, e sia H un sottogruppo di congruenza per $\mathfrak{m}$. Allora esiste un'unica estensione abeliana L/K tale che*

- *i primi (finiti o infiniti) di K che ramificano in L dividono $\mathfrak{m}$*
- *$H = \ker(\Phi^{\mathfrak{m}}_{L/K})$.*

Con questi due teoremi possiamo ricavare la seguente corrispondenza “alla Galois".

Teorema 3.4.3 (**Corrispondenza tra sottogruppi di congruenza e estensioni abeliane**) *[Kob, Thm 2.9.5]*

Sia $\mathfrak{m}$ un modulo di K. Allora c'è una corrispondenza biunivoca tra le estensioni abeliane di K che ammettono $\mathfrak{m}$ e i sottogruppi di congruenza per $\mathfrak{m}$, e questa bigezione rovescia le inclusioni.

Più precisamente, se F ed L sono estensioni abeliane di K che ammettono $\mathfrak{m}$, allora

$$F \subseteq L \iff \ker(\Phi^{\mathfrak{m}}_{L/K}) \subseteq \ker(\Phi^{\mathfrak{m}}_{F/K}).$$

Dimostrazione. La bigezione è data dai due teoremi appena enunciati. Rimane da vedere che le inclusioni si rovesciano.

($\implies$) Preso $\mathfrak{p}$ un primo (finito) di K che non divide $\mathfrak{m}$, per il punto 3 della Proposizione 3.1.2 abbiamo che $\mathrm{res}_{L/F}\left(\left(\frac{L/K}{\mathfrak{p}}\right)\right) = \left(\frac{F/K}{\mathfrak{p}}\right)$. Estendendo per moltiplicatività a tutto $\mathcal{I}_K(\mathfrak{m})$ otteniamo $\mathrm{res}_{L/K} \circ \Phi^{\mathfrak{m}}_{L/K} = \Phi^{\mathfrak{m}}_{F/K}$ che chiaramente conclude.

($\impliedby$) Per Reciprocità di Artin, $\mathcal{I}_K(\mathfrak{m})/\ker(\Phi^{\mathfrak{m}}_{L/K}) = \mathrm{Gal}(L/K)$. In questo gruppo, $\ker(\Phi^{\mathfrak{m}}_{F/K})$ corrisponde per la teoria di Galois a un'estensione intermedia $L/F'/K$. Grazie alla parte di unicità nel teorema di esistenza abbiamo $F = F'$, da cui segue la tesi.

□

3.5 Class Field Theory per $K = \mathbf{Q}$

I teoremi che abbiamo enunciato sono di difficile uso pratico, perché si suppone di sapere lavorare agilmente con gli ideali frazionari e con i primi del campo di numeri considerato. Inoltre calcolare le mappe di Artin può essere molto complicato. Per $K = \mathbf{Q}$ la situazione è più gestibile, e si riescono ad ottenere risultati più espliciti.

Prima di enunciare il teorema di questa sezione, analizziamo l'estensione $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ dal punto di vista della Class Field Theory. In particolare mostriamo che ammette il modulo $\mathfrak{m} = (n)\infty$ (dove indichiamo con ∞ l'unico primo infinito di $\mathbf{Q}$), e calcoliamo il nucleo della mappa di Artin relativa a questo modulo.

Chiamiamo $L = \mathbf{Q}(\zeta_n)$. Per la Proposizione 3.2.3, tutti i primi che ramificano in L dividono $\mathfrak{m}$. Ricordiamo che per questo modulo i gruppi di interesse sono

$$\mathcal{I}_{\mathbf{Q}}(\mathfrak{m}) = \left\{ \frac{a}{b}\mathbf{Z} : a, b \in \mathbf{Z} \text{ sono coprimi con } n \right\}$$

$$\mathcal{P}_{\mathbf{Q},1}(\mathfrak{m}) = \left\{ \frac{a}{b}\mathbf{Z} \in \mathcal{I}_{\mathbf{Q}}(\mathfrak{m}) : \frac{a}{b} \equiv 1 \text{ modulo } n, \frac{a}{b} > 0 \right\}.$$

Lemma 3.5.1 *Il nucleo della mappa di Artin $\Phi^{\mathfrak{m}}_{L/\mathbf{Q}}$ è $\mathcal{P}_{\mathbf{Q},1}(\mathfrak{m})$. Inoltre L ammette $\mathfrak{m}$ come modulo.*

Dimostrazione. Nel Lemma 3.2.4 abbiamo visto che $\left(\frac{L/\mathbf{Q}}{p}\right) = p \in (\mathbf{Z}/n)^\times$ quando il simbolo di Artin è definito, ossia quando p non divide n. Estendendo moltiplicativamente a tutto $\mathcal{I}_K(\mathfrak{m})$ abbiamo

$$\Phi^{\mathfrak{m}}_{L/\mathbf{Q}}\left(\frac{a}{b}\mathbf{Z}\right) = ab^{-1} \in (\mathbf{Z}/n)^\times,$$

dove abbiamo preso il generatore positivo $\frac{a}{b} > 0$ dell'ideale frazionario $\frac{a}{b}\mathbf{Z}$. Entrambe le affermazioni sono ora ovvie.

□

Siamo pronti ad usare i teoremi della sezione precedente per classificare tutte le estensioni abeliane del campo dei razionali: dimostriamo il seguente teorema, che è storicamente uno dei primi teoremi della Class Field Theory.

