Note di Teoria dei Numeri
A.A. 2019-20

Orazio Puglisi

Indice

Capitolo 1

Reticoli

1.1 Gruppi topologici

In questa sezione ricordiamo alcuni fatti riguardanti gruppi topologici.

Definizione 1.1.1 *Sia G un gruppo dotato di una topologia τ. Diremo che G è un* gruppo topologico *se le due applicazioni*

$$\begin{aligned} \iota : G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned} \qquad\qquad \begin{aligned} \mu : G \times G &\longrightarrow G \\ (g,h) &\longmapsto gh \end{aligned}$$

sono continue.

Esempi di gruppi topologici non sono difficicili da trovare.

- Ogni gruppo dotato della topologia discreta è un gruppo topologico.
- $\mathbb{R}^n$ con la topologia usuale è un gruppo topologico.
- Il gruppo $\mathbb{S}^1 = \{z \mid z \in \mathbb{C}\ |z| = 1\}$ con la topologia indotta da quella di $\mathbb{C}$ è un gruppo topologico.

Se G è un gruppo topologico ed N è un suo sottogruppo normale, è possibile definire una topologia nel gruppo quoziente G/N, in modo che la proiezione canonica $\pi : G \longrightarrow G/N$ risulti continua. Infatti, scegliendo $\mathcal{A} = \{A \subseteq G/N \mid \pi^{-1}(A) \text{ è aperto di } G\}$ come insieme di aperti, si vede immediatamente che π risulta continua e, inoltre, ogni topologia su G/N che renda continua π è contenuta in $\mathcal{A}$. Pertanto, nel contesto dei gruppi topologici, i quozienti vengono sempre pensati dotati di questa topologia, detta appunto la *topologia quoziente*. Come è facile intuire, gli usuali teoremi di omomorfismo hanno un loro corrispettivo *topologico*, la cui formulazione (ed eventuale dimostrazione) è lasciata al lettore.

Un esempio di applicazione del I Teorema di isomorfismo è il seguente.

Esempio Sia $\sigma : \mathbb{R} \longrightarrow \mathbb{C}^*$ la funzione definita da $\sigma(x) = e^{2\pi ix}$. I gruppi $(\mathbb{R}, +)$ e $(\mathbb{C}^*, \cdot)$ li pensiamo dotati delle loro usuali topologie. Si controlla immediatamente che σ è un morfismo continuo di gruppi, e che $\sigma(\mathbb{R}) = \mathbb{S}^1$. Inoltre $\ker(\sigma) = \mathbb{Z}$ e, pensando $\mathbb{R}/\mathbb{Z}$ dotato della topologia quoziente. si ottiene che $\mathbb{R}/\mathbb{Z}$ è isomorfo, come **gruppo topologico**, a $\mathbb{S}^1$. Ci servirà, in particolare, osservare che $\mathbb{R}/\mathbb{Z}$ è compatto. Tutto questo può facilmente essere modificato per ottenere il seguente utile risultato.

Proposizione 1.1.2 *Si consideri il gruppo topologico* $\mathbb{R}$ *e si scelga* $0 \neq a \in \mathbb{R}$. *Posto* $N = \langle a \rangle$ *il sottogruppo generato da* a, *i gruppi* $\mathbb{R}/N$ *ed* $\mathbb{S}^1$ *sono isomorfi come gruppi topologici. In particolare* $\mathbb{R}/N$ *è compatto.*

Per dimostrarlo si osserva che N è isomorfo a $\mathbb{Z}$ e si modifica il morfismo σ in modo che la sua immagine resti invariata ma il nucleo sia N.

Sia V uno spazio vettoriale su $\mathbb{R}$ di dimensione n. Fissato un isomorfismo $\phi : \mathbb{R}^n \longrightarrow V$, possiamo definire una topologia su V scegliendo come aperti tutti gli insiemi $A \subseteq V$ tali che $\phi^{-1}(A)$ è aperto di $\mathbb{R}^n$. In tal modo ϕ diventa un isomorfismo topologico. Di certo ϕ è continuo per come è stata definita la topologia. Per vedere che ϕ^{-1} è continuo, osserviamo che, se U è un aperto di $\mathbb{R}^n$, $U = \phi^{-1}(\phi(U))$, e quindi $\phi(U) \in \mathcal{A}_\phi$. Questo dice the ϕ^{-1} è continuo. Scelto un altro isomorphismo $\psi : \mathbb{R}^n \longrightarrow V$, possiamo considerare la mappa (tra gruppi topologici)

$$\sigma = \psi\phi^{-1} : (V, \mathcal{A}_\phi) \longrightarrow (V, \mathcal{A}_\psi)$$

Questo è un isomorfismo continuo, perché composizione di isomorfismi continui. Lo stesso vale per σ^{-1}, e quindi σ è un isomorfismo di gruppi topologici. Pertanto $\mathcal{A}_\phi = \mathcal{A}_\psi = \mathcal{A}$, e questa topologia, che dipende quindi solo dalla topolgia di $\mathbb{R}^n$, sarà quella di cui doteremo ogni $\mathbb{R}$-spazio vettoriale. Quindi, quando dovremo considerare uno spazio vettoriale reale V di dimensione n, potremo supporre, se necessario, che V sia $\mathbb{R}^n$. Inoltre quello che abbiamo appena visto ci dice che, scelte una base $x_1, \ldots, x_n$ di $\mathbb{R}^n$ e $v_1 \ldots, v_n$ di V, l'unica funzione lineare tale che $\sigma(x_i) = v_i$ per ogni i, è un isomorfismo topologico. Quindi ogni isomorfismo lineare tra V ed $\mathbb{R}^n$ è un isomorfismo topologico. Sia ϕ uno di questi isomorfismi e si consideri l'insieme

$$\mathcal{B}_\phi = \{\phi(B) \mid B \subseteq \mathbb{R}^n \text{ è limitato}\}.$$

Si controlla facilmente che tale insieme non dipende da ϕ. I suoi elementi sono i *sottoinsiemi limitati* d V.

1.2 Reticoli

Diamo ora la definizione di un tipo di struttura di cui faremo grande uso in seguito.

Definizione 1.2.1 *Sia* V *un* $\mathbb{R}$*-spazio vettoriale di dimensione finita. Un* reticolo *in* V *è un sottogruppo generato da una base di* V.

Se V ha dimensione n e $v_1, \ldots, v_n$ è una base, il reticolo associato a tale base è

$$\langle v_1, \ldots, v_n \rangle = \Big\{ \sum_{i=1}^{n} a_i v_i \mid a_i \in \mathbb{Z} \, \forall i \Big\}.$$

Dato che gli elementi di una base sono indipendenti su $\mathbb{R}$, a maggior ragione lo sono su $\mathbb{Z}$. Allora un reticolo in V è un gruppo libero di rango n, quindi isomorfo a $\mathbb{Z}^n$.

Diamo ora una caratterizzazione dei reticoli. Gli spazi vettoriali su $\mathbb{R}$ si intenderanno dotati della topologia discussa in precedenza. Se X è un sottoinsieme dello spazio vettoriale reale V, indichiamo con $\langle X \rangle_{\mathbb{R}}$ il sottospazio vettoriale generato da X. Il simbolo $\langle X \rangle_{\mathbb{Z}}$ indicherà invece il sottogruppo generato da X.

Teorema 1.2.2 *Siano V uno spazio vettoriale su $\mathbb{R}$ di dimensione n ed A un sottogruppo di V. Sono equivalenti:*

1. *A è un reticolo in V.*
2. *A è discreto e V/A è compatto.*
3. *$\langle A \rangle_{\mathbb{R}} = V$ e, per ogni sottoinsieme $B \subseteq V$ limitato, l'insieme $B \cap A$ è finito.*

Dimostrazione Senza perdere di generalità possiamo pensare $V = \mathbb{R}^n$. Indicheremo con $e_1, e_2, \ldots, e_n$ gli elementi della base canonica.

1) $\Longrightarrow$ 2).

Il reticolo A sia generato dalla base $v_1, v_2, \ldots, v_n$. Allora, detta σ l'unica funzione lineare che soddisfa $\sigma(v_i) = e_i$ per ogni $i = 1, \ldots, n$, abbiamo che σ è un isomorfismo topologico e $\sigma(A) = E = \langle e_1, \ldots e_n \rangle_{\mathbb{Z}}$ è un reticolo. Chiaramente E è discreto e quindi anche A è discreto. Osserviamo ora che $V \simeq \oplus_{i=1}^{n} \langle v_i \rangle_{\mathbb{R}}$ mentre $A \simeq \oplus_{i=1}^{n} \langle v_i \rangle_{\mathbb{Z}}$. Pertanto si ottiene

$$V/A \simeq \frac{\oplus_{i=1}^{n} \langle v_i \rangle_{\mathbb{R}}}{\oplus_{i=1}^{n} \langle v_i \rangle_{\mathbb{Z}}} \simeq \bigoplus_{i=1}^{n} \frac{\langle v_i \rangle_{\mathbb{R}}}{\langle v_i \rangle_{\mathbb{Z}}}.$$

Dato che ogni quoziente $\langle v_i \rangle_{\mathbb{R}} / \langle v_i \rangle_{\mathbb{Z}}$ è isomorfo ad $\mathbb{R}/\mathbb{Z}$, usando l'esempio precedente abbiamo che V/A è isomorfo, come gruppo topologico, a $(\mathbb{S}^1)^n$ ed è pertanto compatto.

2) $\Longrightarrow$ 3).

Poniamo $W = \langle A \rangle_{\mathbb{R}}$. Se $W \neq V$ allora V/W è isomorfo ad $\mathbb{R}^k$ dove $k = \dim(V) - \dim(W) \geq 1$. Dato che A è sottogruppo di W, il terzo teorema di isomorfismo per gruppi topologici ci dice che V/W è isomorfo al quoziente $(V/A)/(W/A)$ ed è quindi immagine, tramite un morfismo continuo, di V/A. Dato che ogni immagine continua di un compatto è compatta, abbiamo una contraddizione. Ne segue che $W = V$.

Sia ora B un sottoinsieme limitato e supponiamo che $A \cap B$ sia infinito. Dato che anche la chiusura di B è un insieme limitato, possiamo supporre che B sia chiuso, quindi compatto.

Dato che $A \cap B$ è un sottoinsieme numerabile di un compatto, contiene una successione infinita $\{x_i \mid i \in \mathbb{N}\}$ che converge ad un certo $x \in B$. In particolare la successione è di Cauchy e, a meno di passare ad una sottosuccessione, possiamo supporre che $0 < |x_i - x_{i-1}| < 2^{-i}$ per ogni $i \geq 1$ (qui $|\cdot|$ indica l'usuale norma di $\mathbb{R}^n$). Ciascuno degli elementi $y_i = x_i - x_{i-1}$ appartiene ad A e chiaramente $\lim y_i = 0 \in A$. Questo vuol dire che 0 non è un punto isolato di A, contraddicendo il fatto che A è discreto.

3) $\Longrightarrow$ 1).

Dato che $\langle A \rangle_{\mathbb{R}} = V$, A deve contenere una base di V. Sia $v_1, v_2, \ldots, v_n$ una tale base e poniamo $M = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$. Chiaramente $M \leq A$. Prendiamo ora un generico elemento $a \in A$. Usando il fatto che i v_i formano una base di V, possiamo scrivere $a = \sum_{i=1}^n \alpha_i v_i$ con gli α_i numeri reali. Ogni α_i si scrive come $\alpha_i = m_i + \lambda_i$ dove $m_i = \lfloor \alpha_i \rfloor$ (la parte intera di α_i) e $\lambda_i = \alpha_i - m_i$ (la parte frazionaria di α_i). Gli m_i sono interi mentre ciascun λ_i appartiene all'intervallo $[0, 1)$. Abbiamo quindi

$$a = \sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^n m_i v_i + \sum_{i=1}^n \lambda_i v_i.$$

L'elemento $m_a = \sum_{i=1}^n m_i v_i$ appartiene ad M (e quindi ad A), mentre $b_a = \sum_{i=1}^n \lambda_i v_i$ è nell'insieme $B = \sum_{i=1}^n [0.1) v_i$, che è un insieme limitato. Dato che $b_a = a - m_a$, anche b_a appartiene ad A, e quindi $b_a \in A \cap B$. Ne deduciamo che $A = M + \langle A \cap B \rangle_{\mathbb{Z}}$. Per ipotesi $A \cap B$ è finito e allora A è un gruppo finitamente generato. Per questo motivo A è isomorfo ad un gruppo del tipo $\mathbb{Z}^m \oplus F$ con F finito ma, essendo A un sottogruppo di $\mathbb{R}^n$, non ha elementi di periodo finito. Quindi A è libero e indichiamo con m il suo rango. Il sottogruppo M è libero di rango n ed il quoziente A/M può essere descritto, per quanto visto in precedenza, come

$$A/M = \{b + M \mid b \in A \cap B\}.$$

Di conseguenza A/M è finito. Sappiamo che questo accade solo quando M ha lo stesso rango di A, quindi $m = n$ ed un qualsiasi sistema libero $\mathcal{L}$ di generatori di A deve essere una base di V, visto che $\langle A \rangle_{\mathbb{R}} = \langle \mathcal{L} \rangle_{\mathbb{R}}$. Quindi A è un reticolo. □

Definizione 1.2.3 *Dati A, un reticolo in $\mathbb{R}^n$, ed una sua base $\mathbf{v} = \{v_1, v_2, \ldots, v_n\}$, l'insieme $D = \{\sum_{i=1}^n \lambda_i v_i \mid \lambda_i \in [0, 1) \, \forall i\} = \sum_{i=1}^n [0, 1) v_i$ si dice un* dominio fondamentale *di A.*

Un dominio fondamentale dipende dalla base scelta, quindi lo stesso reticolo ammette diversi domini fondamentali. Se $v_1, v_2, \ldots v_n$ è una base di A e D è il corrispondente dominio fondamentale, allora $\mathbb{R}^n = \bigcup_{v \in A} (D + v)$ e, se $(D + v) \cap (D + w) \neq \emptyset$, deve essere $v = w$. Infatti, se $(D + v) \cap (D + w) \neq \emptyset$, un elemento nell'intersezione è dellla forma $d_1 + v = d_2 + w$ per opportuni $d_1, d_2 \in D$. Allora $v - w = d_1 - d_2$ e, scrivendo tutti i vettori rispetto alla base $v_1, v_2, \ldots v_n$, si vede che $v - w$ è combinazione intera degli elementi della base, mentre i coefficienti nella scrittura di $d_1 - d_2$ sono tutti numeri reali in modulo strettamente minori di 1. L'unica possibilità è quindi che siano tutti nulli, e di conseguenza $v = w$.

L'insieme $\mathbb{R}^n$ è anche dotato di una misura μ, quella di Lebesgue. Possiamo allora calcolare il volume del dominio fondamentale D che di certo è un insieme misurabile. Se scegliamo un'altra base $\mathbf{w} = \{w_1, \ldots, w_n\}$ per A, ed $M \in M(n, \mathbb{Z})$ è la matrice di passaggio tra le due basi (ovvero $\mathbf{w} = M\mathbf{v}$), abbiamo che, detto $\overline{D}$ il dominio fondamentale rispetto alla nuova base, $\mu(\overline{D}) = |\det(M)|\,\mu(D)$. Dato che M è la matrice di passaggio tra due basi di A, il suo determinante è ± 1. Possiamo allora dare la seguente definizione.

Definizione 1.2.4 *Siano A un reticolo in $\mathbb{R}^n$ e D un suo dominio fondamentale. Definiamo il* covolume *di A come* $\mathrm{cov}(A) = \mu(D)$.

Scelta una base $v_1, \ldots, v_n$ per il reticolo A, il covolume è il valore assoluto del determinante della matrice $K = (v_1 v_2 \cdots v_n)$, ovvero la matrice le cui colonne sono le coordinate, rispetto alla base canonica, dei vettori della base.

1.3 Teorema di Minkowski

In questa sezione dimostreremo un importante teorema che, pur nella sua semplicità, ha diverse conseguenze di notevole importanza. Iniziamo con un lemma.

Lemma 1.3.1 *Siano X un sottoinsieme di $\mathbb{R}^n$ limitato e misurabile ed L un reticolo in $\mathbb{R}^n$. Si consideri inoltre $\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^n/L$ la proiezione canonica. Se $\mathrm{cov}(L) < \mu(X)$, allora la restrizione di π ad X non è iniettiva.*

Dimostrazione. Scegliamo un dominio fondamentale D per L e, per ogni $v \in L$, poniamo $X_v = X \cap (D + v)$. Definiamo poi $Y_v = X_v - v$. Osserviamo che

- gli insiemi X_v sono non vuoti solo per un numero finito di v, dato che X è limitato. Poniamo $I = \{v \mid X_v \neq \emptyset\}$;
- se $v \neq w$ allora $X_v \cap X_w = \emptyset$, visto che $(D + v) \cap (D + w) = \emptyset$;
- $\mu(X_v) = \mu(Y_v)$ dato che la misura di Legesgue è invariante per traslazioni;
- $Y_v \subseteq D$ per ogni $v \in L$.

Abbiamo quindi $\mu(X) = \sum_{v \in I} \mu(X_v) = \sum_{v \in I} \mu(Y_v)$. Ne deduciamo che, per almeno una coppia v, w di elementi distinti di I, deve essere $Y_v \cap Y_w \neq \emptyset$. Per convincerci di questo basta osservare che, se gli insiemi Y_v fossero tutti disgiunti, avremmo $\mu(\bigcup_{v \in I} Y_v) = \sum_{v \in I} \mu(Y_v)$ e, dato che $\bigcup_{v \in I} Y_v \subseteq D$, si otterebbe

$$\mathrm{cov}(L) = \mu(D) \geq \mu(\bigcup_{v \in I} Y_v) = \sum_{v \in I} \mu(Y_v) = \sum_{v \in I} \mu(X_v) = \mu(\bigcup_{v \in I} X_v) = \mu(X) > \mathrm{cov}(L)$$

una contraddizione. Scelti $v, w \in I$ in modo opportuno, abbiamo $Y_v \cap Y_w \neq \emptyset$ e possiamo allora trovare $x_1, x_2 \in X$ tali che $x_1 - v = x_2 - w \in Y_v \cap Y_w$. Da questo si ricava $x_2 = x_1 + (w - v)$ e,

dato che $w - v \in L$, si ha $\pi(x_2) = x_1 + (w - v) = x_1 + (w - v) + L = x_1 + L = \pi(x_1)$. Quindi la restrizione di π ad X non è iniettiva, visto che $x_2 - x_1 = w - v \neq 0$. □

Se X è un sottoinsieme di $\mathbb{R}^n$, diciamo che è *simmetrico* se, ogni volta che $x \in X$, allora anche $-x \in X$. Ricordiamo infine che è possibile provare che ogni sottoinsieme di $\mathbb{R}^n$ che sia convesso e limitato, è misurabile secondo Lebesgue. Possiamo ora enunciare e dimostrare il *Teorema del corpo convesso di Minkowski.*

Teorema 1.3.2 *Siano X un sottoinsieme convesso, limitato e simmetrico di $\mathbb{R}^n$ ed L un reticolo di $\mathbb{R}^n$. Se $2^n \mathrm{cov}(L) < \mu(X)$ allora l'insieme $L \cap X$ contiene almeno un elemento diverso da 0.*

Dimostrazione. Il reticolo $2L$ ha covolume $2^n \mathrm{cov}(L)$ e quindi, per il lemma 1.3.1, esistono $x, y \in X$ distinti ma tali che $x + 2L = y + 2L$. Dato che $x - y \in 2L$ si ha $0 \neq z = \frac{1}{2}(x - y) \in L$. L'insieme X è simmetrico, quindi $-y \in X$. L'elemento z si scrive come

$$z = \frac{1}{2}x + \frac{1}{2}(-y)$$

ed è pertanto una combinazione convessa di due punti di X. Essendo X convesso abbiamo $z \in X$ ed il teorema è dimostrato. □

Per dare un esempio della utilità di questo risultato, dimostriamo il noto *Teorema dei quattro quadrati* di Lagrange. Avremo bisogno di un fatto, la cui dimostrazione è lasciata per esercizio.