Teorema 3.5.2 (**Kronecker-Weber**) *[Cox22, Thm 8.8]*
Sia F un'estensione abeliana finita di $\mathbf{Q}$. Allora F è contenuto in un campo ciclotomico $\mathbf{Q}(\zeta_n)$ per qualche $n \in \mathbf{N}$.

Dimostrazione. Sia $\mathfrak{m}$ un modulo di $\mathbf{Q}$ tale che F ammette $\mathfrak{m}$, che esiste grazie al teorema di reciprocità. Se $\mathfrak{m}$ non è multiplo di ∞, sostituiamolo con $\mathfrak{m}' = \mathfrak{m}\infty$, ed F a maggior ragione ammetterà $\mathfrak{m}'$, e in particolare $\mathcal{P}_{\mathbf{Q},1}(\mathfrak{m}') \subseteq \ker(\Phi^{\mathfrak{m}'}_{F/\mathbf{Q}})$.

Consideriamo $\mathbf{Q}(\zeta_n)$ dove $\mathfrak{m}' = (n)\infty$. Abbiamo visto che $\mathbf{Q}(\zeta_n)$ ammette $\mathfrak{m}'$.

Per il Lemma 3.5.1, $\ker(\Phi^{\mathfrak{m}'}_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}) = \mathcal{P}_{\mathbf{Q},1}(\mathfrak{m}')$.

Siamo ora nelle ipotesi del Teorema 3.4.3, grazie al quale otteniamo $F \subseteq \mathbf{Q}(\zeta_n)$.

□

Corollario 3.5.3 *La massima estensione abeliana $\mathbf{Q}^{\mathrm{ab}}$ di $\mathbf{Q}$ soddisfa*

$$\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q}) = \widehat{\mathbf{Z}}^{\times}.$$

Dimostrazione. Per Kronecker-Weber i campi ciclotomici sono cofinali nelle estensioni abeliane finite di $\mathbf{Q}$. Perciò,

$$\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q}) = \mathrm{Gal}(\varinjlim \mathbf{Q}(\zeta_n)/\mathbf{Q}) = \varprojlim \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) = \varprojlim (\mathbf{Z}/n)^{\times} = \widehat{\mathbf{Z}}^{\times}.$$

□

3.6 Hilbert Class Field

Il teorema di esistenza permette di costruire astrattamente delle estensioni abeliane di un campo di numeri, tenendo sotto controllo la ramificazione. L'esempio più estremo è l'Hilbert Class Field del campo K. Definiamolo e diamone alcune proprietà.

Abbiamo visto nell'Esempio 3.4.1 che $\mathcal{P}_K$ è un sottogruppo di congruenza per il modulo banale $\mathfrak{m} = 1$. Applicando il teorema di esistenza otteniamo un'estensione L di K tale che

- L/K è non ramificata ad ogni primo (finito o infinito) di K
- $\mathrm{Gal}(L/K) = \mathcal{I}_K(1)/\mathcal{P}_{K,1}(1) = \mathcal{I}_K/\mathcal{P}_K = \mathrm{Cl}(K)$.

Come anticipato, L si chiama **Hilbert Class Field** del campo K.

Proposizione 3.6.1 *[Cox22, Thm 5.18]*
Ogni estensione F/K abeliana non ramificata è contenuta nell'Hilbert Class Field L di K. Conseguentemente, L è determinato dal fatto che L/K è non ramificata e $\#\,\mathrm{Gal}(L/K) = \#\mathrm{Cl}(K)$.

Dimostrazione. Fissato K come campo base, entrambi i campi F ed L ammettono $\mathfrak{m} = 1$ come modulo. Per costruzione $\ker(\Phi^{\mathfrak{m}}_{L/K}) = \mathcal{P}_{K,1}(\mathfrak{m})$, e per il teorema di reciprocità vale $\mathcal{P}_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi^{\mathfrak{m}}_{F/K})$. Siamo nelle ipotesi del Teorema 3.4.3, da cui $F \subseteq L$.

Se inoltre $\#\,\mathrm{Gal}(F/K) = \#\mathrm{Cl}(K)$, allora F ed L hanno lo stesso grado su K, da cui $F = L$. □

Proposizione 3.6.2 *[Cox22, Cor 5.25]*
Sia L l'Hilbert Class Field del campo K, e sia $\mathfrak{p}$ un primo finito di K. Allora

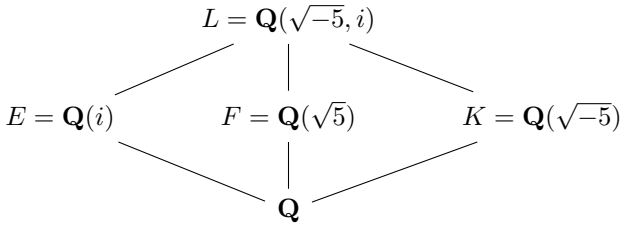
$$\mathfrak{p} \text{ è principale} \iff \mathfrak{p} \text{ spezza completamente in } L.$$

Dimostrazione. Per il punto 2 della Proposizione 3.1.2, il primo $\mathfrak{p}$ spezza completamente in L se e solo se $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. Questo accade se e solo se $\mathfrak{p} \in \ker(\Phi^1_{L/K}) = \mathcal{P}_K$, dove l'ultima uguaglianza è vera per costruzione di L. □

Esempio 3.6.1 *L'Hilbert Class Field di $K = \mathbf{Q}(\sqrt{-5})$ è $L = \mathbf{Q}(\sqrt{-5}, i)$.*

Dimostrazione. Si può calcolare che $\#\mathrm{Cl}(\mathbf{Q}(\sqrt{-5})) = 2 = [L : K]$. Basta dire che L/K è non ramificata, e avremo ottenuto la tesi grazie alla Proposizione 3.6.1. Siccome K non ha primi reali, sarà sufficiente studiare i primi finiti.

Consideriamo alcune estensioni intermedie di $L/\mathbf{Q}$ (in effetti sono tutte quante). Tutte le estensioni segnate sono di grado 2.



I discriminanti di E, F, e K sono rispettivamente $-4, 5, -20$. Gli insiemi dei primi di $\mathbf{Q}$ che ramificano in questi campi sono quindi $\{2\}$, $\{5\}$, e $\{2, 5\}$, rispettivamente.

Sia $\mathfrak{p}$ un primo di K, e sia $p = \mathfrak{p} \cap \mathbf{Z}$ il primo razionale che gli sta sotto. Mostriamo per casi che $\mathfrak{p}$ non ramifica in L.

- Se $p \neq 2, 5$, allora p è non ramificato nei tre campi intermedi, e quindi (stiamo usando la Proposizione 1.2.6) nemmeno nel composto che è L. A maggior ragione $\mathfrak{p}$ non ramifica in L.
- Se per assurdo $p = 2$ e $\mathfrak{p}$ ramificasse in L, otterremmo che p è totalmente ramificato in L. Infatti detto $\mathfrak{P}$ un primo di L sopra a $\mathfrak{p}$, avremmo $e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|p) = 4$. Per la Proposizione 1.2.5, p è totalmente ramificato in F, ma abbiamo detto che p non ramifica in F.
- Il caso $p = 5$ è analogo a $p = 2$, a meno di rovesciare i ruoli di E e di F.

□

3.7 Ring Class Field

Nell'ultima sezione abbiamo assegnato un campo, l'Hilbert Class Field, ad ogni campo di numeri. Raffiniamo la costruzione in modo da assegnare un campo ad ogni ordine $\mathcal{O}$. L'Hilbert Class Field sarà il caso particolare in cui l'ordine considerato è massimale.

Sia $\mathcal{O}$ è un ordine del campo K, ed $f = [\mathcal{O}_K : \mathcal{O}]$. Sia inoltre H il sottogruppo della Proposizione 2.3.8.

Ricordiamo che H è un sottogruppo di congruenza per il modulo $f\mathcal{O}_K$. Per il teorema di esistenza, esiste L estensione di K tale che

- al più i primi non regolari di $\mathcal{O}$ ramificano in L
- la mappa di Artin induce un isomorfismo $\mathrm{Gal}(L/K) = \mathcal{I}_K(f)/H = \mathrm{Cl}(\mathcal{O})$.

Il campo L così costruito è detto **Ring Class Field** dell'ordine $\mathcal{O}$.

Vogliamo calcolare il Ring Class Field dell'ordine $\mathbf{Z}[\sqrt{-23}]$. Innanzitutto ci serve conoscere la cardinalità del suo gruppo delle classi.

Lemma 3.7.1 *Sia $\mathcal{O} = \mathbf{Z}[\sqrt{-23}]$. Allora $\mathrm{Cl}(\mathcal{O})$ ha tre elementi.*

Dimostrazione. Usiamo il bound di Minkowski, un risultato che viene dalla teoria geometrica dei numeri. Questo teorema è più noto per gli ordini massimali, ma la medesima dimostrazione funziona per gli ordini. In sostanza ci dice che per ogni ordine $\mathcal{O}'$, ogni classe di equivalenza in $\mathrm{Cl}(\mathcal{O}')$ è rappresentata da un ideale intero I che soddisfa

$$\mathrm{N}(I) \leq \sqrt{|D|}\frac{4}{\pi}^{r_2}\frac{n!}{n^n},$$

dove $D = \mathrm{disc}(\mathcal{O}')$, r_2 è il numero di coppie di immersioni complesse del campo delle frazioni di $\mathcal{O}'$, ed n è il suo grado su $\mathbf{Q}$.

Nel nostro caso abbiamo

$$\mathrm{N}(I) \leq \sqrt{4 \cdot 23} \cdot \frac{4}{\pi} \cdot \frac{2!}{2^2} \approx 6.1,$$

quindi cerchiamo gli ideali invertibili di norma al più 6. Osserviamo anche che se $I = (a+b\sqrt{-23})$ è principale, allora $\mathrm{N}(I) = a^2 + 23b^2$.

- Se $\mathrm{N}(I) = 1$, $I = \mathcal{O}$ è principale.
- Se $\mathrm{N}(I) = 2$, necessariamente $2 \in I$. Allora I corrisponderà ad un ideale di

  $$\mathcal{O}/2\mathcal{O} = \mathbf{Z}[x]/(2, x^2+23) = \mathbf{F}_2[x]/(x^2+23) = \mathbf{F}_2[x]/(x+1)^2.$$

  C'è quindi un solo ideale di norma 2, ossia $\mathfrak{p} = (2, 1+\sqrt{-23})$, che però non è invertibile siccome $\mathfrak{p}^2 = 2\mathfrak{p}$ (analogamente all'Esempio 2.1.1).
- Se $\mathrm{N}(I) = 3$, allora $3 \in I$, e quindi I corrisponde ad un ideale di $\mathbf{F}_3[x]/(x^2+23) = \mathbf{F}_3[x]/(x+1)(x-1)$. Otteniamo $\mathfrak{p}_1 = (3, \sqrt{-23}+1)$ e $\mathfrak{p}_2 = (3, \sqrt{-23}-1)$.