Lemma 1.3.3 *Sia $\mathbb{F}$ un campo finito. Allora ogni elemento di $\mathbb{F}$ è somma di due quadrati.*

Teorema 1.3.4 *Ogni numero naturale è somma di quattro quadrati.*

Dimostrazione. Per prima cosa mostriamo che è sufficiente provare il teorema per i numeri primi. Per vederlo dobbiamo ricordare alcuni fatti elementari sui quaternioni. Se $q = a + bi + cj + dk \in \mathbb{H}$ è un quaternione, la sua norma è definita da $N(q) = a^2 + b^2 + c^2 + d^2$ e per ogni $u, v \in \mathbb{H}$ vale $N(uv) = N(u)N(v)$. Usando questo si vede immediatamente che, se a, b, c, d e x, y, z, w, sono numeri naturali, allora $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2)$ è ancora la somma di quattro quadrati di numeri naturali. Questa osservazione ci dice che è sufficiente dimostrare che ogni numero primo è somma di quattro quadrati di numeri naturali. La cosa è vera per il primo 2, quindi sia $p \in \mathbb{N}$ un primo dispari. Usando il Lemma 1.3.3 nel caso in cui $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$, possiamo trovare due naturali u, v tali che $u^2 + v^2 + 1 \equiv 0 \pmod{p}$. Definiamo

$$L = \{(x, y, z, w) \in \mathbb{Z}^4 \mid z \equiv ux + vy \pmod{p} \quad \text{e} \quad w \equiv uy - vx \pmod{p}\}.$$

Si controlla immediatamente che L è un sottogruppo di $\mathbb{R}^4$ e, scrivendo esplicitamente le due condizioni date dalle congruenze, si ottiene

$$L = \{(x, y, ux+vy+kp, uy-vx+tp) \mid x, y, k, t \in \mathbb{Z}\} = \langle (1, 0, u, -v), (0, 1, v, u), (0, 0, p, 0), (0, 0, 0, p) \rangle_{\mathbb{Z}}.$$

Il gruppo L è quindi un reticolo ed il suo covolume è dato da

$$\mathrm{cov}(L) = \left| \det \begin{pmatrix} 1 & 0 & u & -v \\ 0 & 1 & v & u \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix} \right| = p^2.$$

Detta $B(r)$ la palla di $\mathbb{R}^4$ di centro 0 e raggio r, abbiamo che $\mu(B(r)) = \pi^2 r^4/2$. Scegliamo r in modo che $r^2 = 1.9p$. Con questa scelta si ha $r^4 > 32p^2/\pi^2$ e quindi

$$2^4 \mathrm{cov}(L) = 2^4 p^2 < \pi^2 r^4/2 = \mu(B(r))$$

per cui è possibile applicare il teorema 1.3.2. Prendiamo quindi $0 \neq x = (a, b, c, d) \in L \cap B(r)$. Dato che x appartiene a $B(r)$ la sua norma non supera r^2. Pertanto $|x| = a^2+b^2+c^2+d^2 \leq r^2 < 2p$. Il vettore x è anche un elemento di L, quindi $c \equiv ua + vb \pmod{p}$ e $d \equiv ua - vb \pmod{p}$. Allora

$$a^2 + b^2 + c^2 + d^2 \equiv a^2 + b^2 + (ua + vb)^2 + (ua - vb)^2 \pmod{p}.$$

Ma $(ua + vb)^2 + (ua - vb)^2 = a^2(u^2 + v^2) + b^2(u^2 + v^2)$ e quindi

$$a^2+b^2+c^2+d^2 \equiv a^2+b^2+a^2(u^2+v^2)+b^2(u^2+v^2) = a^2(u^2+v^2+1)+b^2(u^2+v^2+1) \equiv 0 \pmod{p}.$$

Abbiamo allora che $0 < a^2 + b^2 + c^2 + d^2 < 2p$ e p divide $a^2 + b^2 + c^2 + d^2$. L'unica possibilità è che valga $p = a^2 + b^2 + c^2 + d^2$, ed il teorema è dimostrato. □

Capitolo 2

Gruppo delle classi

2.1 Lo spazio $V_{\mathbb{F}}$

Sia $\mathbb{F}$ un campo di numeri di grado n e si scelga una sua immersione σ. Diremo che σ è *reale* se $\sigma(\mathbb{F}) \leq \mathbb{R}$, altrimenti σ sarà detta *complessa*. Se σ è un'immersione complessa, anche la sua coniugata $\overline{\sigma}$ è un'immersione complessa ed è distinta da σ. Questo ci dice che le immersioni complesse sono sempre in numero pari. Se indichiamo con s il numero di immersioni reali di $\mathbb{F}$, e con $2t$ il numero di immersioni complesse, abbiamo $n = s + 2t$. Il numero t indica il numero di immersioni complesse *a meno di coniugio*. Ad esempio

- se $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ con $d > 0$ intero libero da quadrati, allora $s = 2, t = 0$;
- se $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ con $d < 0$ intero libero da quadrati, allora $s = 0, t = 1$;
- se $\mathbb{F} = \mathbb{Q}[\omega]$ con ω radice m-esima primitiva di 1, allora $s = 0$ e $t = \varphi(m)/2$.

D'ora in avanti, fissato un campo di numeri di grado n, scrivendo $n = s + 2t$ intenderemo che gli interi s, t sono quelli appena definiti, ovvero il numero di immersioni reali e il numero di immersioni complesse a meno di coniugio. Definiamo lo spazio vettoriale reale

$$V_{\mathbb{F}} = (\oplus_{i=1}^{s} \mathbb{R}) \oplus (\oplus_{i=1}^{t} \mathbb{C}) = \mathbb{R}^s \oplus \mathbb{C}^t.$$

Questo spazio ha dimensione $s + 2t = n$, in quanto ogni addendo del tipo $\mathbb{C}$ è un $\mathbb{R}$-spazio di dimensione 2.

Siano ora $\sigma_1, \sigma_2, \ldots, \sigma_s$ le immersioni reali di $\mathbb{F}$ e, dopo aver selezionato un elemento per ciascuna coppia di immersioni complesse coniugate, indichiamo tali elementi con $\sigma_{s+1}, \sigma_{s+2}, \ldots, \sigma_{s+t}$ (quindi σ_{s+i} e σ_{s+j} non sono mai coniugate se $i \neq j$). Una volta fatta questa scelta abbiamo una funzione $\sigma : \mathbb{F} \longrightarrow V_{\mathbb{F}}$ definita da

$$\sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_s(x), \sigma_{s+1}(x), \ldots, \sigma_{s+t}(x)).$$

La funzione σ dipende dalla scelta delle immersioni complesse. Quando, fissato un campo di numeri $\mathbb{F}$, parleremo di σ, daremo per scontato che tale scelta sia stata effettuata.

La funzione σ è $\mathbb{Q}$-lineare e possiede la seguente importante proprietà

Proposizione 2.1.1 *Se $\mathbb{F}$ è un campo di numeri di grado n e $\{v_1, \ldots, v_n\}$ è una $\mathbb{Q}$-base di $\mathbb{F}$, allora $\{\sigma(v_1), \ldots, \sigma(v_n)\}$ è una $\mathbb{R}$-base di $V_{\mathbb{F}}$.*

Dimostrazione. Iniziamo enumerando le immersioni nel modo consueto $\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \ldots, \sigma_{s+t}$ e ponendo

$$\sigma_l(v_k) = \begin{cases} x_{lk} & \text{se } 1 \leq l \leq s \\ y_{lk} + iz_{lk} & \text{se } s+1 \leq l \leq s+t \end{cases}$$

Consideriamo la matrice M la cui k-esima riga è il vettore $\sigma(v_k) = (\sigma_1(v_k), \ldots, \sigma_{s+t}(v_k))$. Per dimostre il nostro risultato dovremo provare che le righe di M sono indipendenti su $\mathbb{R}$. La matrice M ha n-righe ed $s+t$ colonne. Le ultime t colonne contengono però numeri complessi e possiamo, pertanto, pensarle come due colonne di numeri reali nel senso che, se W è una di tali colonne, la scriviamo come $W = Y + iZ$, con Y, Z vettori reali, e la sostituiamo con la coppia (YZ). Una volta compiuta tale operazione con tutte le colonne complesse, possiamo vedere M come una matrice $n \times n$ a coefficienti reali. Volendo essere espliciti scriviamo

$$M = (X_1 X_2 \cdots X_s Y_{s+1} Z_{s+1} \cdots Y_{s+t} Z_{s+t})$$

dove

$$X_l = \begin{pmatrix} x_{l1} \\ x_{l2} \\ \vdots \\ x_{ln} \end{pmatrix} = \begin{pmatrix} \sigma_l(v_1) \\ \sigma_l(v_2) \\ \vdots \\ \sigma_l(v_n) \end{pmatrix} \quad Y_l = \begin{pmatrix} y_{l1} \\ y_{l2} \\ \vdots \\ y_{ln} \end{pmatrix} \quad \text{e } Z_l = \begin{pmatrix} z_{l1} \\ z_{l2} \\ \vdots \\ z_{ln} \end{pmatrix}$$

Dato che ora M è vista come matrice $n \times n$ possiamo vedere che le sue righe sono indipendenti mostrando che $\det(M) \neq 0$. A questo scopo è conveniente pensare la matrice M a coefficienti in $\mathbb{C}$. Eseguiremo alcune operazioni sulle colonne di M, allo scopo di ottenere una matrice il cui determinante è più semplice da calcolare. Iniziamo prendendo in considerazione la sottomatrice $(Y_l Z_l)$. Al posto di questa sottomatrice inseriamo in M la sottomatrice $(Y_l + iZ_l\, Y_l - iZ_l)$. Se chiamiamo M_1 questa nuova matrice vediamo, usando il fatto che il determinante è una funzione multilineare delle colonne, che vale la relazione $\det(M_1) = (-2i)\det(M)$. Infatti, sostituendo alla colonna Y_l la colonna $Y_l + iZ_l$ il determinante non cambia. Ma, per ottenere la colonna $Y_l - iZ_l$, dobbiamo moltiplicare Z_l per $-2i$ (ed il determinante viene moltiplicato per $-2i$) e quindi aggiungere la colonna $Y_l - iZ_l$ (e questo non cambia il valore del determinante). È importante osservare che

$$Y_l + iZ_l = \begin{pmatrix} \sigma_l(v_1) \\ \sigma_l(v_2) \\ \vdots \\ \sigma_l(v_n) \end{pmatrix} \quad Y_l - iZ_l = \begin{pmatrix} \overline{\sigma_l}(v_1) \\ \overline{\sigma_l}(v_2) \\ \vdots \\ \overline{\sigma_l}(v_n) \end{pmatrix}$$

Una volta eseguito questo processo per ciascuna sottomatrice $(Y_l Z_l)$, otteniamo una nuova matrice M_0 e abbiamo $\det(M_0) = (-2i)^t \det(M)$. Allora $\det(M) \neq 0$ se e solo se $\det(M_0) \neq 0$. Dato che l'insieme delle immersioni di $\mathbb{F}$ è $\{\sigma_i, \sigma_{s+j}, \overline{\sigma_{s+j}} \mid i = 1, \dots, s \quad j = 1, \dots, t\}$, vediamo che, se rinominiamo opportunamente le immersioni come $\{\tau_1, \tau_2, \dots, \tau_n\}$, la matrice M_0 ha, nella posizione ij, l'elemento $\tau_j(v_i)$. Allora $(\det(M_0))^2 = \Delta[v_1, v_2, \dots, v_n]$, e questo è diverso da 0 perché $\{v_1, v_2 \dots, v_n\}$ è una base di $\mathbb{F}$. Quindi anche $\det(M) \neq 0$ e la tesi è dimostrata. □

Se analizziamo con attenzione la dimostrazione della proposizione 2.1.1, possiamo ricavare un corollario di grande utilità in diverse situazioni. Gli interi s, t hanno l'usuale significato.

Corollario 2.1.2 *Siano $\mathbb{F}$ un campo di numeri di grado $n = s + 2t$, I un ideale non nullo di $\mathcal{O}_\mathbb{F}$ e σ l'immersione di $\mathbb{F}$ in $V_\mathbb{F}$. Allora $\sigma(I)$ è un reticolo in $V_\mathbb{F}$ e*

$$\mathrm{cov}(\sigma(I)) = \frac{1}{2^t} N(I) \sqrt{|\Delta_\mathbb{F}|}.$$

Dimostrazione. Sia $\{v_1, v_2 \dots v_n\}$ una base del gruppo additivo di $\mathcal{O}_\mathbb{F}$. L'ideale I, pensato come gruppo additivo, è anche lui libero di rango n, generato da una base $\{w_1, \dots, w_n\}$. Ricordiamo che $\Delta_\mathbb{F} = \Delta[v_1, v_2 \dots v_n]$ e $|\Delta[w_1, \dots, w_n]| = N(I)^2 |\Delta_\mathbb{F}|$. Dato che $\{w_1, \dots, w_n\}$ è un insieme indipendente, è anche una $\mathbb{Q}$-base di $\mathbb{F}$. La proposizione 2.1.1 ci dice che $\{\sigma(w_1), \dots, \sigma(w_n)\}$ è una base di $V_\mathbb{F}$ per cui $\sigma(I) = \sigma(\langle w_1, \dots, w_n \rangle_\mathbb{Z}) = \langle \sigma(w_1), \dots, \sigma(w_n) \rangle_\mathbb{Z}$ è un reticolo in $V_\mathbb{F}$. Dato che

$$\mathrm{cov}(L) = \left| \det \begin{pmatrix} \sigma(w_1) \\ \sigma(w_2) \\ \vdots \\ \sigma(w_n) \end{pmatrix} \right|$$

la dimostrazione precedente dice che

$$\mathrm{cov}(L) = \frac{1}{2^t} \sqrt{|\Delta[w_1, \dots, w_n]|} = \frac{1}{2^t} N(I) \sqrt{|\Delta_\mathbb{F}|}$$

come volevamo dimostrare. □

2.2 Finitezza del gruppo delle classi

In questa sezione dimostreremo un risultato di grande importanza, ovvero che il gruppo delle classi per un campo di numeri è finito.

Sia $x = (x_1, \dots, x_{s+t}) \in V_\mathbb{F}$, scegliamo una sua coordinata x_i e poniamo $\|x_i\| = \sqrt{x\overline{x}}$. Osserviamo che, se $x_i \in \mathbb{R}$ (cosa che accade ad esempio quando $i \leq s$), allora $\|x_i\| = |x_i|$. Per ogni numero reale c definiamo

$$\Omega(c) = \left\{ x \in V_\mathbb{F} \;\middle|\; \sum_{i=1}^{s} \|x_i\| + 2 \sum_{i=1}^{t} \|x_{s+i}\| \leq c \right\}.$$

L'insieme $\Omega(c)$ è limitato, simmetrico e convesso ed è importante conoscerne la misura.

Lemma 2.2.1 *Se $n = s + 2t$ e c è un numero reale strettamente positivo, si ha*

$$\mu(\Omega(c)) = 2^s \Big(\frac{\pi}{2}\Big)^t \frac{c^n}{n!}.$$

DIMOSTRAZIONE. Per induzione su $s + t$.

Se $s + t = 1$ dobbiamo considerare due casi. Quando $s = 1$ e $t = 0$, allora $\Omega(c) = \{\, x \in \mathbb{R} \mid |x| \leq c \,\}$ ed è evidente che la misura di questo insieme è $2c$. Se, invece, $s = 0$ e $t = 1$, abbiamo $\Omega(c) = \{\, x \in \mathbb{C} \mid 2\|x\| \leq c \,\}$. Quindi $\Omega(c)$ è un disco di raggio $c/2$ e la sua misura vale $\pi c^2/4 = (\pi/2)(c^2/2)$.

Veniamo allora al passo induttivo, la cui dimostrazione deve essere divisa in due parti. Dobbiamo provarlo nel caso sia la variabile s a crescere, e nel caso in cui cresca la variabile t.

Caso 1. $s \longmapsto s + 1$.

In questo caso $n = s + 1 + 2t$. Abbiamo

$$\mu(\Omega(c)) = \int_{\Omega(c)} d\mu = \int_{-c}^{c} \mu(\Omega(c - |x_1|)dx_1$$

e, sfruttando l'ipotesi induttiva,

$$\int_{-c}^{c} \mu(\Omega(c - |x_1|))dx_1 = \int_{-c}^{c} 2^s \Big(\frac{\pi}{2}\Big)^t \frac{(c - |x_1|)^{n-1}}{(n-1)!} dx_1 = 2^s \Big(\frac{\pi}{2}\Big)^t \frac{1}{(n-1)!} \int_{-c}^{c} (c - |x_1|)^{n-1} dx_1$$

da cui la tesi segue immediatamente.

Caso 2. $t \longmapsto t + 1$.

Se indichiamo con z_1 la prima delle componenti complesse e poniamo $n = s + 2(t + 1)$, abbiamo

$$\mu(\Omega(c)) = \int_{\Omega(c)} d\mu = \int_{\|z_1\| \leq c/2} \mu(\Omega(c - 2\|z_1\|)dz_1 = 2^s \Big(\frac{\pi}{2}\Big)^t \frac{1}{(n-2)!} \int_{\|z_1\| \leq c/2} (c - 2\|z_1\|)^{n-2} dz_1$$

dove, per l'ultima uguaglianza, abbiamo usato l'ipotesi induttiva. Possiamo concentrarci allora nel calcolo dell'ultimo integrale. Passando alle coordinate polari ρ, θ, si ottiene

$$\int_{\|z_1\| \leq c/2} (c - 2\|z_1\|)^{n-2} dz_1 = \int_0^{2\pi} \int_0^{c/2} (c - 2\rho)^{n-2} \rho d\theta d\rho = 2\pi \int_0^{c/2} (c - 2\rho)^{n-2} \rho d\rho.$$

Ponendo $t = c - 2\rho$ si ottiene facilmente che il valore che stiamo cercando è $\pi c^n/2(n-1)n$. Ne segue che, anche in questo caso, la tesi è vera ed il lemma è dimostrato. □

Useremo la seguente (e ben nota) disguaglianza tra media geometrica e media aritmetica.

Lemma 2.2.2 *Se $a_1, a_2, \ldots, a_N$ sono sumeri reali positivi, allora $(\prod_{i=1}^N a_i)^{1/N} \leq (\sum_{i=1}^N a_i)/N$.*

Il prossimo risultato dice, in sostanza, che ogni ideale non nullo in un anello di numeri contiene elementi diversi da 0 e di norma *piccola*.

Proposizione 2.2.3 *Siano $\mathbb{F}$ un campo di numeri di grado $n = s + 2t$ ed I un ideale non nullo di $\mathcal{O}_{\mathbb{F}}$. Allora esiste $\alpha \in I$ tale che $\alpha \neq 0$ e*

$$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} N(I)\sqrt{|\Delta_{\mathbb{F}}|}.$$

Dimostrazione. Facciamo riferimento alle notazioni introdotte nel Lemma 2.2.1. Per ogni naturale $k > 0$ definiamo il numero reale c_k tramite la relazione

$$\mu(\Omega(c_k)) = 2^n \frac{1}{2^t} N(I)\sqrt{|\Delta_{\mathbb{F}}|} + \frac{1}{k}.$$

La successione formata dai c_k è decrescente, come la successione degli insiemi $\Omega(c_k)$ e, definito c tramite l'uguaglianza

$$2^s \left(\frac{\pi}{2}\right)^t \frac{c^n}{n!} = 2^n \frac{1}{2^t} N(I)\sqrt{|\Delta_{\mathbb{F}}|},$$

abbiamo $\Omega(c) = \bigcap_{k=1}^{\infty} \Omega(c_k)$.