  Questi non sono ideali principali siccome 3 non è esprimibile come a^2+23b^2.

  Si può calcolare che $\mathfrak{p}_1^3 = (2-\sqrt{-23})$ è principale. Segue che $[\mathfrak{p}_1] \in \mathrm{Cl}(\mathcal{O})$ ha ordine 3, ed inoltre $[\mathfrak{p}_1] = [\mathfrak{p}_2]^{-1}$ poiché $\mathfrak{p}_1\mathfrak{p}_2 = (3)$.
- Se $\mathrm{N}(I) = 4$, I corrisponde come prima a un ideale di $(\mathbf{Z}/4)[x]/(x^2+23) = (\mathbf{Z}/4)[x]/(x^2-1)$. Controllando a mano, si trovano tre ideali di norma 4. Uno di questi corrisponde a (2) ed è principale. Gli altri due sono $(4, \sqrt{-23}+1)$ e $(4, \sqrt{-23}-1)$. Entrambi non sono invertibili, poiché si può calcolare che $\mathrm{N}(I^2) = 32 \neq 16 = \mathrm{N}(I)^2$, mentre per gli ideali invertibili la norma è moltiplicativa.
- Non ci sono ideali di norma 5. Infatti se $\mathrm{N}(I) = 5$, come prima I corrisponde a un ideale di $\mathbf{F}_5[x]/(x^2+23)$ che è un campo con 5^2 elementi.
- Si controlla a mano che ci sono due ideali di norma 6, ossia $(6, \sqrt{-23}+1) = \mathfrak{p}\mathfrak{p}_1$ e $(6, \sqrt{-23}-1) = \mathfrak{p}\mathfrak{p}_2$. Poiché sono multipli di $\mathfrak{p}$, non sono invertibili.

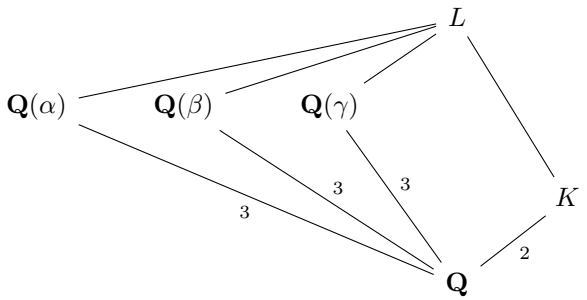
In conclusione $\mathrm{Cl}(\mathcal{O}) = \{[\mathcal{O}], [\mathfrak{p}_1], [\mathfrak{p}_2]\}$ ha 3 elementi.

□

Esempio 3.7.1 *Sia $K = \mathbf{Q}(\sqrt{-23})$ e sia $\mathcal{O} = \mathbf{Z}[\sqrt{-23}]$ un suo ordine. Sia L il campo di spezzamento su $\mathbf{Q}$ del polinomio $f(x) = x^3 - x + 1$. Allora L è il Ring Class Field di $\mathcal{O}$.*

Dimostrazione.

- Il polinomio f è irriducibile. Basta vedere che la riduzione modulo 2 è irriducibile, e questo è ovvio.
- C'è un contenimento $K \subseteq L$. Infatti,
$$-23 = \mathrm{disc}(f) = ((\alpha - \beta)(\alpha - \gamma)(\beta - \gamma))^2,$$
dove α, β, γ sono le radici di f, e quindi -23 è un quadrato in L.
- $\mathrm{Gal}(L/\mathbf{Q}) = S_3$. Infatti L ha almeno una sottoestensione quadratica e almeno una cubica, quindi ha grado multiplo di 6. Inoltre, $\mathrm{Gal}(L/\mathbf{Q}) \subseteq S_3$ considerando l'azione su $\{\alpha, \beta, \gamma\}$. In particolare le estensioni intermedie di $L/\mathbf{Q}$ sono quelle del seguente diagramma, e l'estensione L/K è Galois.



- L'unico primo (finito) che ramifica in $L/\mathbf{Q}$ è 23. Infatti $\mathrm{disc}(\mathbf{Q}(\alpha)) = \mathrm{disc}(\mathbf{Q}(\beta)) = \mathrm{disc}(\mathbf{Q}(\gamma)) = \mathrm{disc}(f) = -23$. Se p è un primo (finito) diverso da 23, abbiamo che p non ramifica in questi tre campi cubici, e quindi non ramifica nel loro composto che è L. In particolare, se un primo di K ramifica in L, allora divide 23.
- Il primo 23 non è totalmente ramificato in L. Infatti, usando il teorema di Dedekind per fattorizzare 23 in $\mathbf{Q}(\alpha)$, abbiamo che $x^3 - x + 1 = (x + 10)^2(x + 3)$ modulo 23. Quindi 23 non è totalmente ramificato in $\mathbf{Q}(\alpha)$ e tantomeno in L.
- Sia $\mathfrak{p}$ un primo di K che divide 23. Allora $\mathfrak{p}$ non ramifica in L. Infatti 23 ramifica in K, e siccome L/K è Galois, se $\mathfrak{p}$ ramificasse in L (detto $\mathfrak{P}$ un primo di L sopra a $\mathfrak{p}$) avremmo $e(\mathfrak{P}|\mathfrak{p}) = 3$ e quindi $e(\mathfrak{P}|23) = 6$. Avremmo che 23 sarebbe totalmente ramificato in $L/\mathbf{Q}$, contro il punto precedente.
- K non ha primi reali, quindi nessun primo infinito di K ramifica in L.

Per concludere, poiché $[L : K] = 3 = \#\mathrm{Cl}(\mathcal{O})$, e nessun primo finito o infinito di K ramifica in L, abbiamo la tesi.

□

Chapter 4

Soluzione di $p = x^2 + ny^2$

4.1 Soluzione del problema

Teorema 4.1.1 *[Cox22, Thm 9.4]*
Consideriamo l'ordine $\mathcal{O} = \mathbf{Z}[\sqrt{-n}]$ del campo quadratico $K = \mathbf{Q}(\sqrt{-n})$. Sia L il Ring Class Field di $\mathcal{O}$. Per un numero primo p, dispari e che non divide n, vale che

$$p = x^2 + ny^2 \iff p \text{ spezza completamente in } L.$$

Dimostrazione. Innanzitutto, siccome $\operatorname{disc}(K) \mid \operatorname{disc}(\mathbf{Z}[\sqrt{-n}]) = -4n$, la condizione su p assicura che p non ramifichi in $\mathcal{O}_K$.

Mostriamo che per un tale primo p le seguenti proprietà sono equivalenti.

1. $p = x^2 + ny^2$.
2. $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ si fattorizza in due primi distinti, entrambi della forma $\alpha\mathcal{O}_K$ con $\alpha \in \mathcal{O}$.
3. $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ si fattorizza in due primi distinti, entrambi appartenenti al sottogruppo H della Proposizione 2.3.8.
4. $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ si fattorizza in due primi distinti, e vale $\left(\frac{L/K}{\mathfrak{p}_i}\right) = 1$.
5. $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ si fattorizza in due primi distinti che spezzano completamente in L.
6. p spezza completamente in L.

(1 $\implies$ 2) Possiamo scomporre $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y) = \alpha_1\alpha_2$, da cui $p\mathcal{O}_K = (\alpha_1\mathcal{O}_K)(\alpha_2\mathcal{O}_K)$. Questi due ideali sono primi poiché lo è la loro norma. Sono distinti poiché p non ramifica in $\mathcal{O}_K$, ed hanno chiaramente la forma richiesta.

(2 $\implies$ 1) Sia $\mathfrak{p}_1 = \alpha\mathcal{O}_K$ con $\alpha \in \mathcal{O}$. Possiamo scrivere quindi $\alpha = x + \sqrt{-n}y$ con $x, y \in \mathbf{Z}$.

Poiché $K/\mathbf{Q}$ è di Galois (ha grado 2), vale $\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2)$. Inoltre

$$p^2 = \mathrm{N}(p\mathcal{O}_K) = \mathrm{N}(\mathfrak{p}_1)\mathrm{N}(\mathfrak{p}_2),$$

da cui $p = \mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(x + \sqrt{-n}y) = x^2 + ny^2$.

(2 $\implies$ 3) Se $\mathfrak{p}_i = \alpha_i\mathcal{O}_K$, allora $\mathrm{N}(\alpha_i) = p$. Inoltre p è coprimo con $f = [\mathcal{O}_K : \mathbf{Z}[\sqrt{-n}]]$, poiché $\operatorname{disc}(\mathbf{Z}[\sqrt{-n}]) = f^2\operatorname{disc}(K)$. Poiché H è generato dagli ideali della forma $\alpha\mathcal{O}_K$ con $\alpha \in \mathcal{O}$ di norma coprima con f, abbiamo concluso.

(3 $\implies$ 2) Poiché $\mathfrak{p}_i$ è un ideale intero di H, la Proposizione 2.3.9 ci dice che $\mathfrak{p}_i$ ha la forma richiesta.

(3 $\iff$ 4) Per costruzione del Ring Class Field L, abbiamo che $\ker(\Phi_{L/K}^{f\mathcal{O}_K}) = H$. Perciò $\mathfrak{p}_i \in H$ se e solo se $\left(\frac{L/K}{\mathfrak{p}_i}\right) = 1$.

(4 $\iff$ 5) Segue immediatamente dal punto 2 della Proposizione 3.1.2.

(5 $\iff$ 6) Questo è ovvio.

□

Vogliamo esprimere la condizione di spezzare completamente in L senza menzionare esplicitamente L. Innanzitutto ci serve qualche proposizione preliminare.

Proposizione 4.1.2 *Sia F un campo di numeri senza primi reali. Sia E un'estensione abeliana di F che ammette il modulo $\mathfrak{m}$. Sia $\varphi : \mathbf{C} \to \mathbf{C}$ un automorfismo tale che $\varphi(F) = F$. Allora $\varphi(E)$ è un'estensione abeliana di F che ammette il modulo $\varphi(\mathfrak{m})$, ed inoltre $\ker(\Phi_{\varphi(E)/F}^{\varphi(\mathfrak{m})}) = \varphi(\ker(\Phi_{E/F}^{\mathfrak{m}}))$.*

(Definendo bene l'azione di φ sui primi infiniti, si può eliminare la prima ipotesi. Poiché useremo questa proposizione solo per $F = \mathbf{Q}(\sqrt{-n})$, non vogliamo perderci in questi dettagli.)