L'intersezione tra $\Omega(c_k)$ ed il reticolo $\sigma(I)$ è finita, essendo $\Omega(c_k)$ limitato, quindi per qualche $\overline{k}$ si deve avere

$$\sigma(I) \cap \Omega(c_{\overline{k}}) = \sigma(I) \cap \Omega(c_k) \qquad \text{per ogni } k \geq \overline{k}$$

Dato che, per costruzione, $2^n \mathrm{cov}(\sigma(I)) < \mu(\Omega(c_k))$ per ogni k, il Teorema di Minkowski ci assicura che l'insieme $\sigma(I) \cap \Omega(c_{\overline{k}})$ contiene almeno un elemento diverso da 0. Pertanto

$$\sigma(I) \cap \Omega(c) = \sigma(I) \cap \Big(\bigcap_{k=1}^{\infty} \Omega(c_k)\Big) = \sigma(I) \cap \Big(\bigcap_{k \geq \overline{k}} \Omega(c_k)\Big) = \sigma(I) \cap \Omega(c_{\overline{k}})$$

contiene almeno un elemento diverso da 0, che avrà la forma $\sigma(\alpha)$ per un opportuno $\alpha \in I$. Se elenchiamo le immersioni di $\mathbb{F}$ come $\tau_1, \tau_2, \ldots, \tau_n$ vediamo che $\sum_{i=1}^{n} \|\tau_i(\alpha)\| = \sum_{i=1}^{s} \|\sigma_i(\alpha)\| + 2\sum_{i=1}^{t} \|\sigma_{s+i}(\alpha)\| \leq c$. Usando il Lemma 2.2.2 troviamo

$$|N(\alpha)| = |\prod_{i=1}^{n} \tau_i(\alpha)| = \prod_{i=1}^{s} |\sigma_i(\alpha)| \cdot \prod_{i=1}^{t} \sigma_{s+i}(\alpha) \cdot \prod_{i=1}^{t} \overline{\sigma_{s+i}(\alpha)} \leq \left(\frac{\sum_{i=1}^{n} \|\tau_i(\alpha)\|}{n}\right)^n \leq \frac{c^n}{n^n}.$$

Usando il modo in cui è stato definito c, ricaviamo

$$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} N(I)\sqrt{|\Delta_{\mathbb{F}}|}.$$

La proposizione è quindi dimostrata. □

Prima di dimostrare il teorema principale, ci servono altri due semplici lemmi.

Lemma 2.2.4 *Siano $\mathbb{F}$ un campo di numeri e $\alpha \in \mathcal{O}_{\mathbb{F}}$ un elemento diverso da 0. Se I è l'ideale generato da α allora $N(I) = |N(\alpha)|$.*

DIMOSTRAZIONE. Fissiamo $v_1, v_2, \dots v_n$ una base per $\mathcal{O}_\mathbb{F}$ per cui ogni intero algebrico si può scrivere come $\sum_{i=1}^n a_i v_i$ con $a_i \in \mathbb{Z}$ per ogni i . Un generico elemento di I ha la forma $\alpha(\sum_{i=1}^n a_i v_i) = \sum_{i=1}^n a_i(\alpha v_i)$ e pertanto $I = \{ \sum_{i=1}^n a_i(\alpha v_i) \mid a_i \in \mathbb{Z} \forall\, i \}$. In altri termini l'ideale I, pensato come gruppo abeliano, è generato dall'insieme $\{\alpha v_1, \alpha v_2, \dots, \alpha v_n\}$ e quindi vale la relazione

$$|\Delta[\alpha v_1, \dots, \alpha v_n]| = N(I)\sqrt{|\Delta_\mathbb{F}|}.$$

Se indichiamo con $\sigma_1, \sigma_2, \dots \sigma_n$ le immersioni di $\mathbb{F}$ abbiamo le seguente relazione

$$M = \begin{pmatrix} \sigma_1(\alpha v_1) & \dots & \sigma_1(\alpha v_n) \\ \sigma_2(\alpha v_1) & \dots & \sigma_2(\alpha v_n) \\ \dots & \dots & \dots \\ \sigma_n(\alpha v_1) & \dots & \sigma_n(\alpha v_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) & \dots & 0 \\ 0 & \sigma_2(\alpha) & 0 \\ 0 & \dots & 0 \\ 0 & \dots & \sigma_n(\alpha) \end{pmatrix} \begin{pmatrix} \sigma_1(v_1) & \dots & \sigma_1(v_n) \\ \sigma_2(v_1) & \dots & \sigma_2(v_n) \\ \dots & \dots & \dots \\ \sigma_n(v_1) & \dots & \sigma_n(v_n) \end{pmatrix}$$

da cui ricaviamo $\Delta[\alpha v_1, \dots, \alpha v_n] = (\det(M))^2 = N(\alpha)^2 \Delta_\mathbb{F}$. La tesi segue immediatamente. □

Lemma 2.2.5 *Se $\mathbb{F}$ è un campo di numeri ed N è un numero reale positivo, gli ideali di $\mathcal{O}_\mathbb{F}$ di norma minore di N sono un numero finito.*

DIMOSTRAZIONE. Dato che ogni ideale è prodotto di primi e che la norma è moltiplicativa, è sufficiente provare che $\mathcal{O}_\mathbb{F}$ possiede solo un numero finito di ideali primi di norma minore di N. Sia allora n il grado di $\mathbb{F}$ e si scelga $\mathcal{P}$ un ideale primo di norma minore di N. L'ideale $\mathcal{P}$ contiene un unico primo razionale, individuato dalla relazione $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, quindi l'ideale $p\mathcal{O}_\mathbb{F}$ è contenuto in $\mathcal{P}$. Questo ci dice the $N(\mathcal{P})$ divide $N(p\mathcal{O}_\mathbb{F}) = p^n$ e ne segue che $p \leq N$. Pertanto i primi di norma minore di N sono tra quelli che dividono gli ideali del tipo $p\mathcal{O}_\mathbb{F}$ con p primo e $p \leq N$. Questi primi sono, ovviamente, in numero finito. □

Possiamo finalmente dimostrare che, per ogni campo di numeri, il gruppo delle classi è finito

Teorema 2.2.6 *Sia $\mathbb{F}$ un campo di numeri. Allora il suo gruppo delle classi è finito.*

Dimostrazione Iniziamo scrivendo il grado di $\mathbb{F}$ come $n = s + 2t$ e ponendo

$$M_{st} = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}.$$

Questo numero è detto *costante di Minkowski* e dipende solo da $\mathbb{F}$. Se $G = \mathcal{C}l(\mathbb{F})$ è il gruppo delle classi di $\mathbb{F}$ e $\omega \in G$, osserviamo che ω contiene un ideale di $\mathcal{O}_\mathbb{F}$. Infatti, preso $J \in \omega$ un qualsiasi ideale frazionario, esiste $0 \neq a \in \mathbb{F}$ tale che $I = aJ \subseteq \mathcal{O}_\mathbb{F}$. Quindi I è ideale di $\mathcal{O}_\mathbb{F}$ e, indicando con $[\cdot]$ la classe di un ideale in G, abbiamo, $[I] = [J(a)] = [J][(a)] = [J] = \omega$. Il punto centrale della dimostrazione sarà provare che ogni classe $\omega \in G$ contiene un ideale I con $N(I) \leq M_{st}\sqrt{|\Delta_\mathbb{F}|}$. A tale scopo prendiamo la classe ω^{-1} e scegliamo un ideale $J \in \omega^{-1}$. Per il Lemma 2.2.3, esiste $0 \neq \alpha \in J$ tale che $|N(\alpha)| \leq M_{st} N(J)\sqrt{|\Delta_\mathbb{F}|}$. Dato che $(\alpha) \subseteq J$ abbiamo $J \mid (\alpha)$ e quindi esiste un ideale I tale che $IJ = (\alpha)$. Passando alle classi in G si ottiene

$[IJ] = [(\alpha)] = 1$ e quindi $[I][J] = 1$, da cui, ricordando che $[J] = \omega^{-1}$, si vede che $[I] = \omega$. Considerando le norme otteniamo $N((\alpha)) = N(IJ) = N(I)N(J)$ e quindi, usando il Lemma 2.2.4,

$$N(I)N(J) = N((\alpha)) = |N(\alpha)| \leq M_{st}N(J)\sqrt{|\Delta_{\mathbb{F}}|}.$$

Dividendo per $N(J)$ otteniamo $N(I) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$. Abbiamo cioè provato che, per ogni classe $\omega \in G$, esiste un ideale $I \in \omega$ tale che $N(I) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$. Allora

$$G = \{\, [I] \mid I \text{ è ideale di } \mathcal{O}_{\mathbb{F}} \,\} = \{\, [I] \mid I \text{ è ideale di } \mathcal{O}_{\mathbb{F}} \text{ e } N(I) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|} \,\}.$$

Ma, per il Lemma 2.2.6, solo un numero finito di ideali di $\mathcal{O}_{\mathbb{F}}$ ha norma minore di $M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$ e questo prova che il gruppo G è finito. □.

C'è un utile e semplice corollario.

Corollario 2.2.7 *Se $\mathbb{F}$ è un campo di numeri di grado $n = s + 2t$, allora $\mathcal{O}_{\mathbb{F}}$ è un UFD se e solo se ogni ideale primo $\mathcal{P}$ tale che $N(\mathcal{P}) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$ è principale.*

Dimostrazione. Se $\mathcal{O}_{\mathbb{F}}$ è UFD allora è anche un PID, quindi ogni suo ideale è principale. Viceversa assumiamo di sapere solo che i primi di norma minore di $M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$ sono principali. Il gruppo dell classi di $\mathbb{F}$ si può descrivere, per quanto visto sopra, come $G = \{\, [I] \mid N(I) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|} \,\}$ e quindi, dato che ogni ideale si decompone nel prodotto di primi,

$$G = \langle\, [\mathcal{P}] \mid \mathcal{P} \text{ è primo e } N(\mathcal{P}) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|} \,\rangle.$$

Ma, nelle nostre ipotesi, $[\mathcal{P}] = 1$ se il primo $\mathcal{P}$ ha norma minore di $M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$, di conseguenza G è il gruppo banale e $\mathcal{O}_{\mathbb{F}}$ è UFD. □

2.3 Alcuni esempi

Calcoliamo, in questa sezione, il gruppo delle classi in alcuni casi particolari. Da quanto provato nella sezione precedente sembra utile, nello studiare il gruppo delle classi di un campo di numeri $\mathbb{F}$, conoscere il valore del numero $M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$. Ci tornerà utile la seguente tabella nella quale, per campi del tipo $\mathbb{Q}[\sqrt{d}]$, valutiamo questa costante (il valore è approssimato per eccesso).

d	$\Delta_{\mathbb{F}}$	$M_{st}\sqrt{\lvert\Delta_{\mathbb{F}}\rvert}$
2	8	1.42
3	12	1.74
5	5	1.12
10	40	3.17
-1	-4	1.28
-5	-20	2.85
-7	-7	1.69
-19	-19	2.78
-14	-56	4.77
-21	-84	5.9

Quando il valore $M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$ è strettamente minore di 2 l'anello degli interi è un UFD, dato che ogni ideale primo (anzi ogni ideale proprio) deve avere norma almeno 2. Ne segue che, per quanto riguarda gli esempi riportati sopra, $\mathcal{O}_{\mathbb{F}}$ è UFD (e quindi un PID) quando $\mathbb{F} \in \{\, \mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}], \mathbb{Q}[\sqrt{5}], \mathbb{Q}[\sqrt{-1}], \mathbb{Q}[\sqrt{-7}] \,\}$. Il caso $\mathbb{Q}[\sqrt{5}]$ è particolarmente interessante. L'anello degli interi, in questo caso $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, è un PID ma ha un sottoanello, $\mathbb{Z}[\sqrt{5}]$, che non è un UFD.

Analizziamo alcuni casi.

1. $d = 10$.

Cerchiamo gli ideali di norma minore di 3.17. Questi, se esistono, devono aveer norma 2 o 3 e sono quindi da cercare tra i divisori degli ideali (2) e (3). L'anello degli interi è $\mathbb{Z}[\sqrt{10}]$ ed il polinomio minimo di $\sqrt{10}$ è $x^2 - 10$. allora 2 si ramifica totalmente mentre 3 si spezza completamente. La decomposizione è la seguente

$$(2) = (2, \sqrt{10})^2 \quad (3) = (3, 1 + \sqrt{10})(3, 1 - \sqrt{10}).$$

L'ideale $((2, \sqrt{10})$ ha quindi norma 2 e, se fosse principale, sarebbe generato da un elemento $a + b\sqrt{10}$ di norma 2. Ma l'equazione diofantea $a^2 - 10b^2 = \pm 2$ non ha soluzioni, dato che la congruenza $a^2 \equiv \pm 2 \pmod 5$ non ha soluzioni. Questo ci dice, intanto, che il gruppo delle classi non è banale. In modo analogo si prova che anche gli ideali $(3, 1 + \sqrt{10})$ e $(3, 1 - \sqrt{10})$ non sono principali. Abbiamo anche che $[(3, 1+\sqrt{10})] = [(3, 1-\sqrt{10})]^{-1}$ visto che $(3, 1+\sqrt{10})(3, 1-\sqrt{10}) = (3)$ è un ideale principale. Se calcoliamo il quadrato di $(3, 1 + \sqrt{10})$ otteniamo

$$(3, 1 + \sqrt{10})^2 = (9, 3 + 3\sqrt{10}, 11 + 2\sqrt{10}) = (9, 3 + 3\sqrt{10}, 2 + 2\sqrt{10}) = (9, 1 + \sqrt{10}) = (1 + \sqrt{10})$$

da cui ricaviamo $h^2 = 1$ e $h = h^{-1}$. In definitiva il gruppo delle classi G è $G = 1, g, h$ dato che g, h sono le uniche classi non banali ad avere un rappresentante di norma minore di 3.17. Dobbiamo a questo punto osservare che G non può avere ordine 3, dato che possiede elementi di ordine 2. Sapendo che G non è banale, ne deduciamo che G è ciclico di ordine 2. In particolare

$g = h$ e $gh = 1$. Questo ci dice che l'ideale $I = (2, \sqrt{10})(3, 1 + \sqrt{10})$ deve essere principale. Proviamo a verificarlo direttamente. Eseguendo il prodotto si ottiene

$$I = (6, 2 + 2\sqrt{10}, 3\sqrt{10}, 10 + \sqrt{10}) = (6, 2 + 2\sqrt{10}, 3\sqrt{10}, 9\sqrt{10})$$

da cui si osserva che $\alpha = 2 - \sqrt{10} = (2 + 2\sqrt{10}) - 3\sqrt{10}$ appartiene ad I. Pertanto $N((\alpha))$ divide $N(I)$. Ma $N((\alpha)) = |N(\alpha)| = 6$ e $N(I) = N((2, \sqrt{10}))N((3, 1 + \sqrt{10})) = 2 \cdot 3 = 6$. Di conseguenza $I = (\alpha)$.

2. $d = -19$.

In questo caso l'anello degli interi è $\mathbb{Z}[\omega]$ dove $\omega = \frac{1+\sqrt{-19}}{2}$. Come prima cerchiamo gli ideali di norma minore di 2.78 e, analogamente al caso precedente, vediamo che gli unici ideali di questo genere vanno cercati tra i divisori dell'ideale (2). Ma 2 è inerte e quindi ogni ideale ha norma maggiore o uguale a 3. Per questo motivo $\mathbb{Z}[\omega]$ è un PID. Questo anello ci interessa particolarmente perché, usando un risultato dimostrato in [8], si vede che $\mathbb{Z}[\omega]$ non è un dominio euclideo per ogni possibile scelta di una funzione norma. In questo modo abbiamo, finalmente, un esempio di un PID che non sia un dominio euclideo.

3. $d = -14$.

L'anello degli interi è $\mathbb{Z}[\omega]$ dove $\omega = \sqrt{-14}$ ed il gruppo delle classi è $G = \{\ [I]\ \mid N(I) \leq 4.77\ \}$. Gli ideali la cui norma soddisfa questa condizione sono da ricercare tra i divisori degli ideali (2) e (3). Questi ideali si fattorizzano come $(2) = (2, \omega)^2$ e $(3) = (3, 1 + \omega)(31 - \omega)$. Dato che, come si verifica immediatamente, nessun elemento di $\mathbb{Z}[\omega]$ ha norma 2 o 3, i fattori primi che compaiono in queste fattorizzazioni non sono principali. Posto $h = [((2, \omega)]$, $g = [(3, 1 + \omega)]$, vediamo subito che $h^2 = 1$ (perché $(2, \omega)^2$ è principale) e che $g^{-1} = [(3, 1 - \omega)]$ ((perché $(3, 1 + \omega)(3, 1 - \omega)$ è principale). Abbiamo quindi $G = \{\ 1,\ h,\ g,\ g^{-1}\ \}$, visto che gli unici ideali di norma minore o uguale a 4 sono (2), i suoi fattori primi ed i fattori primi di (3). Allora G ha ordine pari (contiene un elemento di periodo 2) e minore o uguale a 4. Se G avesse ordine 2, si avrebbe $g = h$ per cui $gh = 1$. Dal punto di vista degli ideali questo vuol dire che $I = (2, \omega)(3, 1 + \omega)$ è principale. Ma la norma di I è 6 e, dato che nessun elemento di $\mathbb{Z}[\omega]$ può avere norma 6, ne segue che I non è principale. Allora G ha ordine 4 e le due possibilità sono che G sia un gruppo d Klein oppure un gruppo ciclico. Se G fosse un gruppo di Klein anche g avrebbe ordine 2, per cui G conterrebbe tre elementi, una contraddizione. Di conseguenza G è ciclico di ordine 4.

4. $d = -21$.

In questo caso il gruppo delle classi è $G = \{\ [I]\ \mid N(I) \leq 5.9\ \}$ e conviene inizare il nostro studio determinandone i generatori, ovvero le classi dei primi di norma minore di 5.9. Questi vanno cercati tra i divisori degli ideali (p) con $p = 2, 3, 5$. L'anello degli interi è $\mathbb{Z}[\sqrt{-21}]$ e si vede che 2 e 3 sono ramificati, mentre 5 si spezza. Posto $\omega = \sqrt{-21}$ abbiamo le seguenti fattorizzazioni:

$$(2) = (2, 1 + \omega)^2, \quad (3) = (3, \omega)^2 \quad (5) = (5, 1 + \omega)(5, 1 - \omega)$$

ed i fattori primi hanno norma, rispettivamente, $2, 3$ e 5. Dato che le equazioni diofantee $x^2 + 21y^2 = 2, 3, 5$ non hanno soluzione, non esistono elementi di norma $2, 3$ o 5 e quindi gli ideali $I = (2, 1 + \omega), J = (3, \omega), K = (5, 1 + \omega)$ e $H = (5, 1 - \omega)$ non sono principali. Dato che il quadrato degli ideali $(2, 1 + \omega)$ e $(3, \omega)$ è principale, le classi di questi ideali sono elementi di periodo 2 del gruppo delle classi G. Inoltre presi due elementi distinti $U, V \in \{ I, J, K, H \}$ la norma del loro prodotto è almeno 6 e quindi supera la costante 5.9. Ne deduciamo che $G = \{ 1, [I], [J], [K], [H] \}$. Ma, dato che G possiede elementi di perido 2, il suo ordine deve essere pari e, d conseguenza, G ha ordine 2 o 4. Sia $L = IJ$. Questo è un ideale di norma 6 e, se fosse principale, sarebbe generato da un elemento $a + b\omega$ di norma 6. Ma l'equazione diofantea $x^2 + 21y^2 = 6$ non ha soluzioni, quindi nessun elemento ha norma 6 e, conseguentemente, l'ideale L non è principale. Questo ci dice che G ha almeno due elementi di ordine due (ad esempio $[I]$ e $[J]$) ed avendo ordine minore di 4 deduciamo che G è isomorfo al gruppo di Klein $C_2 \times C_2$.

2.4 Equazione di Nagell-Ramanujan

In questa sezione useremo gli strumenti che abbiamo sviluppato, per risolvere una particolare equazione diofantea. Nel 1913 Ramanujan aveva congetturato che le soluzioni dell'equazione diofantea $x^2 + 7 = 2^n$ fossero solo quelle riportate nella seguente tabella

$\pm x$	n
1	3
3	4
5	5
11	7
181	15

La congettura di Ramanujan è stata in seguito confermata da Nagell in [6]. Dimostreremo questo fatto seguendo la dimostrazione riportata nel capitolo 4 di [11].

Iniziamo con un lemma che riguarda le unità di certi anelli quadratici.