Dimostrazione.

- $\varphi(E)/F$ è abeliana. Infatti φ induce un'isomorfismo

$$\begin{aligned} \mathrm{Gal}(E/F) &\to \mathrm{Gal}(\varphi(E)/F) \\ \sigma &\mapsto \varphi\sigma\varphi^{-1} \end{aligned}$$

  tra i gruppi di Galois.

- I primi di F che ramificano in $\varphi(F)$ dividono $\varphi(\mathfrak{m})$. Se $\mathfrak{p}$ finito ramifica in $\varphi(E)$, allora $\varphi^{-1}(\mathfrak{p})$ ramifica in E, da cui $\varphi^{-1}(\mathfrak{p})|\mathfrak{m}$ e quindi $\mathfrak{p}|\varphi(\mathfrak{m})$.

- In modo del tutto analogo al punto 1 della Proposizione 3.1.2 si mostra che

$$\varphi\left(\frac{E/F}{\mathfrak{p}}\right)\varphi^{-1} = \left(\frac{\varphi(E)/F}{\varphi(\mathfrak{p})}\right)$$

  per ogni $\mathfrak{p}$ primo di F coprimo con $\mathfrak{m}$. Estendendo per moltiplicatività otteniamo

$$\varphi\Phi_{E/F}^{\mathfrak{m}}(I)\varphi^{-1} = \Phi_{\varphi(E)/F}^{\varphi(\mathfrak{m})}(\varphi(I))$$

  per ogni $I \in \mathcal{I}_K(\mathfrak{m})$, e la tesi segue.

- Mostriamo che $\varphi(F)$ ammette $\varphi(\mathfrak{m})$.

  Sia $\alpha \in \mathcal{O}_F$ con $\alpha \equiv 1 \mod \varphi(\mathfrak{m})$. Allora $\varphi^{-1}(\alpha) \equiv 1 \mod \mathfrak{m}$, e quindi $\varphi^{-1}\alpha \in \ker(\Phi_{E/F}^{\mathfrak{m}})$, e per il punto precedente $\alpha \in \ker(\Phi_{\varphi(E)/F}^{\varphi(\mathfrak{m})})$.

□

Proposizione 4.1.3 *[Cox22, Lemma 9.3]*
Sia $\mathcal{O} = \mathbf{Z}[\sqrt{-n}]$ un ordine di $K = \mathbf{Q}(\sqrt{-n})$, e sia L il suo Ring Class Field. Allora $L/\mathbf{Q}$ è un'estensione di Galois.

Dimostrazione. Dobbiamo mostrare che $L/\mathbf{Q}$ è normale, ossia che le $[L:\mathbf{Q}]$ immersioni di L in $\mathbf{C}$ hanno immagine L.

Le immersioni di L in $\mathbf{C}$ sono della forma σ oppure $\tau\circ\sigma$, dove $\sigma\in\mathrm{Gal}(L/K)$ e $\tau:\mathbf{C}\to\mathbf{C}$ è il coniugio. Infatti queste sono distinte, e sono tutte quante per cardinalità. Poiché $\mathrm{Gal}(L/K)$ manda L in sé, basta mostrare che $\tau(L)=L$.

Usiamo la Proposizione 4.1.2. Il campo $\tau(L)$ è un'estensione abeliana di K che ammette $\tau(f\mathcal{O}_K)=f\mathcal{O}_K$. Inoltre il nucleo della mappa di Artin è $\ker(\Phi^{f\mathcal{O}_K}_{\varphi(L)/K})=\tau(\mathcal{P}_{K,\mathbf{Z}}(f))$.

Per il teorema di esistenza, mostrare che $\tau(L)=L$ equivale a mostrare che i due campi hanno gli stessi nuclei della mappa di Artin per $\mathfrak{m}$. In altre parole rimane da dimostrare che $\tau(\mathcal{P}_{K,\mathbf{Z}}(f))=\mathcal{P}_{K,\mathbf{Z}}(f)$.

Un insieme di generatori per $\mathcal{P}_{K,\mathbf{Z}}(f)$ sono gli $\alpha\in\mathcal{O}_K$ tali che $\alpha\equiv a \mod f\mathcal{O}_K$ dove $a\in\mathbf{Z}$ è coprimo con f. Per un tale α, vale che $\tau(\alpha)\in\tau(a)+\tau(f\mathcal{O}_K)=a+f\mathcal{O}_K$. L'insieme di generatori è quindi invariante per coniugio, da cui la tesi.

□

Abbiamo dimostrato che $L/\mathbf{Q}$ è un'estensione di Galois, e che $\tau\in\mathrm{Gal}(L/\mathbf{Q})$. Sia $F=L\cap\mathbf{R}$ il sottocampo di L fissato dal coniugio. Per teoria di Galois, $[L:F]=2$. Inoltre siccome $K\not\subseteq\mathbf{R}$, abbiamo che $L=KF$.

Sia $F=\mathbf{Q}(\alpha)$ con α intero, e sia $f(x)$ il polinomio minimo di α su $\mathbf{Q}$. Notiamo che $f(x)$ è anche il polinomio minimo di α su K, siccome annulla α ed ha il grado giusto.

Enunciamo il seguente lemma. Omettiamo la dimostrazione, che utilizza semplici considerazioni su indici di ramificazione e gradi di inerzia nelle estensioni di Galois.

Lemma 4.1.4 *Sia $E/F/D$ una torre di estensioni, con E ed F di Galois su D. Sia $\mathfrak{p}$ un primo di D. Allora le seguenti proprietà sono equivalenti.*

1. *$\mathfrak{p}$ spezza completamente in E*
2. *$\mathfrak{p}$ spezza completamente in F, ed ogni primo di F che divide $\mathfrak{p}$ spezza completamente in E*
3. *$\mathfrak{p}$ spezza completamente in F, ed esiste un primo di F che divide $\mathfrak{p}$ che spezza completamente in E.*

Teorema 4.1.5 *[Cox22, Thm 9.2]*
Riprendendo la notazione, sia $K=\mathbf{Q}(\sqrt{-n})$, sia $\mathcal{O}=\mathbf{Z}[\sqrt{-n}]$, e sia L il Ring Class Field di $\mathcal{O}$. Sia $f(x)$ il polinomio minimo su $\mathbf{Q}$ di un generatore intero di $F/\mathbf{Q}$, dove F è la massima sottoestensione reale di L.

Se p è un primo dispari che non divide né n, né il discriminante di $f(x)$, allora

$$p=x^2+ny^2 \iff \begin{cases}\left(\frac{-n}{p}\right)=1\\ f(x)\text{ ha una radice modulo }p.\end{cases}$$

Dimostrazione. Sia $p\nmid 2,n,\mathrm{disc}(f(x))$ come nelle ipotesi.

Per il Teorema 4.1.1,

$$p=x^2+ny^2 \iff p \text{ spezza completamente in } L.$$

Per il Lemma 4.1.4 applicato alla torre $L/K/\mathbf{Q}$ abbiamo che

$$p \text{ spezza completamente in } L \iff p \text{ spezza completamente in } K, \text{ e un primo } \mathfrak{p}|p \text{ spezza completamente in } L.$$

Lemma 4.1.6 *Il primo p spezza completamente in K se e solo se $\left(\frac{-n}{p}\right) = 1$.*

Dimostrazione. Poiché $\mathrm{disc}(\mathbf{Z}[\sqrt{-n}]) = f^2\mathrm{disc}(K)$ è uguale a $-4n$ che non è multiplo di p, anche f non è multiplo di p. Siamo nelle ipotesi del Teorema 1.4.1, grazie al quale fattorizzare $p\mathcal{O}_K$ equivale a fattorizzare $x^2 + n$ modulo p. In particolare, p spezza completamente in K se e solo se $x^2 + n$ modulo p si spezza in due fattori distinti. Poiché p è dispari questo accade se e solo se $\left(\frac{-n}{p}\right) = 1$.

□

Lemma 4.1.7 *Supponiamo che p spezzi completamente in K, e sia $\mathfrak{p}|p$ un primo di K. Allora*

$$\begin{aligned} \mathfrak{p} \text{ spezza completamente in } L &\iff f(x) \text{ ha una radice mod } \mathfrak{p} \\ &\iff f(x) \text{ ha una radice mod } p. \end{aligned}$$

Dimostrazione. Poiché p non divide $\mathrm{disc}(f(x))$, non divide nemmeno $\mathrm{disc}(F)$. Poiché p non ramifica né in F né in K, non ramifica nel composto L. In particolare $\mathfrak{p}$ non ramifica in L.

- Mostriamo la prima equivalenza. Abbiamo visto che $f(x)$ è anche il polinomio minimo di α su K, e siamo nelle ipotesi del Teorema 1.4.1. Poiché $\mathfrak{p}$ non ramifica in L ed L/K è Galois (e quindi i gradi di inerzia dei primi sopra a $\mathfrak{p}$ sono tutti uguali), $\mathfrak{p}$ spezza completamente in L se e solo se esiste un primo di L sopra $\mathfrak{p}$ con grado di inerzia 1, e per il Teorema 1.4.1 questo accade se e solo se la fattorizzazione di $f(x)$ modulo $\mathfrak{p}$ contiene un fattore di grado 1. Questo equivale a chiedere che $f(x)$ abbia una radice modulo $\mathfrak{p}$.

- Una freccia della seconda equivalenza è banale: se esiste $a \in \mathbf{Z}$ con $f(a) \in (p)$, a maggior ragione $f(a) \in \mathfrak{p}$. Per l'altra freccia ci serve osservare che, poiché p spezza completamente in K, vale $\mathcal{O}_K/\mathfrak{p} = \mathbf{Z}/p$. Se $\alpha \in \mathcal{O}_K$ è una radice di $f(x)$ modulo $\mathfrak{p}$, possiamo scegliere $a \in \mathbf{Z}$ tale che $a \equiv \alpha \mod \mathfrak{p}$. Ma allora $f(a) \in \mathfrak{p} \cap \mathbf{Z} = (p)$.

□

Mettendo tutto insieme otteniamo la tesi.