Lemma 2.4.1 *Siano d un intero negativo e libero da quadrati e $U(d)$ il gruppo delle unità dell'anello degli interi di $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$. Allora*

1. $U(-1) = \{ \pm 1, \pm i \}$;
2. $U(-3) = \{ \pm 1, \pm\varepsilon, \pm\varepsilon^2 \}$ *con ε radice terza primitiva di 1;*
3. $U(d) = \{ \pm 1 \}$ *negli altri casi.*

Dimostrazione. Sia $\alpha \in \mathcal{O}_{\mathbb{F}}$ un invertibile. Sappiamo allora che $N(\alpha) = \pm 1$, ma essendo $N(\alpha) = \alpha\overline{\alpha}$, deve essere $N(\alpha) = 1$. L'elemento α si scrive come $a + b\sqrt{d}$ per una unica scelta di $a, b \in \mathbb{Q}$. Se $d \equiv 2, 3 \pmod 4$ allora a, b sono interi, altrimenti a, b appartengono a $\frac{1}{2}\mathbb{Z}$. La norma

di α vale $a^2+|d|b^2$ e quindi, se d è congruo a 2 o 3 modulo 4, b deve essere 0 non appena $|d|>1$. Questo prova che $U(d)=\{\pm 1\}$ quando $d\equiv 2,3 \pmod 4$ e $d\neq -1$. Se $d=-1$ l'equazione diofantea $a^2+b^2=1$ ammette le soluzioni $(\pm 1,0),(0,\pm 1)$ provando che $U(-1)=\{\pm 1,\pm i\}$. Veniamo allora al caso $d\equiv 1 \pmod 4$. Possiamo scrivere $a=A/2$, $b=B/2$ per opportuni interi A,B e la nostra equazione diventa $A^2+|d|B^2=4$. Se $|d|>3$ abbiamo che deve valere $|d|\geq 5$ e, pertanto, $B=0$. Da questo si ottiene $a=\pm 1$, confermando che $U(d)=\{\pm 1\}$ quando $d\neq -1,-3$. Rimane allora il caso $d=-3$ che porta all'equazione diofantea $A^2+3B^2=4$. Chiaramente $|B|\leq 1$, quindi è sufficiente controllare le soluzioni delle due equazioni $A^2=4$ e $A^2+3=4$. Si ottengono allora le soluzioni $(A,B)=(\pm 2,0),(\pm 1,\pm 1)$ che, a loro volta, ci danno $U(-3)=\{\pm 1,\pm\varepsilon,\pm\varepsilon^2\}$, visto che $\varepsilon=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$. □

Torniamo allo studio della nostra equazione, esaminando il caso in cui n è pari. Scrivendo $n=2m$ la nostra equazione assume la forma $(2^m)^2-x^2=7$ e quindi $(2^m-x)((2^m+x)=7$. Per l'unicità della fattorizzazione in $\mathbb{Z}$ questa equazione è equivalente ai seguenti sistemi

$$\begin{cases} 2^m-x=1 \\ 2^m+x=7 \end{cases} \quad \begin{cases} 2^m-x=7 \\ 2^m+x=1 \end{cases} \quad \begin{cases} 2^m-x=-1 \\ 2^m+x=-7 \end{cases} \quad \begin{cases} 2^m-x=-7 \\ 2^m+x=-1 \end{cases}$$

I primi due sistemi hanno soluzioni $(x,m)=(\pm 3,2)$ mentre gli ultimi due non hanno soluzioni. Tornando alla nostra equazione otteniamo le soluzioni $(\pm 3,4)$. Possiamo quindi assumere n dispari e, dato che per $n=3$ otteniamo $x=\pm 1$ possiamo supporre, d'ora in avanti, $n\geq 5$. Supponiamo che (a,n) sia una soluzione.

Se $m=n-2$ abbiamo la relazione

$$\frac{a^2+7}{4}=2^m$$

e, pensando di lavorare in $\mathbb{F}=\mathbb{Q}[\sqrt{-7}]$, possiamo scrivere

$$\frac{a+\sqrt{-7}}{2}\,\frac{a-\sqrt{-7}}{2}=2^m$$

e gli elementi $\frac{a\pm\sqrt{-7}}{2}$ sono interi algebrici di $\mathbb{F}$. Abbiamo visto nel capitolo precedente, che l'anello $\mathcal{O}_{\mathbb{F}}=\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ è un PID e quindi a fattorizzazione unica. Possiamo allora fattorizzare $2=(\frac{1+\sqrt{-7}}{2})(\frac{1-\sqrt{-7}}{2})$ e ciascuno dei due fattori è primo, visto che entrambi hanno norma 2. Tornando alla relazione precedente abbiamo

$$\frac{a+\sqrt{-7}}{2}\,\frac{a-\sqrt{-7}}{2}=\alpha^m\,\overline{\alpha}^m$$

dove $\alpha=(1+\sqrt{-7})/2$ è uno dei fattori primi di 2. Poniamo, per comodità di notazioni, $\omega=\sqrt{-7}$. Dato che siamo in un dominio a fattorizzazione unica, i due interi algebrici $(a\pm\omega)/2$ sono divisibili solo per α e $\overline{\alpha}$ e, se avessero un fattore comune, avremmo che α o $\overline{\alpha}$ dividerebbero $(a+\omega)/2-(a-\omega)/2=\omega$. Questo non può accadere perché $N(\alpha)=2$ e quindi non divide $N(\omega)=7$. Sfruttando l'unicità della fattorizzazione e il fatto che, per il Lemma 2.4.1, gli unici

elementi invertibili di $\mathcal{O}_{\mathbb{F}}$ sono ± 1, otteniamo

$$\begin{cases} \dfrac{a+\sqrt{-7}}{2} = \alpha^n \\ \dfrac{a-\sqrt{-7}}{2} = \overline{\alpha}^n \end{cases} \qquad \text{oppure} \qquad \begin{cases} \dfrac{a+\sqrt{-7}}{2} = -\alpha^n \\ \dfrac{a-\sqrt{-7}}{2} = -\overline{\alpha}^n. \end{cases}$$

Ci sono, in realtà , altre due possibilità che si ottengono scambiando α e $\overline{\alpha}$. Questo porterebbe a determinare, al termine della dimostrazione, l'intero $-a$ invece di a. Possiamo quindi limitarci a considerare solo questi due casi. Deduciamo che $\alpha^m - \overline{\alpha}^m = \pm\omega$ e il prossimo obiettivo che ci poniamo è decidere quale sia il segno corretto. Faremo vedere, ragionando per assurdo, che $\alpha^m - \overline{\alpha}^m = -\omega$. Supponiamo quindi $\alpha^m - \overline{\alpha}^m = \omega$. Partendo dalla relazione $\alpha + \overline{\alpha} = 1$ e prendendone il quadrato, si ottiene

$$1 = \alpha^2 + \overline{\alpha}^2 + 2\alpha\overline{\alpha} = \alpha^2 + \overline{\alpha}^2 + (\alpha\overline{\alpha})\alpha\overline{\alpha} = \alpha^2 + \overline{\alpha}^2 + \alpha^2\overline{\alpha}^2$$

e quindi $\alpha^2 \equiv 1 \pmod{\overline{\alpha}^2}$. Da questo si ottiene $\alpha^t \equiv 1 \pmod{\overline{\alpha}^2}$ per ogni t dispari maggiore o uguale a 3. Notiamo ora che $\alpha - \overline{\alpha} = \omega = \alpha^m - \overline{\alpha}^m$ e ricaviamo,

$$\alpha - \overline{\alpha} = \alpha^m - \overline{\alpha}^m \equiv \alpha \pmod{\overline{\alpha}^2}$$

e $\overline{\alpha} \equiv 0 \pmod{\overline{\alpha}^2}$ che è una evidente contraddizione. Possiamo allora dire che $\alpha^m - \overline{\alpha}^m = -\omega$, ovvero

$$\begin{cases} \dfrac{a+\sqrt{-7}}{2} = -\alpha^m \\ \dfrac{a-\sqrt{-7}}{2} = -\overline{\alpha}^m. \end{cases}$$

Espandendo le potenze abbiamo

$$-\omega = \alpha^m - \overline{\alpha}^m = \frac{1}{2^m}\left\{ \left(\sum_{j=0}^{m} \binom{m}{j} \omega^j \right) - \left(\sum_{j=0}^{m} \binom{m}{j} (-1)^j \omega^j \right) \right\} = \frac{1}{2^{m-1}} \sum_{\substack{j \le m \\ \text{dispari}}} \binom{m}{j} \omega^j$$

e, moltiplicando per $2^{m-1}/\omega$,

$$\sum_{\substack{j \le m \\ \text{dispari}}} \binom{m}{j} \omega^{j-1} = -2^{m-1}.$$

Quando $j \geq 3$ ciascuno dei termini ω^{j-1} è multiplo di 7 e, passando alle congruenze, otteniamo

$$-2^{m-1} = \sum_{\substack{j \le m \\ \text{dispari}}} \binom{m}{j} \omega^{j-1} \equiv m \pmod{7}.$$

Supponiamo che $(a_1, n_1), (a_2, n_2)$ siano due soluzioni con $n_1 \neq n_2$ ma$n_1 \equiv n_2 \pmod 7$. Posto $m_i = n_i - 2$ abbiamo che entrambi questi interi soddisfano la congruenza $m_i \equiv -2^{m_i - 1} \pmod 7$.

Dato che gli m_i sono dispari abbiamo che $m_1 - m_2$ è pari e quindi è un multiplo di 14. Inoltre $2^{m_1-1} \equiv 2^{m_2-1} \pmod 7$ per cui $m_1 - m_2$ è multiplo di 3 che è l'ordine di $2 + 7\mathbb{Z}$ nel

gruppo moltiplicativo del campo $\mathbb{Z}/7\mathbb{Z}$. In definitiva $2 \cdot 3 \cdot 7 = 42$ divide $m_1 - m_2$. Si controlla manualmente che, se (a, n) è una soluzione con n dispari ed $n - 2 \in [0, 42)$ allora $n = 3, 5, 7$ o 15. Per concludere la dimostrazione rimane solo da dimostrare che non ci sono soluzioni (a, n) per cui $n - 2$ non appartiene all'intervallo $[0, 42)$.

Ci serve ora un risultato tecnico.

Lemma 2.4.2 *Siano $a \in \mathcal{O}_{\mathbb{F}}$ ed $s = 7^k l \in \mathbb{N}$ con $7 \nmid l$. Allora $(1 + a\omega)^s \equiv 1 + sa\omega \pmod{7^{k+1}}$.*

Dimostrazione. Induzione su k. Se $k = 0$ usiamo la formula del binomio di Newton e otteniamo

$$(1 + a\omega)^s = 1 + \binom{s}{1} a\omega + \sum_{2 \le j \le s} \binom{s}{j} a^j \omega^j$$

e, dato che ω^j è un multiplo di 7 per ogni $j \ge 2$, $(1 + a\omega)^s \equiv 1 + sa\omega \pmod{7}$.

Supponiamo la tesi vera fino per $k - 1$. Esiste allora $b \in \mathcal{O}_{\mathbb{F}}$ tale che

$$(1 + a\omega)^{s/7} = 1 + \frac{s}{7} a\omega + 7^k b = \eta + 7^k b.$$

Usiamo nuovamente il binomio di Newton per ottenere

$$(1 + a\omega)^s = \left((1 + a\omega)^{s/7}\right)^7 = \left(\eta + 7^k b\right)^7 = \eta^7 + \sum_{i=2}^{7} \binom{7}{i} \eta^{7-i} (7^k b)^i.$$

Concentriamo la nostra attenzione sull'ultima sommatoria. Dato che $ik \ge k + 1$ per ogni $i \ge 2$, ogni addendo è divisibile per 7^{k+1} e quindi

$$(1 + a\omega)^s \equiv \left(1 + \frac{s}{7} a\omega\right)^7 \pmod{7^{k+1}}.$$

Usando per l'ennesima volta il binomio di Newton ricaviamo

$$\left(1 + \frac{s}{7} a\omega\right)^7 = 1 + 7\,\frac{s}{7} a\omega + \sum_{j=2}^{7} \binom{7}{j} \left(\frac{s}{7} a\omega\right)^j = 1 + sa\omega + \sum_{j=2}^{6} \binom{7}{j} \left(7^{k-1} l\, a\omega\right)^j + 7^{7k-4} l^7 a^7 \omega$$

Dato che $k \ge 1$ si ha $7k - 4 \ge k + 1$. Inoltre, per ogni $2 \le j \le 6$, l'addendo della sommatoria corrispondente all'indice j è divisibile per $7^{j(k-1)+\lfloor j/2 \rfloor + 1}$ (usiamo il fatto che i coefficienti binomiali $\binom{7}{j}$ sono multipli di 7) e $j(k-1) + \lfloor j/2 \rfloor + 1 \ge k + 1$. Di conseguenza

$$\left(1 + \frac{s}{7} a\omega\right)^7 \equiv 1 + sa\omega \pmod{7^{k+1}}.$$

ed il lemma è dimostrato.

Siano ora $(a_1, n_1), (a_2, n_2)$ sue soluzioni con $n_1 \ne n_2$ ed $m_1 = n_1 - 2 \equiv n_2 - 2 = m_2 \pmod{42}$. Possiamo assumere $m_2 > m_1$ e porre $s = m_2 - m_1 = 7^k l$ con $7 \nmid l$. Dato che 3 divide s possiamo scrivere

$$2^s = (2^3)^{s/3} = (1 + 7)^{s/3} = (1 + (-\omega)\omega))^{s/3}.$$

Usando il Lemma 2.4.2 otteniamo

$$2^s \equiv 1 + \frac{s}{3}7 \pmod{7^{k+1}}$$

e quindi

$$2^s \equiv 1 \pmod{7)^{k+1}}$$

perché 7^{k+1} divide $7s/3$. Allora, per ogni $a \in \mathcal{O}_{\mathbb{F}}$, abbiamo $2^s a \equiv a \pmod{7^{k+1}}$. Dato che $\alpha^s = (1+\omega)^s/2^s$ usiamo l'osservazione precedente per vedere che

$$(1+\omega)^s = 2^s\alpha^s \equiv \alpha^s \pmod{7^{k+1}}.$$

Calcoliamo $\alpha^{m_1} - \alpha^{m_2} = \alpha^{m_2}(1-\alpha^s)$. Per quanto appena visto e usando il Lemma 2.4.2 ricaviamo

$$\alpha^{m_1} - \alpha^{m_2} \equiv \alpha^{m_1}(1-(1+\omega)^s) \equiv -\alpha^{m_1} s\omega \pmod{7^{k+1}}.$$

Coniugando abbiamo anche

$$\overline{\alpha}^{m_1} - \overline{\alpha}^{m_2} \equiv \overline{\alpha}^{m_1} s\omega \pmod{7^{k+1}}.$$

Prendendo la differenza membro a membro

$$(\alpha^{m_1} - \overline{\alpha}^{m_1}) - (\alpha^{m_2} - \overline{\alpha}^{m_2}) \equiv s - \omega(\alpha^{m_1} + \overline{\alpha}^{m_1}) \pmod{7^{k+1}}$$

e, ricordando che $\alpha^{m_i} = -\dfrac{a+\omega}{2}$, si arriva alla congruenza

$$0 \equiv sa\omega \pmod{7^{k+1}}.$$

Per convincersi che tale congruenza è falsa basta ricordare che ω è un primo e osservare che la massima potenza di ω che divide $sa\omega$ è ω^{2k+1} e quindi $sa\omega$ non può essere divisibile per $7^{k+1} = \pm\omega^{2(k+1)}$. Questa contraddizione mostra che le uniche soluzioni della nostra equazione sono quelle elencate all'inizio.

2.5 Teorema di Hermite

Diamo un'altra interessante applicazione del Teorema di Minkowski, dimostrando un importante risultato dovuto ad Hermite.

Teorema 2.5.1 *Sia $\Delta \in \mathbb{Z}$. Allora esistono solo un numero finito di campi di numeri $\mathbb{F}$ tali che $\Delta_{\mathbb{F}} = \Delta$.*

Dimostrazione. Sia $\mathbb{F}$ un campo di numeri (che supponiamo diverso da $\mathbb{Q}$) con $\Delta_{\mathbb{F}} = \Delta$, indichiamo con n il suo grado e scriviamo $n = s + 2t$ dove s, t hanno l'usuale significato. Scelte le immersioni $\sigma_1, \sigma_2, \ldots, \sigma_s, \sigma_{s+1}, \ldots \sigma_{s+t}$ abbiamo l'immersione $\sigma : \mathbb{F} \longrightarrow V_{\mathbb{F}}$. Il primo fatto che notiamo è che n è limitato in termini di Δ. Per vedere questo ricordiamo che, se ω è un

elemento del gruppo delle classi di $\mathbb{F}$, allora c'è un ideale $I \in \omega$ con $N(I) \leq M_{st}\sqrt{|\Delta|}$. Questo implica $M_{st}\ \sqrt{|\Delta|} \geq 1$ e quindi

$$\left[\left(\frac{\pi}{4}\right)^t \frac{n^n}{n!}\right]^2 \leq |\Delta|.$$

Non è difficile vedere che il primo membro di questa disuguaglianza tende a $+\infty$ al tendere di n a $+\infty$, pertanto n è limitato in termini di Δ. Abbiamo cioè che, se $\mathbb{F}$ ha discriminante Δ, il suo grado è limitato da $n = n(\Delta)$.

Definiamo il sottoinsieme $B \subseteq V_{\mathbb{F}}$ come

$$B = \begin{cases} \{\, x \mid \|x_1\| \leq 1 + \sqrt{|\Delta|} \ \text{ e } \ \|x_i\| < 1 \ \forall\ i \geq 2 \,\} & \text{se } s \neq 0 \\ \{\, x \mid |\mathrm{Re}(x_1)| < 1,\ |\mathrm{Im}(x_1)| \leq 1 + \sqrt{|\Delta|} \ \text{ e } \ \|x_i\| < 1 \quad \forall\ i \geq 2 \,\} & \text{se } s = 0 \end{cases}$$

L'insieme B è un prodotto diretto di intervalli e dischi, quindi è simmetrico, limitato e convesso, , ed il suo volume vale

$$\mu(B) = \begin{cases} (1 + \sqrt{|\Delta|})2^s\pi^t & \text{se } s \neq 0 \\ 4(1 + \sqrt{|\Delta|})\pi^{t-1} & \text{se } s = 0 \end{cases}$$

Il reticolo $L = \sigma(\mathcal{O}_{\mathbb{F}})$ ha covolume $\sqrt{|\Delta|}/2^t$ e quindi

$$2^n \mathrm{cov}(L) = 2^{s+t}\sqrt{|\Delta|} < \mu(B)$$

IL teorema di Minkowski ci assicura l'esistenza di un elemento non nullo $\sigma(a) \in L \cap B$. L'elemento a è un intero algebrico non nullo e allora la sua norma, in valore assoluto, deve valere almeno 1. Scrivendo esplicitamente

$$|N(a)| = \begin{cases} |\sigma_1(a)| \cdot \prod_{i=2}^{s} |\sigma_i(a)| \cdot \prod_{i=s+1}^{s+t} \|\sigma_i(a)\|^2 = |\sigma_1(a)| \cdot u & \text{se } s \neq 0 \\ \|\sigma_1(a)\|^2 \cdot \prod_{i=2}^{t} \|\sigma_i(a)\|^2 = \|\sigma_1(a)\|^2 \cdot v & \text{se } s = 0 \end{cases}$$

e ricordando la definizione di B, otteniamo che $u < 1$ e $v \leq 1$ (anzi $v < 1$ se $t \geq 2$).

Caso 1. $s \neq 0$. In questa situazione $|\sigma_1(a)| > 1$ visto che $|\sigma_1(a)| \cdot u \geq 1$, e quindi $\sigma_1(a) \neq \tau(a)$ per ogni immersione $\tau \neq \sigma_1$.

Caso 2. $s = 0$.

In questa situazione $\|\sigma_1(a)\| \geq 1$ e quindi $\sigma_1(a)$ non è un numero reale , visto che $|\mathrm{Re}(x_1)| < 1$. Allora $\sigma_1(a) \neq \overline{\sigma_1}(a)$. Inoltre $\sigma_1(a) \neq \sigma_i(a)$, se $i \geq 2$, perché $\|\sigma_i(a)\| < 1$. Anche in questo caso abbiamo allora $\sigma_1(a) \neq \tau(a)$ per ogni immersione $\tau \neq \sigma_1$. Elenchiamo le immersioni come $\tau_1, \ldots, \tau_n$.

Il polinomio

$$f = \prod_{i=1}^{n} (x - \tau_i(a))$$

ammette $\sigma_1(a)$ come radice singola. Ciascun elemento $\tau(a)$ è uno zero di g, il polinomio minimo di a su $\mathbb{Q}$ e, se k è il grado di $\mathbb{Q}[a]$ su $\mathbb{Q}$, si deve avere $f = g^{n/k}$. Ma allora ogni radice di f ha

molteplicità n/k e quindi $k = n$. Di conseguenza $f = g$ ed $\mathbb{F} = \mathbb{Q}[a]$. Dato che a è un intero algebrico, $f \in \mathbb{Z}[x]$.

Scriviamo $f = x^n + \sum_{i=0}^{n-1} a_i x^i$ ed osserviamo che esiste una costante C_Δ, dipendente solo da Δ, tale che $\|\tau_i(a)\| \leq C_\Delta$ per ogni i. Fissiamo $k \in [1, n-1]$ e poniamo $\Gamma(k) = \{\, I \mid I \subseteq [1, 2, \ldots, n] \text{ e } |I| = k \,\}$. Si verifica immediatamente che, per ogni $i \in [0, n-1]$, si ha

$$a_i = (-1)^{n-i} \sum_{I \in \Gamma(n-i)} \prod_{l \in I} \tau_l(a)$$

e quindi

$$|a_i| \leq \sum_{I \in \Gamma(n-i)} \prod_{l \in I} \|\tau_l(a)\| \leq \sum_{I \in \Gamma(n-i)} {C_\Delta}^{n-i} = \binom{n}{n-i} {C_\Delta}^{n-i} \leq \binom{n}{\lfloor n/2 \rfloor} {C_\Delta}^{n} = M_\Delta.$$

Sia

$$\Omega = \left\{ h |\ h \in \mathbb{Z}[x],\, h = \sum_{i=0}^{n} b_i x^i \quad \text{e } |b_i| \leq M_\Delta \ \forall\, i \right\}.$$

Quello che abbiamo visto è che, se un campo di numeri $\mathbb{F}$ ha discriminante Δ, allora $\mathbb{F} = \mathbb{Q}[a]$ con a zero di un polinomio appartenente all'insieme Ω. Visto che Ω è finito, il numero di campi $\mathbb{F}$ di discriminante Δ è finito. □

Capitolo 3

Anelli euclidei

In questo capitolo cercheremo di determinare per quali campi quadratici immaginari $\mathbb{F}$, l'anello degli interi $\mathcal{O}_\mathbb{F}$ è euclideo rispetto alla usuale norma $N(a+ib) = a^2 + b^2$. Osserviamo che, in questa situazione, la norma di $\mathbb{C}$ coincide con la norma *algebrica* del campo $\mathbb{F}$. In questo caso parleremo di anelli N*-euclidei*. Ci serve, come prima cosa, trovare una caratterizzazione che sia più adatta alla nostra situazione.

Se $\mathcal{O}_\mathbb{F}$ è N-euclideo si ha che, per ogni coppia di elementi $\alpha, \beta \in \mathcal{O}_\mathbb{F}$ con $\beta \neq 0$, devono esistere $q, r \in \mathcal{O}_\mathbb{F}$ tali che

$$\alpha = \beta q + r \quad \text{ e } N(r) < N(\beta).$$

Dividento per β, spostando qualche termine e ricordando le proprietà della norma otteniamo

$$\frac{\alpha}{\beta} - q = \frac{r}{\beta} \quad \text{ e } N\Big(\frac{r}{\beta}\Big) < 1.$$

Dato che ogni elemento di $\mathbb{F}$ si ottiene come quoziente di due interi algebrici in $\mathcal{O}_\mathbb{F}$, una forma equivalente della proprietà di essere N-euclideo è la seguente:

$(*)$ Se $\mathbb{F}$ è una estensione quadratica immaginaria, l'anello $\mathcal{O}_\mathbb{F}$ è N-euclideo se e solo se, per ogni $\alpha \in \mathbb{F}$, esiste $\beta \in \mathcal{O}_\mathbb{F}$ tale che $N(\alpha - \beta) < 1$.

In termini geometrici questo vuol dire che ogni elemento di $\mathbb{F}$ appartiene ad almeno un insieme della forma $B(x,1) = \{\, y \in \mathbb{C} \mid \|x - y\| < 1 \,\}$ (il disco aperto di centro x e raggio 1) per qualche $x \in \mathcal{O}_\mathbb{F}$. Questa condizione si esplora facilmente, ottenendo il seguente teorema.

Teorema 3.0.1 *Sia $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ con d un intero negativo e libero da quadrati. Allora l'anello degli interi di $\mathbb{F}$ è N-euclideo se e solo se $d \in \{\, -1, -2, -3, -7, -11 \,\}$.*

Dimostrazione. Iniziamo col vedere che, se d appartiene all'insieme $\{\, -1, -2, -3, -7, -11 \,\}$, l'anello degli interi di $\mathbb{Q}[\sqrt{d}]$ è N-euclideo. Usiamo la caratterizzazione data sopra. Se $d \equiv 2, 3 \pmod 4$ (ovvero $d = -1$ o -2) l'anello degli interi è $\mathbb{Z}[\sqrt{d}]$. Prendiamo $\alpha = a + b\sqrt{d} \in \mathbb{F}$ e scegliamo interi n, m in modo che $|a - n| \leq 1/2$ e $|b - m| \leq 1/2$e si pone $\beta = n + m\sqrt{d}$ Allora

$\alpha - \beta = (a-n) + (b-m)\sqrt{d}$ e quindi

$$N(\alpha-\beta) = (a-n)^2 + |d|(b-m)^2 \leq \frac{1}{4} + \frac{|d|}{4} = \frac{1+|d|}{4} \leq \frac{3}{4} < 1.$$

Nei casi rimanenti, scelto un qualsiasi $\alpha = a + b\sqrt{d} \in \mathbb{F}$, scegliamo intanto un intero m tale che $|2b - m| \leq 1/2$. Fatta questa scelta si prende un intero n in modo che $|(a - m/2) - n| \leq 1/2$. Posto $\beta = n + m\frac{1+\sqrt{d}}{2} \in \mathcal{O}_{\mathbb{F}}$ si ha

$$N(\alpha-\beta) = \Big(a - \frac{m}{2} - n\Big)^2 + |d|\Big(b - \frac{m}{2}\Big)^2 \leq \frac{1}{4} + |d|\frac{1}{16} = \frac{4+|d|}{2} \leq \frac{15}{16} < 1.$$

Per concludere la dimostrazione dobbiamo ora vedere che, se d non appartiene all'insieme $\{-1, -2, -3, -7, -11\}$, l'anello degli interi non è N-euclideo.

Basterà mostrare che esiste qualche elemento $\alpha \in \mathbb{F}$ tale che $N(\alpha - \beta) \geq 1$ per ogni $\beta \in \mathcal{O}_{\mathbb{F}}$. Trattiamo separatamente due casi. Se $d \equiv 2, 3 \pmod 4$ prendiamo $\alpha = \sqrt{d}/2$. Se $\beta = n + m\sqrt{d}$ è un qualsiasi elemento di $\mathcal{O}_{\mathbb{F}}$ abbiamo

$$N(\alpha-\beta) = n^2 + |d|\Big(m - \frac{1}{2}\Big)^2 \geq \frac{|d|}{4} \geq$$

Dato che $|d| \geq 6$ abbiamo che $N(\alpha - \beta) > 1$ per ogni scelta di β e quindi $\mathcal{O}_{\mathbb{F}}$ non può essere euclideo.

Se $d \equiv 1 \pmod 4$ scegliamo $\alpha = \frac{1}{4} + \frac{1}{4}\sqrt{d}$. Ancora, se Se $\beta = n + m\frac{1+\sqrt{d}}{2} \in \mathcal{O}_{\mathbb{F}}$, si ha

$$N(\alpha-\beta) = \Big(\frac{1}{4} - n - \frac{m}{2})\Big)^2 + |d|\Big(\frac{1}{4} - \frac{m}{2}\Big)^2 \geq \frac{1}{16} + |d|\frac{1}{16} = \frac{1+|d|}{16}.$$

Dato che $|d| \geq 15$ s ottiene, anche in questo caso, $N(\alpha - \beta) \geq 1$, ed il teorema è dimostrato. □

Questo teorema lascia aperta la possibilità che, rispetto ad altre funzioni norma, esistano altri anelli quadratici immaginari che sono euclidei. Questo in realtà non accade. Si possono usare i risultati contenuti in [8] per dimostrare il seguente fatto.

Teorema 3.0.2 *Sia $\mathbb{F}$ un campo di numeri quadratico immaginario. Allora $\mathcal{O}_{\mathbb{F}}$ è euclideo se e solo se è N-euclideo.*

Il caso delle estensioni quadratiche reali la situazione è invece più articolato e, in buona parte, ancora non chiaro. Scriviamo la nostra estensione quadratica come $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ con d intero positivo e libero da quadrati e, per ogni α in $\mathbb{F}$ poniamo $\delta(\alpha) = |N(\alpha|$. Se $\mathcal{O}_{\mathbb{F}}$ è euclideo rispetto alla funzione norma δ, ancora diremo che è N-euclideo. Negli articoli [4] e [2] si dimostra che l'anello degli interi dell'estensione quadratica $\mathbb{Q}[\sqrt{d}]$ è N-euclideo se e solo se $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$. Ma, al contrario di quanto accade per le estensioni quadratiche immaginarie, ci sono anelli di interi che sono euclidei ma non N-euclidei. Ad esempio in [3] si dimostra che l'anello degli interi di $\mathbb{Q}[\sqrt{69}]$ è euclideo (ma non N-eucliede per quanto detto prima). Recentemente è stato dimostrato che esistono al più due campi quadratici reali che sono PID ma non euclidei (vedi [7]). Al momento non si conoscono tali esempi che,

comunque, sembra improbabile esistano. Infatti, assumendo vera la Congettura di Riemann Generalizzata, si può mostrare che ogni campo reale quadratico che sia un PID è anche euclideo (rispetto a qualche norma). Infine ricordiamo che è stato congetturato da Gauss che, per infiniti interi d positivi e liberi da quadrati, l'anello degli interi di $\mathbb{Q}[\sqrt{d}]$ è un PID. Se tale congettura fosse vera avremmo allora una famiglia infinita di anelli quadratici euclidei ma non N-euclidei.

Capitolo 4

Unità

Scopo di questo capito è dimostrare il *Teorema delle unità di Dirichlet* che descrive la struttura del gruppo degli elementi invertibili di $\mathcal{O}_{\mathbb{F}}$. Un elemento invertibile verrà spesso detto una *unità* di $\mathcal{O}_{\mathbb{F}}$. Un prima osservazione è che un elemento α di $\mathcal{O}_{\mathbb{F}}$ è invertibile se e solo se $|N(\alpha)| = 1$. Infatti, se $\alpha\beta = 1$ per qualche β in $\mathcal{O}_{\mathbb{F}}$, abbiamo $1 = N(\alpha\beta) = N(alpha)N(\beta)$ e, dato che $N(\alpha), N(\beta) \in \mathbb{Z}$ segue che $N(\alpha) = \pm 1$. Per vedere il viceversa iniziamo elencando le immersioni di $\mathbb{F}$ come $\mathrm{id}_{\mathbb{F}} = \sigma_1, \sigma_2, \ldots, \sigma_n$ e ponendo $\beta = \prod_{i \neq 1} \sigma_i(\alpha)$. Il numero complesso β è un intero algebrico e, dato che $\alpha\beta = N(\alpha) = \pm 1$, $\beta = \pm\alpha^{-1} \in \mathbb{F}$. Ne deduciamo che β appartiene a $\mathcal{O}_{\mathbb{F}}$ e questo prova che α è invertibile.

4.1 Teorema delle unità di Dirichlet

Iniziamo dimostrando due risultati tecnici, il primo dei quali riguarda matrici reali.

Lemma 4.1.1 *Sia A una matrice reale $n \times n$ e indichiamo con a_{ij} l'elemento di posto (i, j). Se*

1. $a_{ij} < 0 \quad \forall\, i \neq j$ *e*
2. $\sum_{i=1}^{n} a_{ij} > 0$

allora A è invertibile.

Dimostrazione. Sia $A_i = (a_{i1} a_{i2} \ldots a_{in})$ la riga i-esima di A. Se per assurdo, la matrice A non fosse invertibile, potremmo trovare una combinazione lineare $\sum_{i=1}^{n} \lambda_i A_i = 0$, con almeno uno dei λ_i diverso da 0. Sia $|\lambda_k| = \max\{|\lambda_k| \mid i = 1, \ldots, n\}$. Senza perdere di generalità possiamo assumere $\lambda_k > 0$, per cui $\lambda_k \geq \lambda_i$ per ogni i. Nelle nostre ipotesi abbiamo quindi $\lambda_k a_{ik} \leq \lambda_i a_{ik}$ per ogni i e, sommando su i,

$$\sum_{i=1}^{n} \lambda_i a_{ik} \geq \sum_{i=1}^{n} \lambda_k a_{ik} = \lambda_k \sum_{i=1}^{n} a_{ik} > 0.$$

D'altra parte $\sum_{i=1}^{n} \lambda_i a_{ik}$ è la k-esima coordinata del vettore $\sum_{i=1}^{n} \lambda_i A_i$ e quindi vale 0. Questa contraddizione conclude la dimostrazione. □

Il secondo lemma prova l'esistenza di successioni con proprietà particolari. Le notazioni sono quelle usuali.

Lemma 4.1.2 *Sia $\mathbb{F}$ un campo di numeri di grado $n = s + 2t$, $\sigma_1, \dots \sigma_s$ le immersioni reali e $\sigma_{s+1}, \dots, \sigma_{s+t}$ quelle complesse a meno di coniugio. Per ogni indice $i \in [1, s+t]$ esiste una successione $\{ \alpha_m(i) \mid m \in \mathbb{N} \}$ tale che*

1. *$|N(\alpha_m(i))| \leq 1 + \sqrt{|\Delta_{\mathbb{F}}|}$ per ogni $m \in \mathbb{N}$ e*
2. *per ogni $j \neq i$, $\|\sigma_j(\alpha_m(i))\| > \|\sigma_j(\alpha_{m+1}(i))\|$ per ogni $m \in \mathbb{N}$.*

Dimostrazione. Preso $\mathbf{b} = (b_1, b_2, \dots, b_{s+t})$ con i b_j numeri reali strettamente positivi, definiamo

$$B(\mathbf{b}) = \{ x \in V_{\mathbb{F}} \mid \|x_i\| \leq b_i \ \forall\ i \}.$$

Ciascuno di questi insiemi è un prodotto cartesiano di intervalli e dischi e si vede facilmente che

$$\mu(B(\mathbf{b})) = 2^s \prod_{j=1}^{s} b_j \cdot \pi^t \prod_{j=s+1}^{s+t} {b_j}^2.$$

Inoltre tutti questi insiemi sono limitati, simmetrici e convessi.

Fissiamo adesso l'indice i e, per semplificare le notazioni, indichiamo gli elementi della successione soltanto come α_m, sottointendendo la dipendenza da i.

Prendiamo $\alpha_0 = 1$. Supponendo di aver già trovato $\alpha_0, \alpha_1, \dots, \alpha_m$ e mostriamo come trovare α_{m+1}. Poniamo, per ogni $j \neq i$, $b_j = \frac{1}{2}\|\sigma_j(\alpha_m)\|$ e definiamo b_i tramite la relazione

$$\mu(B(b_1, \dots, b_{s+t})) = s^s \pi^t (1 + \sqrt{|\Delta_{\mathbb{F}}|}).$$

Notiamo che tutti i b_j sono numeri strettamente positivi e $\prod_{i=1}^{s} b_i \cdot (\prod_{i=1}^{t} b_{s+i})^2 = 1 + \sqrt{|\Delta_{\mathbb{F}}|}$. Se $\sigma : \mathbb{F} \longrightarrow V_{\mathbb{F}}$ è l'usuale immersione, il reticolo $L = \sigma(\mathcal{O}_{\mathbb{F}})$ ha covolume $\sqrt{|\Delta_{\mathbb{F}}|}/2^t$. Pertanto vale la disuguaglianza $2^n \mathrm{cov}(L) < \mu(B(b_1, \dots, b_{s+t}))$ ed è possibile applicare il teorema di Minkowski. C'è un elemento α tale che $\sigma(\alpha) \in B(b_1, \dots, b_{s+t}) \cap (L \setminus \{ 0 \})$. Abbiamo allora che, per ogni indice $j \neq i$, $\|\sigma_j(\alpha)\| \leq b_j/2 < \|\sigma_j(\alpha_m\|)$. Inoltre

$$|N(\alpha)| = \prod_{i=1}^{s} \|\sigma_i(\alpha)\| \cdot \left(\prod_{i=1}^{t} \|\sigma_{s+i}(\alpha)\| \right)^2 \leq \prod_{i=1}^{s} b_i \cdot \left(\prod_{i=1}^{t} b_{s+i} \right)^2 = 1 + \sqrt{|\Delta_{\mathbb{F}}|}.$$

Basta quindi porre $\alpha_{m+1} = \alpha$. □

Prima di enunciare il risultato principale di questo capitolo, ricordiamo che un gruppo abeliano G finitamente generato è isomorfo ad un prodotto diretto del $F \times \mathbb{Z}^m$ con F sottogruppo finito ed $m \in \mathbb{N}$. Il sottogruppo F è l'insieme degli elementi di periodo finito, detto il *sottogruppo di torsione* di G, e verrà indicato con $T(G)$. Si controlla facilmente che il gruppo G/T non ha elementi di periodo finito.

Teorema 4.1.3 (Teorema delle unità di Dirichlet) *Siano $\mathbb{F}$ un campo di numeri di grado $n = s + 2t$. Se U è il gruppo delle unità di $\mathcal{O}_{\mathbb{F}}$ allora U è finitamente generato e $U/T(U)$ è un gruppo libero di rango $s + t - 1$.*

DIMOSTRAZIONE. Siano $\sigma_1, \dots, \sigma_s$ le immersioni reali di $\mathbb{F}$ e $\sigma_{s+1}, \dots, \sigma_{s+t}$ quelle complesse a meno di coniugio. Come sempre abbiamo la funzione $\sigma : \mathbb{F} \longrightarrow V_{\mathbb{F}}$.

Definiamo, per ciascuna immersione σ_i e per ogni $a \in \mathbb{F}$,

$$\nu_i(a) = \begin{cases} |\sigma_i(a)| & 1 \leq i \leq s \\ \|\sigma_i(a)\|^2 & s+1 \leq i \leq s+t \end{cases}.$$

Ci servirà in seguito il fatto che $|N(a)| = \prod_{i=1}^{s+t} \nu(\sigma_i(a))$ per ogni $a \in \mathbb{F}$. La funzione $\psi : U \longrightarrow \mathbb{R}^{s+t}$ definita da

$$\psi(a) = (\log(\nu_1(a)), \dots, \log(\nu_{s+t}(a)))$$

è un morfismo di gruppi e, dato che $U/\ker(\psi) \simeq \mathrm{Im}(\psi) \leq \mathbb{R}^{s+t}$, il sottogruppo di torsione di U deve essere contenuto in $\ker(\psi)$. Abbiamo $\ker(\psi) = \{\, a \mid \|\sigma_i(a)\| = 1 \quad \forall\, i \,\}$ e quindi

$$\sigma(\ker(\psi)) \subseteq B = \{\, x \mid \|x_i\| \leq 1 \quad \forall\ i \,\}.$$

Dato che l'insieme B è limitato, il sottoinsieme $\sigma(\mathcal{O}_{\mathbb{F}}) \cap B$ è finito, e quindi anche $\sigma(\ker(\psi))$ è finito. Ne segue che anche $\ker(\psi)$ è finito visto che σ è iniettiva. Se m è l'ordine di $\ker(\psi)$ e $a \in \ker(\psi)$, si ha $a^m = 1$, e questo prova che $a \in T(U)$. In definitiva abbiamo visto che $\ker(\psi) = T(U)$. Ogni elemento di $\ker(\psi)$ è una radice m-esima di 1, quindi $\ker(\psi) \leq \langle\, e^{2\pi i/m} \,\rangle$ e, in particolare, $\ker(\psi)$ è un gruppo ciclico finito. Per concludere la dimostrazione basta mostrare che $H = \mathrm{Im}(\psi) \simeq \mathbb{Z}^{s+t-1}$.