□

4.2 Qualche esempio

Esempio 4.2.1 *Sia $p \neq 2, 5$ un primo. Allora*

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \mod 20.$$

Dimostrazione. Questo esempio riprende l'Esempio 3.6.1. Con la notazione del Teorema 4.1.5 abbiamo $K = \mathbf{Q}(\sqrt{-5})$, $L = \mathbf{Q}(\sqrt{-5}, i)$, $F = \mathbf{Q}(\sqrt{5})$, e scegliamo $\alpha = \sqrt{5}$ che ha polinomio minimo $x^2 - 5$, di discriminante 20. Se $p \neq 2, 5$ le ipotesi del Teorema 4.1.5 sono soddisfatte.

Abbiamo quindi

$$\begin{aligned} p = x^2 + 5y^2 &\iff \left(\frac{-5}{p}\right) = 1 \text{ ed } x^2 - 5 \text{ ha una radice modulo } p \\ &\iff \left(\frac{-5}{p}\right) = 1 \text{ e } \left(\frac{5}{p}\right) = 1 \\ &\iff \left(\frac{-1}{p}\right) = 1 \text{ e } \left(\frac{5}{p}\right) = 1 \\ &\iff \left(\frac{-1}{p}\right) = 1 \text{ e } \left(\frac{p}{5}\right) = 1 \\ &\iff p \equiv 1 \mod 4 \text{ e } p \equiv 1, 4 \mod 5 \\ &\iff p \equiv 1, 9 \mod 20, \end{aligned}$$

dove per passare da $\left(\frac{5}{p}\right)$ a $\left(\frac{p}{5}\right)$ abbiamo usato la legge di reciprocità quadratica.

□

Esempio 4.2.2 *Sia $p \neq 2, 23$. Allora*

$$p = x^2 + 23y^2 \iff \begin{cases} \left(\frac{-23}{p}\right) = 1 \\ x^3 - x + 1 \text{ ha una radice modulo } p. \end{cases}$$

Dimostrazione. Dall'Esempio 3.7.1 sappiamo che L è il campo di spezzamento del polinomio $x^3 - x + 1$. Tra le radici $\{\alpha, \beta, \gamma\}$, almeno una è reale (in effetti solo una). Supponiamo che α sia reale. Allora con la notazione del Teorema 4.1.5, abbiamo $F = \mathbf{Q}(\alpha)$. Poiché $p \neq 2, 23$, ricordando che $\operatorname{disc}(x^3 - x + 1) = -23$, il Teorema 4.1.5 ci dà la tesi.

□

4.3 Condizioni di congruenza

In questa sezione, un primo è un primo finito di $\mathbf{Q}$. Inoltre $\mathrm{Spl}(M)$ è l'insieme dei primi che spezzano completamente in M.

Dati $A, B \subseteq \mathbf{N}$, scriviamo $A \dot{\subseteq} B$ per dire che $A \setminus B$ è finito (in altre parole, A è contenuto in B con finite eccezioni).

Inoltre scriviamo $A \doteq B$ per dire $A \dot{\subseteq} B$ e $B \dot{\subseteq} A$. Questa è una relazione equivalenza.

Diciamo che un insieme di primi S è **definito da congruenze** se esistono $N, x_1, \ldots, x_k \in \mathbf{N}$ tali che

$$S \doteq \{p : p \text{ è primo, e } p \equiv x_1, \ldots, x_k \mod N\}.$$

Teorema 4.3.1 *Sia M un campo di numeri. Allora $\mathrm{Spl}(M)$ è definito da congruenze se e solo se $M/\mathbf{Q}$ è abeliana.*

Corollario 4.3.2 *Dato un intero $n > 0$, l'insieme $\{p : p = x^2 + ny^2\}$ è definito da congruenze se e solo se $L/\mathbf{Q}$ è abeliana, dove L è il Ring Class Field di $\mathbf{Z}[\sqrt{-n}]$.*

Dimostrazione. Il Teorema 4.1.1 ci dice che $\{p : p = x^2 + ny^2\} \doteq \mathrm{Spl}(L)$. Quindi $\{p : p = x^2 + ny^2\}$ è definito da congruenze se e solo se lo è $\mathrm{Spl}(L)$. La tesi segue ora dal Teorema 4.3.1. □

Esempio 4.3.1 *Nell'Esempio 4.2.1 abbiamo visto che* $\{p : p = x^2+5y^2\}$ *è definito da congruenze. Infatti,*

$$\mathrm{Gal}(L/\mathbf{Q}) = \mathbf{Z}/2 \times \mathbf{Z}/2$$

è abeliano.

Esempio 4.3.2 *L'insieme* $\{p : p = x^2 + 23y^2\}$ *non è definito da congruenze. Infatti,*

$$\mathrm{Gal}(L/\mathbf{Q}) = S_3$$

non *è abeliano.*

Bibliografia

[Bou] N. Bourbaki. *Algèbre commutative, Chapitres 1 à 4*.

[Con] K. Conrad. *The Conductor Ideal of an Order*. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf.

[Cox22] David A. Cox. *Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication*. AMS Chelsea Publishing, Providence, RI, [2022] ©2022.

[Kob] A. Kobin. *Class Field Theory*. URL: https://www.andrewkobin.com/course-notes.

[Mar18] Daniel A. Marcus. *Number fields*. Springer, Cham, 2018.

[Mil] J. Milne. *Class Field Theory*. URL: https://www.jmilne.org/math/CourseNotes/cft.html.

[Sut] Andrew Sutherland. *Properties of Dedekind Domains*. URL: https://ocw.mit.edu/courses/18-785-number-theory-i-fall-2021/mit18_785f21_lec3.pdf.