Per ogni $a \in U$ sappiamo che $|N(a)| = 1$, quindi

$$\sum_{i=1}^{s+t} \log(\nu_i(a)) = \log\big(\prod_{i=1}^{s+t} \nu_i(a)\big) = \log(|N(a)|) = 0.$$

L'immagine di ψ è allora contenuta in $W = \{\, x \in \mathbb{R}^{s+t} \mid \sum_{i=1}^{s+t} x_i = 0 \,\}$ che è un sottospazio di $\mathbb{R}^{s+t}$ di dimensione $s + t - 1$. Proveremo allora che H è libero di rango $s + t - 1$, mostrando che H è un reticolo in W. Per far questo mostreremo che H contiene una base di W e che, per ogni B, sottoinsieme limitato di W, l'insieme $H \cap B$ è finito. Fissiamo un indice i e costruiamo una successione $\{\alpha_m \mid m \in \mathbb{N}\}$ con le proprietà descritte nel Lemma 4.1.2. L'deale (α_m) ha norma $|N(\alpha_m|)$ (vedi Lemma 2.2.4) quindi $N((\alpha_m)) \leq 1 + \sqrt{|\Delta_{\mathbb{F}}|}$ per ogni $m \in \mathbb{N}$. Il Lemma 2.2.5 ci dice che il numero di ideali di norma limitata da $1 + \sqrt{|\Delta_{\mathbb{F}}|}$ è finito e di conseguenza troviamo interi $l < m$ tali che $(\alpha_l) = (\alpha_m)$. Dato che $\mathcal{O}_{\mathbb{F}}$ è un dominio, questo vuol dire che α_l ed α_m sono associati. In altri termini $\varepsilon_i = \alpha_m/\alpha_l$ è un elemento di U. È importante mettere in evidenza che, per ogni $j \neq i$

$$\|\sigma_j(\varepsilon_i)\| = \|\sigma_j(\alpha_m/\alpha_l)\| = \left\|\frac{\sigma_j(\alpha_m)}{\sigma_j(\alpha_l)}\right\| = \frac{\|\sigma_j(\alpha_m)\|}{\|\sigma_j(\alpha_l)\|} < 1$$

e quindi $\nu_j(\varepsilon_i) < 1$. Mostriamo ora che l'insieme $\{\, \psi(\varepsilon_1), \dots, \psi(\varepsilon_{s+t}) \,\}$ è un insieme di generatori di W. Di sicuro questi vettori generano un sottospazio di dimensione al minore o uguale ad $s+t-1$. Pensiamo ora questi vettori come colonne e scriviamo la matrice

$$M = \left(\begin{array}{c|c|c} \psi(\varepsilon_1) & \cdots & \psi(\varepsilon_{s+t}) \end{array} \right)$$

come

$$M = \left(\begin{array}{ccc|c} & & & \log(\nu_1(\varepsilon_{s+t})) \\ & A & & \vdots \\ & & & \log(\nu_{s+t-1}(\varepsilon_{s+t})) \\ \hline \log(\nu_{s+t}(\varepsilon_1)) & \dots & \log(\nu_{s+t}(\varepsilon_{s+t-1})) & \log(\nu_{s+t}(\varepsilon_{s+t})) \end{array} \right)$$

Per quanto osservato prima tutte le entrate di A che sono fuori dalla diagonale principale sono numeri strettamente negativi, mentre la somma di ciascuna colonna di A è strettamente positiva dato che la somma di ciascuna colonna di M è nulla e gli elementi $\log(\nu_{s+t}(\varepsilon_i))$ sono negativi per ogni $i \neq s+t$. Il Lemma 4.1.1 può essere usato e ne segue che il rango di A (e quindi anche quello di M) è $s+t-1$. Questo dimostra che $\mathrm{Im}(\psi)$ contiene un sottoinsieme indipendente di ordine $s+t-1$ e quindi una base di W. Fissato un numero reale $N > 0$, sia $C(N) = \{\, x \in \mathbb{R}^{s+t} \mid |x_i| \leq N \,\}$. Se $\psi(a) \in C(N)$ vuol dire che $|\log(\nu_i(a))| \leq N$ per ogni i e questo implica $|\sigma_i(a)| \leq e^N$ per ogni $i = 1, \dots, s$ e $\|\sigma_i(a)\| \leq e^{N/2}$ quando $i = s+1, \dots s+t$. Dato che $\sigma(\mathcal{O}_\mathbb{F})$ è un reticolo in $V_\mathbb{F}$, la sua intersezione con l'insieme limitato $B(N) = \{\, v \mid \|v_i\| \leq e^N \,\forall i = 1, \dots s,\ \|v_i\| \leq e^{N/2} \,\forall i = s+1, \dots s+t \,\}$ è finito. Da quanto appena visto abbiamo che $a \in \mathcal{O}_\mathbb{F}$ è tale che $\psi(a) \in C(N)$ se e solo se $\sigma(a) \in B(N)$ e quindi $\mathrm{Im}(\psi) \cap C(N)$ è un insieme finito. Se B è un sottoinsieme limitato di W, allora esiste $N > 0$ tale che $B \leq W \cap C(N)$ e quindi $\mathrm{Im}(\psi) \cap B \subseteq \mathrm{Im}(\psi) \cap C(N)$ è finito. Abbiamo quindi che H è un reticolo in W e il teorema è dimostrato. □

Il risultato appena provato ha molte conseguenze importanti. Ad esempio ci dice che, quando $s+t-1 \neq 0$, gli elementi invertibili sono sempre infiniti. Ma $s+t = 1$ se e solo se $n = s+2t = 2$ e $s = 0, t = 1$, ovvero il campo di numeri è una estensione quadratica immaginaria.

Un'altra applicazione è la seguente

Corollario 4.1.4 *Per ogni intero positivo d libero da quadrati, l'equazione di Pell $x^2 - dy^2 = 1$ ha infinite soluzioni.*

Dimostrazione. Per il Teorema 4.1.3, il gruppo delle unità dell'anello degli interi di $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ è isomorfo al prodotto diretto $U = F \times \mathbb{Z}$ dove F è il sottogruppo delle radici dell'unità contenute in $\mathcal{O}_\mathbb{F}$. Dato $\mathbb{F}$ è un sottocampo dei reali, $F = \{\pm 1\}$ e quindi ogni elemento di U è della forma $\pm\varepsilon^n$ con $n \in \mathbb{Z}$ e ε un opportuno elemento. Se $d \equiv 2, 3, \pmod 4$ allora l'anello degli interi di $\mathbb{F}$ è $\mathbb{Z}[\sqrt{d}]$, $\varepsilon = a + b\sqrt{d}$ e $a^2 - db^2 = \pm 1$. In ogni caso $N(\varepsilon^2) = 1$ e quindi, posto $\varepsilon^{2n} = u_n + v_n\sqrt{d}$, ciascuna coppia (u_n, v_n) è soluzione dell'equazione $x^2 - dy^2 = 1$. Dato che ε ha periodo infinito, tutte queste soluzioni sono distinte. Quando invece $d \equiv 1 \pmod 4$ possiamo vedere che esistono infinite coppie di interi (a, b) tali che $(a + b/2)^- db^2/4 = 1$. Da questo fatto otteniamo l'esistenza

di infinite soluzioni (u, v) per l'equazione $x^2 - db^2 = 4$. Per il lemma dei cassetti ci saranno due soluzioni distinte $(u, v), (\overline{u}, \overline{v})$ tali che $u \equiv \overline{u} \pmod 4$ e $v \equiv \overline{v} \pmod 4$. Usando un lemma visto nella trattazione *elementare* dell'equazione di Pell, ne deduciamo l'esistenza di una soluzione non banale (r, s) (ad esempio $r = (u\overline{u} - dv\overline{v})4$ e $s = (u\overline{v} - v\overline{u})/4$). Le potenze $(r + s\sqrt{d})^n = r_n + s_n\sqrt{d}$ forniscono le soluzioni (r_n, s_n), tutte distinte. □

4.2 Una applicazione alla teoria dei gruppi

Il materiale di questa sezione si basa su parte del capito 2 di [9]. Iniziamo questa sezione richiamando, senza dimostrazioni, la costruzione degli anelli gruppali e mettendo in evidenza alcune loro proprietà che dovremo usare in seguito.

Siano G un gruppo ed R un anello commutativo. Indichiamo con RG il sottoinsieme di R^G formato dalle funzioni f tali che $\text{supp}(f) = \{ g \mid f(g) \neq 0 \}$ è finito. Questo insieme è chiaramente un sottogruppo di R^G. Per ogni $r \in R$ definiamo la funzione f_r ponendo

$$f_r(g) = \begin{cases} 1 & \text{se } g = 1 \\ 0 & \text{se } g \neq 1. \end{cases}$$

Infine, prese $f, g \in RG$, definiamo la funzione $fg \in R^G$ ponendo

$$(fg)(a) = \sum_{xy=a} f(x)g(y).$$

Un facile controllo mostra che $fg \in RG$. Si dimostra che RG con l'operazione di somma e con il prodotto appena definito è un anello. Inoltre la funzione $\iota : R \longmapsto RG$, $\iota(r) = f_r$ è un morfismo iniettivo di anelli. Pertanto identificheremo l'immagine di ι con R e indicheremo ciascuna funzione f_r con r. Se invece $x \in G$, possiamo considerare la funzione ϵ_x definita da

$$\epsilon_x(g) = \begin{cases} 1 & \text{se } g = x \\ 0 & \text{se } g \neq x. \end{cases}$$

$\epsilon_x(y) = 1$ se $x = y$ e 0 altrimenti. Se $x = 1$ $\epsilon_1 = f_1 = 1$. Per ogni $x, y \in G$ si ha $\epsilon_x\epsilon_y = \epsilon_{xy}$ per cui la funzione

$$\begin{aligned} \epsilon : G &\longrightarrow RG \\ x &\longmapsto \epsilon_x \end{aligned}$$

ha immagine nel gruppo degli invertibili di RG. Essendo ϵ iniettiva, possiamo identificare G con $\epsilon(G)$ ed ogni ϵ_x verrà indicato semplicemente con x. Le identificazioni fatte hanno lo scopo di semplificare i calcoli in RG. Ci si accorge che

1. $\{f_r \mid r \in R\}$ è un sottoanello di RG isomorfo ad R. Questo giustifica la scelta di indicare f_r con r;

2. $RG = \{ \sum_{x \in G} r_x x \mid r_x \neq 0$ solo per un numero finito di $x \}$ e

3. $rx = xr$ per ogni $r \in R$ ed $x \in G$

Questi fatti rendono agevole l'esecuzione dei calcoli. L'anello RG è caratterizzato dalla seguente proprietà

$(*)$ *se A è un anello, $\sigma : R \longrightarrow A$ un morfismo di anelli e $\tau : G \longrightarrow U(A)$ un morfismo di gruppi tale che $\tau(g)\sigma(r) = \sigma(r)\tau(g)$ per ogni $g \in G$ ed ogni $r \in R$, allora esiste un morfismo di anelli $\rho : RG \longrightarrow A$ tale che $\rho_{|R} = \sigma$ e $\rho_{|G} = \tau$.*

Una situazione in cui tale costruzione si rivela utile è la seguente:

supponiamo di avere un gruppo abeliano A (per il quale useremo la notazione additiva) e sia G un gruppo che agisce su A (ovvero è dato un morfismo $\tau : G \longrightarrow \mathrm{Aut}(A)$). Per ogni $n \in \mathbb{Z}$ sia $s_n \in \mathrm{End}(A)$ l'endomorfismo definito da $s_n(a) = na$ (na è il *multiplo* di a secondo n). Ciascun s_n commuta con ogni endomorfismo, e la la mappa $\sigma : \mathbb{Z} \longrightarrow \mathrm{End}(A)$ definita da $\sigma(n) = s_n$ è un morfismo di anelli. Esiste quindi un morfismo $\rho : \mathbb{Z}G \longrightarrow \mathrm{End}(A)$ e quindi A è uno $\mathbb{Z}G$-modulo. Pertanto, nello studio di una simile situazione, è possibile utilizzare gli strumenti (ed il linguaggio) forniti dalla teoria dei moduli. Ad esempio, in questo contesto, diremo che A è un G-modulo e, se $a \in A$ e $g \in G$, indicheremo $\tau(g)(a)$ semplicemente con ga. Un sotto-G-modulo B di A sarà allora un sottogruppo tale che $gb \in B$ per ogni $b \in B$ e $g \in G$. Il modulo A sarà *semplice* se gli unici suoi sottomoduli sono 0 ed A. Più, se A è anche un R-modulo, un argomento simile mostra che è possibile dotarlo di una struttura di RG-modulo. Lo scenario sopra descritto è piuttosto comune in certi ambiti della teoria dei gruppi. Il caso forse più importante è quello dei *gruppi risolubili*. Se H è un gruppo risolubile allora possiede sottogruppi abeliani normali non banali. Se A è uno di questi ed h è un qualsiasi elemento di h, il coniugio tramite h induce un automorfismo di A. Abbiamo allora un morfismo $\alpha : H \longrightarrow \mathrm{Aut}(A)$ che associa ad ogni h la restrizione ad A del coniugio tramite h. Il nucleo di tale morfismo è $C_H(A)$ e quindi resta definito un morfismo iniettivo $\tau : G = H/C_H(A) \longrightarrow \mathrm{Aut}(A)$. Dunque A possiede la struttura di H-modulo (o di G-modulo) e questo punto di vista può essere utile per ottenere informazioni sia su A che su G. Nel caso in cui il gruppo H sia finito, è chiaro il motivo per cui lo studio di questa situazione risulta naturale: i gruppi A e G hanno ordine inferiore a quello di H, e quindi ci sono i presupposti per utilizzare ragionamenti di tipo induttivo. Anche nel caso di gruppi infiniti, pur non potendo sempre disporre di argomenti di tipo induttivo, questo tipo di approccio fornisce risultati interessanti, a costo di scegliere il sottogruppo A in maniera adeguata. Una scelta di solito fruttuosa è quella di prendere A un sottogruppo normale minimale. Questo, in termini di moduli, significa che A è un H-modulo semplice. Purtroppo, nel caso infinito, tali sottogruppi potrebbero non esistere, anche in situazioni estremamente semplici.

Vediamone un esempio

Esempio 4.2.1 *Sia* $H = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a = \pm 1\, b \in \mathbb{Z} \right\}$. *Il sottogruppo* $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z} \right\}$ *è abeliano e di indice* 2, *quindi normale. Se* $x \in H \setminus N$ *si controlla che* $u^x \neq u$ *per ogni* $u \in N$ *con* $n \neq 1$. *Il gruppo* N *è isomorfo a* $\mathbb{Z}$ *quindi il gruppo* H *è risolubile (ad esempio la*

serie $1 \leq N \leq G$ *è una serie normale a fattori abeliani). Dato che* N *è isomorfo a* $\mathbb{Z}$ *ogni sottogruppo non banale di* N *ha indice finito in* N*. Inoltre, dato un sottogruppo* $M \neq 1$ *di* N *ed* $h \in H$*, abbiamo che* $M^h \leq N^h$ *e l'indice di* M^h *in* N *è uguale all'indice di* M *in* N*. Allora* $M^h = M$ *perché* N *possiede un unico sottogruppo di indice* k *per ogni naturale* $k \geq 1$*. Questo dice che tutti i sottogruppi di* N *sono normali in* H *e pertanto* N *non può contenere sottogruppi che siano normali minimali in* H*. Infatti, per ogni sottogruppo non banale* $A \leq N$*, il sottogruppo* $A^2 = \{ a^2 | a \in A \}$ *è non banale e strettamente contenuto in* A*. Ne deduciamo che* G *non possiede sottogruppi abeliani normali minimali. Infatti, se* A *fosse uno di questi, non potrebbe essere contenuto in* N *e quindi* $AN = G$*. Ma avremmo anche* $A \cap N = 1$ *perché, come osservato in precedenza, nessun elemento fuori da* N *centralizza elementi di* N *diversi da* 1*. Ma* $[A, N] \leq A \cap N = 1$ *e ne risulta che* A *ed* N *commutano, provando che* $H = AN \simeq A \times N$*. Ma allora* A *è ciclico di ordine* 2 *e* H *sarebbe abeliano, una contraddizione.*

Osserviamo comunque che, in questo esempio, tutti i sottogruppi abeliani normali hanno indice finito in N (in realtà anche in H ma questo non è importante).

Occorre quindi, per le applicazioni ai gruppi infiniti, una definizione che possa sostituire, senza far perdere molto, quella di modulo semplice.

Ci limitiamo intanto a gruppi A senza torsione. Se A è un G-modulo, è immediato verificare che G agisce anche su $M = \mathbb{Q} \otimes_{\mathbb{Z}} A$ ponendo, per ogni $q \in \mathbb{Q}, a \in A$ e $g \in G$, $g(q \otimes a) = q \otimes ga$ ed estendendo poi per linearità a tutto M. In tal modo G ha una azione su uno spazio vettoriale. Il caso per noi interessante è quello in cui $A \simeq \mathbb{Z}^n$ perché, in questa situazione, $\mathbb{Q} \otimes_{\mathbb{Z}} A \simeq \mathbb{Q}^n$ è uno spazio vettoriale di dimensione finita. Possiamo allora pensare questo spazio vettoriale come un modulo per l'anello $\mathbb{Q}G$ e il guadagno che otteniamo è che, in questo contesto, i sottomoduli di $\mathbb{Q} \otimes_{\mathbb{Z}} A$ sono sottospazi. Allora, dato che lo spazio ha dimensione finita esisteranno, ad esempio, sia sottomoduli minimali che sottomoduli massimali cosa che, nel caso del modulo A, non è in generale vera. Diamo allora la seguente definizione:

Definizione 4.2.2 *Siano* A *un gruppo abeliano e* G *un gruppo che agisce su* A*. Diremo che* A *è* razionalmente irriducibile *se*

(i) $A \simeq \mathbb{Z}^n$ *per qualche* $n \geq 1$*;*

(ii) Il $\mathbb{Q}G$*-modulo* $\mathbb{Q} \otimes_{\mathbb{Z}} A$ *è semplice.*

Chiaramente ogni $A \simeq \mathbb{Z}^n$ che sia un G-modulo semplice è razionalmente irriducibile, ma l'esempio 4.2.1 prova che non è sempre vero il viceversa. La dimostrazione del seguente fatto viene lasciata al lettore.

Proposizione 4.2.3 *Sia* $A \simeq \mathbb{Z}^n$ *un* G*-modulo. Allora* A *è razionalmente irriducibile se e solo se per ogni* B *sottomodulo non nullo, si ha* A/B *finito.*

Prendiamo adesso un gruppo risolubile G infinito, e supponiamo che N sia un suo sottogruppo normale isomorfo a $\mathbb{Z}^n$. Allora, tra tutti i sottogruppi normali contenuti in N, possiamo sceglierne

uno che abbia rango minimo. Se A è uno di questi, allora A è G-modulo razionalmente irriducibile. Infatti che $B \leq A$ è normale in G, allora è G-sottomodulo di A, ma il suo rango è lo stesso del rango di A. Pertanto A/B deve essere finito e la proposizione 4.2.3 ci dice che A è razionalmente irriducibile. Questa osservazione indica che il concetto di modulo razionalmente irriducibile ha, rispetto a quello di modulo semplice, maggiori possibilità di applicazione.

Vediamo un importante esempio.

Esempio 4.2.4 *Siano $\mathbb{F}$ un campo di numeri, $A = \mathcal{O}_\mathbb{F}$ pensato come gruppo additivo e $G = U(\mathcal{O}_\mathbb{F})$ il gruppo delle unità di $\mathcal{O}_\mathbb{F}$. Supponiamo anche che $\mathbb{Z}[U] = \mathcal{O}_\mathbb{F}$. Il gruppo G agisce in modo naturale su A, tramite la moltiplicazione di $\mathcal{O}_\mathbb{F}$. Vediamo che A è G-modulo razionalmente irriducibile. Intanto sappiamo che $A \simeq \mathbb{Z}^n$ dove n è il grado di $\mathbb{F}$. Se B è un sottomodulo di A, mostriamo che è un ideale in $\mathcal{O}_\mathbb{F}$. Preso $b \in B$ ed $a \in \mathcal{O}_\mathbb{F}$, scriviamo $a = m_1u_1 + \cdots m_ku_k$ per certi $u_i \in U$ ed $m_i \in \mathbb{Z}$. Allora*

$$ab = (m_1u_1 + \cdots m_ku_k)b = m_1u_1b + \cdots m_ku_kb$$

e questo è in B dato che ciascun u_ib appartiene a B. Ne segue che A/B è finito. Per la Proposizione 4.2.3 A è razionalmente irriducible come G-modulo.

Vedremo ora che questo esempio è molto vicino al caso generale. Per enunciare correttamente il risultato che ci interessa introduciamo qualche notazione.

Se il gruppo G agisce su A denotiamo l'azione di g su a con $g.a$. Se, invece x, y sono elementi di un anello, indicheremo il loro prodotto con $x \cdot y$ o xy.

Proposizione 4.2.5 *Siano G un gruppo abeliano ed A un G-modulo fedele e razionalmente irriducibile. Allora esistono un campo di numeri $\mathbb{F}$ e morfismi iniettivi $\sigma : A \longrightarrow \mathcal{O}_\mathbb{F}$, $\tau : G \longrightarrow U = U(\mathcal{O}_\mathbb{F})$ tali che, per ogni $g \in G$ ed $x \in A$, $\sigma(g.x) = \tau(g) \cdot \sigma(x)$. Inoltre $\sigma(A)$ e $\mathbb{Z}[\tau(G)]$ hanno indice finito in $\mathcal{O}_\mathbb{F}$*

Dimostrazione. Poniamo $R = \mathbb{Q}G$ e $V = \mathbb{Q} \otimes_\mathbb{Z} A$. Nelle nostre ipotesi R è un anello commutativo e V è un R-modulo semplice. Identifichiamo A con il sottogruppo $1 \otimes A$ di V indicando quindi con il simbolo a ogni elemento del tipo $1 \otimes a$. Di conseguenza ogni elemento di V del tipo $q \otimes a$ verrà indicato col simbolo qa. Inoltre, se $r \in R$ ed $x \in A$, indicheremo l'azione di r su x come $r.x$. Se consideriamo R come R-modulo e fissiamo $a \in A$ diverso da zero, la funzione

$$\begin{aligned} \lambda : R &\longrightarrow V \\ r &\longmapsto r.a \end{aligned}$$

è un morfismo di moduli e, dato che V è semplice, λ è suriettivo. Se I è il nucleo di λ si verifica, usando la commutatività di R, che $I = \mathrm{ann}(V)$ e quindi è un ideale. Ogni ideale dell'anello R/I è un R-sottomodulo e, essendo V R-isomorfo a ad R/I, gli unici ideali di R/I

sono l'intero anello e lo 0. Di conseguenza I è massimale ed R/I è un campo, che indicheremo con $\mathbb{F}$. Pensato come spazio vettoriale su $\mathbb{Q}$ il campo $\mathbb{F}$ è isomorfo a $\mathbb{Q}^n$ quindi è un campo di numeri. Prendiamo $v \in V$ e supponiamo si possa scrivere come $v = r.a = \overline{r}.a$. Allora $(r-\overline{r})a = 0$ e quindi $r - \overline{r} \in I$. Questo vuol dire che $r + I = \overline{r} + I$ e che porre $\eta(r.a) = r + I$ definisce una funzione da V in R/I che è chiaramente un isomorfismo di R-moduli. Scegliamo $a_1, \ldots, a_n$ dei generatori di A e consideriamo gli elementi $v_i = \eta(a_i) \in R/I = \mathbb{F}$. Sappiamo che, per ogni elemento v di $\mathbb{F}$, esiste un intero non nullo m tale che $mv \in \mathcal{O}_{\mathbb{F}}$. Possiamo allora scegliere m in modo che $mv_i \in \mathcal{O}_{\mathbb{F}}$ per ogni $i = 1, \ldots, n$. A questo punto definiamo la funzione

$$\begin{aligned} \sigma : A &\longrightarrow \mathbb{F} \\ x &\longmapsto m\eta(x) \end{aligned}$$

Per quanto osservato in precedenza, $\mathrm{Im}(\sigma) \subseteq \mathcal{O}_{\mathbb{F}}$ e σ è un morfismo iniettivo di gruppi. Abbiamo allora che $\mathrm{Im}(\sigma)$ è un gruppo libero dello stesso rango di $\mathcal{O}_{\mathbb{F}}$ e dunque $\mathcal{O}_{\mathbb{F}}/\mathrm{Im}(\sigma)$ è finito. Sia $\tau : G \longrightarrow \mathbb{F}$ la restrizione a G della proiezione canonica da R in R/I. Chiaramente τ rispetta i prodotti. Se $\tau(g) = 1$ abbiamo $g - 1 \in I$ e quindi $0 = (g-1).b$. Da questo otteniamo che $g.b = b$ per ogni $b \in A$ e, vista la fedeltà di G, ne deduciamo $g = 1$. Pertanto τ è iniettivo. Prendiamo $g \in G$ ed $x = ra \in A$. Abbiamo

$$\sigma(g.x) = m\eta(g.r.a) = m\eta((gr).a) = mgr + I = (g+I)(mr+I) = \tau(g) \cdot \sigma(x)$$

e quindi, per concludere la dimostrazione, rimane da provare che $\mathrm{Im}(\tau)$ è contenuta in U, il gruppo delle unità di $\mathcal{O}_{\mathbb{F}}$, e che $\mathbb{Z}[\tau(G)]$, il sottoanello generato da $\tau(G)$, ha indice finito in $\mathcal{O}_{\mathbb{F}}$. Per dimostrare la prima affermazione scegliamo un $g \in G$. Fissata una base di A l'elemento g, nella sua azione su A, si può rappresentare tramite una matrice $\mu_g \in \mathrm{GL}(n, \mathbb{Z})$. Se $f = \sum_{i=0}^{n-1} c_i x^i + x^n = \det(xI - \mu_g)$ è il polinomio caratteristico di μ_g, il Teorema di Cayley-Hamilton ci dice che $f(\mu_g) = 0$. Allora $f(\mu_g).a = 0$ e, applicando σ a questa uguaglianza, troviamo

$$\begin{aligned} 0 = \sigma\Big(\Big(\sum_{i=0}^{n-1} c_i g^i + g^n\Big).a\Big) = \sigma\Big(\sum_{i=0}^{n-1} c_i g^i.a + g^n.a\Big) = \\ = \sum_{i=0}^{n-1} c_i \tau(g)^i \cdot \sigma(a) + \tau(g)^n \cdot \sigma(a) = \Big(\sum_{i=0}^{n-1} c_i \tau(g)^+ \tau(g)^n\Big) \cdot \sigma(a) = \\ = f(\tau(g)) \cdot \sigma(a) = 0. \end{aligned}$$

Dato che siamo in un dominio questa uguaglianza implica $f(\tau(g)) = 0$. Essendo $\tau(g)$ zero di un polinomio monico e non nullo a coefficienti in $\mathbb{Z}$, ne segue che $\tau(g) \in \mathcal{O}_{\mathbb{F}}$. Prendiamo ora un elemento $r + I \in R/I$ ed osserviamo che esiste un intero $k \neq 0$ tale che $k(r+I) \in \mathbb{Z}G + I/I = \mathbb{Z}[\tau(G)]$. In particolare questo dice ogni elemento del quoziente $\mathcal{O}_{\mathbb{F}}/\mathbb{Z}[\tau(G)]$ ha periodo finito. Dato che questo gruppo è finitamente generato, questa affermazione equivale a dire che $\mathcal{O}_{\mathbb{F}}/\mathbb{Z}[\tau(G)]$ è finito, dimostrando quindi la proposizione. □

Questo risultato è uno strumento fondamentale per indagare la struttura dei gruppi risolubili. Una conseguenza importante è la seguente.

Corollario 4.2.6 *Sia G un gruppo abeliano che agisce in modo fedele e razionalmente irriducibile su $A \simeq \mathbb{Z}^n$. Allora G è finitamente generato, $T(G)$ è ciclico ed il rango di $G/T(G)$ è minore o uguale ad $n-1$.*

Dimostrazione. Usando la Proposizione 4.2.3 vediamo che G è isomorfo ad un sottogruppo del gruppo delle unità di $\mathcal{O}_{\mathbb{F}}$, per qualche campo di numeri di grado $n = s + 2t$ (s, t hanno l'usuale significato). Il Teorema delle unità di Dirichlet ci dice allora che $T(G)$ è ciclico e che il rango di $G/T(G) \leq s + t - 1 \leq n - 1$. □

Capitolo 5

Estensioni ciclotomiche

In questo capitolo ci occuperemo di una importante classe di estensioni di $\mathbb{Q}$, ovvero le *estensioni ciclotomiche*. Un numero complesso ω è una *radice n-esima* dell'unità se $\omega^n = 1$. Se inoltre l'ordine di ω è n, si dice che ω è una radice n-esima *primitiva*. Ogni estensione di $\mathbb{Q}$ tramite una radice dell'unità si dice una estensione ciclotomica e, se $\mathbb{F} = \mathbb{Q}[\omega]$ con ω radice n-esima primitiva di 1, diremo che $\mathbb{F}$ è l'*n-esima estensione ciclotomica*. Le estensioni ciclotomiche sono un argomento centrale nella teoria algebrica dei numeri e vedremo, in questo capitolo, alcune delle loro proprietà fondamentali. Come applicazione dimostreremo il cosiddetto *Primo Caso* del celebre risultato di Kummer riguardante il Teorema di Fermat per primi regolari.

Iniziamo il nostro studio, dimostrando alcuni fatti nel caso in cui n sia la potenza di un primo.

Proposizione 5.0.1 *Siano $n = p^k$ con p primo ed ω una radice n-esima primitiva di 1. Se $\mathbb{F} = \mathbb{Q}[\omega]$ allora*

- *l'elemento $\pi = 1 - \omega$ è primo in $\mathcal{O}_\mathbb{F}$ e $(p) = (\pi)^{\varphi(n)}$;*
- *l'elemento $1 + \omega$ è una unità di $\mathcal{O}_\mathbb{F}$;*
- *il grado di $\mathbb{F}$ è $\varphi(n) = p^{k-1}(p-1)$;*
- *$\mathcal{O}_\mathbb{F}/(\pi) \simeq \mathbb{Z}/p\mathbb{Z}$.*

Dimostrazione. Sia $f = \sum_{i=0}^{p-1} x^{ip^{k-1}}$. Dato che $x^{p^k} - 1 = f(x^{p^{k-1}} - 1)$, per ogni ζ radice n-esima primitiva di 1, si deve avere $f(\zeta) = 1$. Dato che ogni radice n-esima primitiva è della forma ω^m per qualche m coprimo con n e nell'intervallo $[0, n[$, tali radici sono $\varphi(n)$ e, di conseguenza, deve essere

$$f = \prod_{\zeta \text{ primitiva}} (x - \zeta)$$

Ne deduciamo che il polinomio minimo di ω, che deve dividere f, ha grado minore o uguale a $\varphi(n)$. Osserviamo che $p = f(1)$ e, usando la fattorizzazione di f, possiamo scrivere $p = \prod_{\zeta \text{ primitiva}}(1-\zeta)$.

Ogni fattore $1-\zeta$ è un intero algebrico. Prendiamo ora due qualsiasi radici n-esime primitive, α e β, e scriviamo $\alpha = \beta^m$. Ricaviamo allora

$$\frac{1-\alpha}{1-\beta} = \frac{1-\beta^m}{1-\beta} = 1 + \beta + \cdots + \beta^{m-1} \in \mathbb{Z}[\beta] \leq \mathcal{O}_{\mathbb{F}}.$$

Dato che questo vale per ogni coppia di radici n-esime primitive, si ha che tutti gli elementi del tipo $(1-\alpha)/(1-\beta)$ sono unità di $\mathcal{O}_{\mathbb{F}}$. Possiamo allora scrivere

$$p = \prod_{\zeta \text{ primitiva}} (1-\zeta) = \prod_{\zeta \text{ primitiva}} \frac{1-\zeta}{1-\omega}(1-\omega) = u\pi^{\varphi(n)}$$

dove u è il prodotto di tutti i fattori $(1-\zeta)/(1-\omega)$ ed è quindi una unità di $\mathcal{O}_{\mathbb{F}}$. Passando agli ideali otteniamo $(p) = (\pi)^{\varphi(n)}$ e questa uguaglianza prova che ogni primo che divide (p) ha indice di ramificazione maggiore o uguale a $\varphi(n)$. D'altra parte sappiamo che tale indice non può superare il grado di $\mathbb{F}$ e dunque, usando quanto osservato sopra, otteniamo che il grado di $\mathbb{F}$ è $\varphi(n)$. Un'altra conseguenza è che (π) deve essere primo, dato che il numero di fattori primi nella decomposizione di (p) è limitato dal grado di $\mathbb{F}$. Per mostrare che $1+\omega$ è invertibile, partiamo dall'uguaglianza $x^{p^k} - 1 = f(x^{p^{k-1}} - 1)$ e valutiamola in -1. Si ottiene $-2 = f(-1)(-2$ e quindi $f(-1) = 1$. Ricordando la fattorizzazione di f possiamo scrivere

$$1 = (1+\omega) \cdot \prod_{\substack{\zeta \text{ primitiva} \\ \zeta \neq \omega}} (1+\zeta)$$

e questo dice che $1+\omega$ è un intero algebrico invertibile, dato che tutti i fattori della produttoria sono interi algebrici.

Infine, sempre come conseguenza della relazione tra grado, indici di inerzia e di ramificazione, deduciamo che l'indice di inerzia di (π) è 1, ovvero $\mathcal{O}_{\mathbb{F}}/(\pi) \simeq \mathbb{Z}/p\mathbb{Z}$. □

5.1 Discriminanti

Abbiamo bisogno di alcuni risultati che ci aiutino a calcolare il discriminante di certe estensioni ciclotomiche.

Lemma 5.1.1 *Siano $\mathbb{F} = \mathbb{Q}[a]$ un campo di numeri di grado n ed f il polinomio minimo di a su $\mathbb{Q}$. Allora $\Delta[1, a, \ldots . a^{n-1}] = (-1)^{\binom{n}{2}} N(f'(a))$.*

Dimostrazione. Indichiamo con $a_i = \sigma_i(a)$ le immagini di a tramite le immersioni $\sigma_1, \ldots, \sigma_n$ di $\mathbb{F}$. Allora $f = \prod_{i=1}^n (x - a_i)$ e

$$f' = \sum_{i=1}^{n} \prod_{j \neq i} (x - a_j).$$

Se $l \neq i$ abbiamo $\prod_{j \neq i}(a_l - a_j) = 0$ perché $0 = (a_l - a_l)$ è uno dei fattori in questo prodotto, e dunque

$$\sigma_l(f'(a)) = f'(\sigma_l(a)) = f'(a_l) = \prod_{j \neq l} (a_l - a_j).$$

Otteniamo allora

$$N(f'(a)) = \prod_{i=1}^{n} \sigma_i(f'(a)) = \prod_{i=1}^{n} \prod_{j \neq i} (a_i - a_j) = \prod_{j \neq i} (a_i - a_j).$$

Raggruppando alcuni termini abbiamo

$$N(f'(a)) = \prod_{i<j} (a_i - a_j)(a_j - a_i) = \prod_{i<j} -1 \cdot (a_i - a_j)^2 = (-1)^{\binom{n}{2}} \prod_{i<j} (a_i - a_j)^2.$$

Per concludere basta ricordare che $\Delta[1, a, \ldots, a^{n-1}] = \prod_{i<j}(a_i - a_j)^2$. □.

Il prossimo lemma fornisce un semplice metodo per determinare il segno del discriminante di un campo di numeri.

Lemma 5.1.2 *Sia $\mathbb{F}$ un campo di numeri con $2t$ immersioni complesse. Allora il segno di $\Delta_{\mathbb{F}}$ è $(-1)^t$.*

Dimostrazione. Scriviamo $n = |\mathbb{F} : \mathbb{Q}| = s + 2t$ ed elenchiamo le immersioni di $\mathbb{F}$ come $\sigma_1, \ldots, \sigma_n$ in modo che σ_i sia una immersione reale se e solo se $i \leq s$. Enumeriamo le immersioni complesse in modo che $\overline{\sigma_{s+i}} = \sigma_{s+t+i}$. Scegliamo ora $a \in \mathcal{O}_{\mathbb{F}}$ in modo che $\mathbb{F} = \mathbb{Q}[a]$. Inoltre, se $s \neq 0$, chiediamo anche $a \in \mathbb{R}$. Posto $a_i = \sigma_i(a)$ abbiamo che $a_i \in \mathbb{R}$ se e solo se $i \leq s$. Ovviamente basta provare che $a_i \notin \mathbb{R}$ se $i > s$. Questo è immediato una volta che si osserva che $\sigma_i(\mathbb{F}) = \mathbb{Q}[a_i]$. Dalla relazione $\Delta[1, a, \ldots, a^{n-1}] = |\mathcal{O}_{\mathbb{F}}/\mathbb{Z}[a]|^2 \, \Delta_{\mathbb{F}}$ si deduce che il segno di $\Delta_{\mathbb{F}}$ è uguale al segno di $\Delta[1, a, \ldots, a^{n-1}]$ e quindi cercheremo di determinare questo. Scriviamo

$$\Delta = \Delta[1, a, \ldots, a^{n-1}] = \prod_{i<j} (a_i - a_j)^2$$

e notiamo che, per ogni $1 \leq i < j \leq s$, il fattore $(a_i - a_j)^2$ è positivo e non influisce sul segno di Δ. Se invece $i \leq s$ mentre $j > s$, esiste un indice $j \neq k > s$ tale che $a_k = \overline{a_j}$ e quindi nella produttoria troviamo i fattori $(a_i - a_j)^2$ e $(a_i - a_k)^2 = (a_i - \overline{a_j})^2 = \overline{(a_i - a_j)^2}$. Dato che

$$(a_i - a_j)^2 \cdot (a_i - a_k)^2 = (a_i - a_j)^2 \cdot \overline{(a_i - a_j)^2} > 0$$

anche questi fattori non influiscono su segno di Δ. Infine, se $i, j > s$ e $a_i \neq \overline{a_j}$, poniamo $a_l = \overline{a_i}$ e $a_k = \overline{a_j}$. Comunque siano ordinati gli indici i, j, k ed l, nella nostra produttoria compare il fattore

$$(a_i - a_j)^2 \cdot (a_l - a_k)^2 = (a_i - a_j)^2 \cdot \overline{(a_i - a_j)^2} > 0.$$

Pertanto anche questi fattori possono essere omessi senza alterare il segno del discriminante. Rimangono quindi i soli fattori del tipo $(a_i - a_j)^2$ dove $i < j$ e a_j è il coniugato di a_i. Vista la numerazione scelta per le immersioni si ha $j = i + t$. Di conseguenza il segno Δ è uguale al segno del numero reale

$$\alpha = \prod_{i=1}^{t} (a_{s+i} - a_{s+t+i})^2 = \prod_{i=1}^{t} (a_{s+i} - \overline{a_{s+i}})^2 = \prod_{i=1}^{t} (\mathrm{im}(a_{s+i}))^2$$

e, visto tutte le parti immaginarie $\mathrm{im}(a_{s+i})$ sono diverse da zero, i loro quadrati sono numeri reali strettamente negativi. A questo punto è chiaro che il segno di α è $(-1)^t$. □

Veniamo ora al caso delle estensioni ciclotomiche. Per molti dei risultati che proveremo in seguito, la seguente proposizione, per quanto poco precisa, sarà sufficiente.

Proposizione 5.1.3 *Sia ω una radice n-esima primitiva di 1 e indichiamo con m il grado di $\mathbb{F} = \mathbb{Q}[\omega]$. Allora $\Delta_{\mathbb{F}}$ divide n^m. In particolare, se $n = p^k$ con p un primo, $\Delta_{\mathbb{F}}$ è una potenza di p.*

Dimostrazione. Indichiamo con Φ il polinomio minimo di ω e scriviamo $x^n - 1 = g \cdot \Phi$ con $g \in \mathbb{Z}[x]$ un opportuno polinomio. Differenziando si ottiene $nx^{n-1} = g'\Phi + g\Phi'$ e valutando in ω

$$n\omega^n = g'(\omega)\Phi(\omega) + g(\omega)\Phi'(\omega) = g(\omega)\Phi'(\omega).$$

Passando alle norme

$$N(n\omega^n) = N(g(\omega)\Phi'(\omega)) = N(g(\omega))\, N(\Phi'(\omega))$$

e, dato che $N(\omega) = 1$, $n^m = N(g(\omega))\, N(\Phi'(\omega))$. Gli elementi $g(\omega)$ e $\Phi'(\omega)$ sono intero algebrici, quindi le loro norme sono interi. Ne segue che $N(\Phi'(\omega))$ divide n^m. Dalla relazione

$$\Delta[1, \omega, \ldots \omega^{n-1}] = \Delta_{\mathbb{F}}\, |\mathcal{O}_{\mathbb{F}}/\mathbb{Z}[\omega]|^2$$

otteniamo che $\Delta_{\mathbb{F}}$ divide $\Delta[1, \omega, \ldots \omega^{n-1}]$. Per concludere basta usare il Lemma 5.1.1 che ci dice che $N(\Phi'(\omega)) = \pm\Delta[1, \omega, \ldots \omega^{n-1}]$. □

Cercheremo adesso di calcolare il discriminante nel caso di estensioni con radici di ordine $n = p^k$.

Proposizione 5.1.4 *Siano $n = p^k \geq 3$ con p un primo ed ω una radice n-esima di 1. Posto $\mathbb{F} = \mathbb{Q}[\omega]$ si ha $\Delta_{\mathbb{F}} = (-1)^{\varphi(n)/2} p^c$ dove $c = p^{k-1}(pk - k - 1)$.*

Dimostrazione. Il polinomio minimo Φ di ω è stato determinato nella dimostrazione della Proposizione 5.0.1 e possiamo scrivere $x^{p^k} - 1 = \Phi(x^{p^{k-1}} - 1)$. Possiamo anche usare la Proposizione 5.1.3 per ottenere l'uguaglianza $p^{\varphi(n)k} = N(\omega)N(\omega^{p^{k-1}} - 1)$. Osserviamo che $\zeta = \omega^{p^{k-1}}$ è una radice p-esima primitiva di 1. Il campo $\mathbb{K} = \mathbb{Q}[\zeta]$ è una estensione ciclotomica di grado $p - 1$ e le sue immersioni sono automorfismi in $G = \mathcal{G}al(\mathbb{K}|\mathbb{Q})$. Ciascuno di questi si estende a $m = \varphi(n)/(p-1)$ differenti immersioni di $\mathbb{F}$, anche queste elementi di $H = \mathcal{G}al(\mathbb{F}|\mathbb{Q})$. Quindi

$$N(\zeta - 1) = \prod_{\sigma \in H} \sigma(\zeta - 1) = \prod_{\tau \in G} (\tau(\zeta - 1))^m = \left(\prod_{\tau \in G} \tau(\zeta - 1) \right)^m$$

Ma $\prod_{\tau \in G}(\tau(\zeta - 1))$ è la norma di $\zeta - 1$ nel campo $\mathbb{K}$. Per evitare confusione la indicheremo con $N_{\mathbb{K}}(\zeta - 1)$. Dato che $\mathbb{K} = \mathbb{Q}[\zeta - 1]$, il polinomio minimo di $\zeta - 1$ ha grado $p - 1$. Se f è il polinomio minimo di ζ ed $h = f(1 + x)$, abbiamo $h(\zeta - 1) = f(\zeta) = 0$ ed, essendo $\deg(f) = \deg(h)$, h

è il polinomio minimo di $\zeta - 1$. Allora, a meno del segno, $N_{\mathbb{K}}(\zeta - 1)$ è , il termine noto di h, quindi $|N_{\mathbb{K}}(\zeta - 1)| = |h(0)| = |f(1)|$. Dato che $f = \sum_{i=0}^{p-1} x^i$ si ottiene $|N_{\mathbb{K}}(\zeta - 1)| = p$. Possiamo determinare il valore assoluto di $N(\Phi'(\omega))$ ottenendo

$$|N(\Phi'(\omega))| = \frac{p^{\varphi(n)k}}{p^{\varphi(n)/(p-1)}} = p^{p^{k-1}(pk-k-1)}.$$

Infine, essendo $n \geq 3$, tutte le immersioni di $\mathbb{F}$ sono complesse e, usando il Lemma 5.1.2, otteniamo $N(\Phi'(\omega)) = (-1)^{\varphi(n)/2} p^{p^{k-1}(pk-k-1)}$ come richiesto. □

Possiamo ora determinare ora il grado di una qualsiasi estensione ciclotomica.

Proposizione 5.1.5 *Sia ω una radice n-esima primitiva di 1. Allora il grado di $\mathbb{F} = \mathbb{Q}[\omega]$ è $\varphi(n)$.*

Dimostrazione. La dimostrazione procede per induzione su n. Se $n = 2, 3$ il risultato è vero Assumiamo la tesi vera per tutti gli interi minori di n. Se n è potenza di un primo usiamo la Proposizione 5.0.1, quindi possiamo assumere che n abbia la forma $n = p^k m$ con p primo e $p \nmid m$. Definiamo $\zeta = \omega^{p^k}$ ed $\varepsilon = \omega^m$ e poniamo $\mathbb{K} = \mathbb{Q}[\varepsilon]$, $\mathbb{L} = \mathbb{Q}[\zeta]$. Abbiamo allora

- ζ è una radice m-esima primitiva ed ε è una radice p^k-esima primitiva;
- $|\mathbb{K} : \mathbb{Q}| = \varphi(p^k)$ e $|\mathbb{L} : \mathbb{Q}| = \varphi(m)$, per ipotesi induttiva.
- $\mathbb{F} = \mathbb{K}[\zeta] = \mathbb{L}[\varepsilon]$ perché, se scriviamo $1 = ap^k + bm$, abbiamo $\omega = \omega^{ap^k}\omega^{bm} = \zeta^a \varepsilon^b$ e quindi $\omega \in \mathbb{K}[\zeta]$ e $\omega \in \mathbb{L}[\varepsilon]$.

Abbiamo visto che $p\mathcal{O}_{\mathbb{K}} = ((1-\varepsilon)\mathcal{O}_{\mathbb{K}})^{\varphi(p^k)}$ e p è l'unico primo ramificato in $\mathbb{K}$ essendo l'unico primo che divide $\Delta_{\mathbb{K}}$. Per la Proposizione 5.1.3 p non divide $\Delta_{\mathbb{L}}$ e quindi p non si ramifica in $\mathbb{L}$. Abbiamo la fattorizzazione $p\mathcal{O}_{\mathbb{L}} = \mathcal{P}_1\mathcal{P}_2 \cdots \mathcal{P}_l$ ove i $\mathcal{P}_i$ sono primi distinti ed $l \leq \varphi(m)$. Se consideriamo la fattorizzazione di $p\mathcal{O}_{\mathbb{F}}$ abbiamo due modi per studiarla. Da un lato

$$p\mathcal{O}_{\mathbb{F}} = ((1-\varepsilon)\mathcal{O}_{\mathbb{K}})^{\varphi(p^k)}\mathcal{O}_{\mathbb{F}} = ((1-\varepsilon)\mathcal{O}_{\mathbb{F}})^{\varphi(p^k)}$$

e questo ci dice che, se Q è un primo che divide $p\mathcal{O}_{\mathbb{F}}$, il suo esponente nella fattorizzazione è un multiplo di $\varphi(p^k)$. Se invece pensiamo $p\mathcal{O}_{\mathbb{F}}$ come $(\mathcal{P}_1\mathcal{P}_2 \cdots \mathcal{P}_l)\mathcal{O}_{\mathbb{F}}$ otteniamo

$$p\mathcal{O}_{\mathbb{F}} = \prod_{i=1}^{l} \mathcal{P}_i\mathcal{O}_{\mathbb{F}}.$$

Dato che p è ramificato in $\mathbb{F}$ almeno uno dei primi $\mathcal{P}_i$ deve ramificarsi in $\mathbb{F}$, altrimenti $\prod_{i=1}^{l} \mathcal{P}_i\mathcal{O}_{\mathbb{F}}$ sarebbe un prodotto di primi distinti. Dunque, essendo $\mathbb{F}$ una estensione di Galois, tutti i primi nella decomposizione di $p\mathcal{O}_{\mathbb{F}}$ devono avere lo stesso indice di ramificazione e. Fissiamo la nostra attenzione su uno dei fattori di $p\mathcal{O}_{\mathbb{F}}$, ad esempio $\mathcal{P}_1\mathcal{O}_{\mathbb{F}}$. Scrivendo $\mathbb{F} = \mathbb{L}[\varepsilon]$ vediamo che l'estensione $\mathbb{F}|\mathbb{L}$ è di Galois ed il suo grado d è minore o uguale a $\varphi(p^k)$. Di conseguenza tutti i primi nella decomposizione di $\mathcal{P}_1\mathcal{O}_{\mathbb{F}}$ sono ramificati con indice di ramificazione e_1 e, per

la nota relazione tra grado, indici di ramificazione e di inerzia, deve essere $e_1 \leq d \leq \varphi(p^k)$. Se Q è uno dei primi che divide $\mathcal{P}_1\mathcal{O}_{\mathbb{F}}$ allora non può dividere nessuno degli ideali $\mathcal{P}_i\mathcal{O}_{\mathbb{F}}$ quando $i \neq 1$ altrimenti $Q \cap \mathcal{O}_{\mathbb{L}} \supseteq (\mathcal{P}_1, \mathcal{P}_i) = \mathcal{O}_{\mathbb{L}}$. Allora Q compare con esponente e_1 nella fattorizzazione di $p\mathcal{O}_{\mathbb{F}}$, provando che $e_1 = e$. Abbiamo già ottenuto la disuguaglianza $\varphi(p^k) \leq e$ e allora, avendo anche $e \leq d \leq \varphi(p^k)$, otteniamo $e = d = \varphi(p^k)$. Da questo ricaviamo

$$|\mathbb{F} : \mathbb{Q}| = |\mathbb{F} : \mathbb{L}| \cdot |\mathbb{L} : \mathbb{Q}| = \varphi(m)\varphi(p^k) = \varphi(n)$$

e la dimostrazione è conclusa. □

Concludiamo descrivendo il gruppo di Galois.

Proposizione 5.1.6 *Siano ω una radice n-esima primitiva di 1 ed $\mathbb{F} = \mathbb{Q}[\omega]$. Allora il gruppo di Galois G di $\mathbb{F}|\mathbb{Q}$ è isomorfo al gruppo U_n degli invertibili dell'anello $\mathbb{Z}/n\mathbb{Z}$..*

Dimostrazione. Sappiamo già che $|G| = \varphi(n) = |U|$. Ogni elemento di G induce un automorfismo di $\langle\omega\rangle$ ed in questo modo abbiamo un morfismo da G in $\mathrm{Aut}(\langle\omega\rangle) \simeq U_n$. Se σ è elemento del nucleo di tale morfismo, allora $\sigma(\omega) = \omega$ e quindi σ deve essere l'identità provando che G è isomorfo ad un sottogruppo di U_n. Quanto detto in precedenza sugli ordini di G ed U_n, mostra che G ed U_n sono isomorfi. □

Una utile conseguenza è contenuta nel seguente corollario.

Corollario 5.1.7 *Se $\mathbb{F}$ è una estensione ciclotomica e $\mathbb{K} \leq \mathbb{F}$ è un sottocampo, allora $\mathbb{K}|\mathbb{Q}$ è un'estensione di Galois.*

Dimostrazione.Il gruppo di Galois dell'estensione è abeliano e quindi tutti i suoi sottogruppi sono normali. Per le note proprietà della corrispondenza si Galois, ogni sottocampo $\mathbb{K}$ è estensione di Galois di $\mathbb{Q}$. □

5.2 Anelli ciclotomici

In questa sezione determineremo l'anello degli interi di una qualsiasi estensione ciclotomica. Ricordiamo che, se A, B sono sottoanelli di un anello C, si indica con AB il sottoanello generato dai prodotti del tipo ab al variare di $a \in A$ e $b \in B$.

Lemma 5.2.1 *Siano $\mathbb{F}, \mathbb{K}$ campi di numeri di grado n ed m e poniamo $d = MCD(\Delta_{\mathbb{F}}, \Delta_{\mathbb{K}})$. Se $\mathbb{E}$ è il campo generato da $\mathbb{F}$ e $\mathbb{K}$ e $|\mathbb{E} : \mathbb{Q}| = nm$, allora si ha*

$$\mathcal{O}_{\mathbb{E}} \subseteq \frac{1}{d}\mathcal{O}_{\mathbb{F}}\mathcal{O}_{\mathbb{K}}.$$

Dimostrazione. L'ipotesi $|\mathbb{E} : \mathbb{Q}| = nm$ ha diverse utili conseguenze. Per prima cosa si ottiene $|\mathbb{E} : \mathbb{F}| = m$ e $|\mathbb{E} : \mathbb{K}| = n$ e quindi, ad esempio, ogni $\mathbb{Q}$-base di $\mathbb{K}$ è anche una $\mathbb{F}$-base di $\mathbb{E}$.

Inoltre ogni immersione di $\mathbb{F}$ si estende ad m distinte immersioni di $\mathbb{E}$. Scegliamo basi intere $\{ a_1, \ldots, a_n \}$, $\{ b_1, \ldots, b_m \}$ per $\mathcal{O}_\mathbb{F}$ ed $\mathcal{O}_\mathbb{K}$ e osserviamo che l'insieme

$$\{ a_i b_j \mid i = 1, \ldots n,\ j = 1, \ldots, m \}$$

è una $\mathbb{Q}$-base per $\mathbb{E}$. Ogni elemento di $\mathbb{E}$ si può quindi scrivere come combinazione, a coefficienti razionali, degli $a_i b_j$. Preso $c \in \mathcal{O}_\mathbb{E}$ è possibile scriverlo come

$$c = \sum_{ij} \frac{x_{ij}}{r} a_i b_j$$

dove r e gli x_{ij} sono interi e, per ogni primo p che divide r, c'è almeno una coppia (i, j) per cui p non divide x_{ij}. L'dentità di $\mathbb{K}$ si estende ad n immersioni $\sigma_1, \ldots . \sigma_n$ di $\mathbb{E}$ e, applicandole alla precedente equazione, otteniamo le n equazioni

$$\begin{cases} \sigma_l(c) = \sum_{ij} \frac{x_{ij}}{r} \sigma_l(a_i) b_j \\ l = 1, 2, \ldots, n \end{cases}$$

Se poniamo $y_i = \sum_{j=1}^{m} \frac{x_{ij}}{r} b_j$ per ogni $i = 1, \ldots, n$, possiamo riscrivere queste relazioni nella forma

$$\begin{cases} \sigma_l(c) = \sum_{i=1}^{n} \sigma_l(a_i) y_i \\ l = 1, 2, \ldots, n \end{cases}$$

da cui è chiaro che $(y_1, \ldots, y_n)$ è una soluzione del sistema

$$\mathcal{S} : \begin{cases} \sigma_l(c) = \sum_{i=1}^{n} \sigma_l(a_i) t_i \\ l = 1, 2, \ldots, n. \end{cases}$$

Le immersioni σ_i, ristrette ad $\mathbb{F}$, ci danno immersioni τ_i di $\mathbb{F}$ e queste sono tutte distinte. Infatti, se $\tau_l = \tau_k$ allora, per ogni coppia (i, j) avremmo

$$\sigma_l(a_i b_j) = \sigma_l(a_i) b_j = \tau_l(a_i) b_j = \tau_k(a_i) b_j = \sigma_k(a_i) b_j = \sigma_k(a_i b_j)$$

e questo implica $\sigma_l = \sigma_k$. La matrice incompleta si $\mathcal{S}$ è $A = (\sigma_l(a_k)) = (\tau_l(a_k))$ e dunque, visto che $\det(a)^2 = \Delta_\mathbb{F}$, il suo determinante non è 0. Indichiamo con A_i la matrice ottenuta da A sostituendo alla colonna i-esima la colonna dei termini noti. Il teorema di Cramer dice allora che, per ogni $i = 1, \ldots n$,

$$y_i = \frac{det(A_i)}{\det(A)} = \frac{u_i}{v}$$

dove $v^2 = \Delta_\mathbb{F}$. Si ottiene $\Delta_\mathbb{F}\, y_i = v u_i$ che è quindi un intero algebrico. Esplicitando questa uguaglianza possiamo scrivere

$$\Delta_\mathbb{F}\, y_i = \sum_{j=1}^{m} \Delta_\mathbb{F} \frac{x_{ij}}{r} b_j$$

e questo prova che $\Delta_\mathbb{F}\, y_i$ appartiene a $\mathbb{K}$ e quindi a $\mathcal{O}_\mathbb{K}$. Ma $\{ b_1, \ldots, b_m \}$ è una $\mathbb{Z}$-base di $\mathcal{O}_\mathbb{K}$ e dunque tutti i coefficienti $\Delta_\mathbb{F} \frac{x_{ij}}{r}$ devono essere interi. Sia p^k una potenza di primo che divide r

e scegliamo (i,j) in modo che p non divida x_{ij}. Il fatto che $\Delta_{\mathbb{F}}\frac{x_{ij}}{r}$ sia un intero implica $p^r|\Delta_{\mathbb{F}}$. Dato che questo accade per ogni potenza di primo che divida r abbiamo provato che r divide $\Delta_{\mathbb{F}}$ e, invertendo i ruoli di $\mathbb{F}$ e $\Delta_{\mathbb{K}}$ otteniamo $r|\Delta_{\mathbb{K}}$. Allora r divide d ovvero $d/r \in \mathbb{Z}$. Possiamo quindi scrivere c come

$$c = \sum_{ij} \frac{x_{ij}}{r} a_i b_j = \sum_{ij} \frac{x_{ij}}{d}\frac{d}{r} a_i b_j = \frac{1}{d}\sum_{ij} x_{ij}\frac{d}{r} a_i b_j \in \frac{1}{d}\mathcal{O}_{\mathbb{F}}\mathcal{O}_{\mathbb{K}}$$

e la dimostrazione è conclusa. □

Possiamo adesso descrivere l'anello degli interi di una generica estensione ciclotomica.

Teorema 5.2.2 *Siano ω una radice n-esima dell'unità ed $\mathbb{F} = \mathbb{Q}[\omega]$. Allora $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\omega]$.*

Dimostrazione. Dimostreremo la tesi per induzione su n. Se $n = 3$ il teorema è vero per la proposizione 5.0.1. Supponiamo quindi che il teorema valga per tutti i naturali minori di n. Se n è una potenza di primo possiamo ancora usare la Proposizione 5.0.1 e concludere. Altrimenti scriviamo $n = lm$ con $MCD(l,m) = 1$ e poniamo $\varepsilon = \omega^l$, $\zeta = \omega^m$. Definiamo anche $\mathbb{K} = \mathbb{Q}[\varepsilon]$ ed $\mathbb{L} = \mathbb{Q}[\zeta]$. Dato che ε e ζ sono, rispettivamente, radici m-esime ed l-esime primitive di 1, le proposizione 5.1.3 e 5.1.5 ci dicono che $\Delta_{\mathbb{K}}| m^{\varphi(m)}$ e $\Delta_{\mathbb{L}}| l^{\varphi(l)}$. Da questo segue che $MCD(\Delta_{\mathbb{K}}, \Delta_{\mathbb{L}}) = 1$. Abbiamo già osservato che $\mathbb{Q}[\varepsilon,\zeta] = \mathbb{Q}[\omega]$ e sappiamo, per la Proposizione 5.1.5, che $|\mathbb{F} : \mathbb{Q}| = |\mathbb{K} : \mathbb{Q}| \cdot |\mathbb{L} : \mathbb{Q}|$. Il Lemma 5.2.1 ci assicura dunque che $\mathcal{O}_{\mathbb{F}} \subseteq \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$. Per ipotesi induttiva $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\varepsilon]$ e $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta]$, quindi $\mathcal{O}_{\mathbb{F}} \subseteq \mathbb{Z}[\varepsilon]\mathbb{Z}[\zeta] = D$. Ma il sottoanello D è contenuto in $\mathbb{Z}[\omega]$ visto che $\varepsilon, \zeta \in \mathbb{Z}[\omega]$ e si ha

$$\mathbb{Z}[\omega] \leq \mathcal{O}_{\mathbb{F}} \leq D \leq \mathbb{Z}[\omega]$$

provando che $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\omega]$. □

Se $\mathbb{F} = \mathbb{Q}[\omega]$ è l'estensione ciclotomica ottenuta aggiungendo una radice n-esima primitiva, il suo gruppo di Galois ha ordine $\varphi(n)$ e, dato che gli elementi di G inducono automorfismi del gruppo $\langle\omega\rangle$, che è isomorfo al gruppo U degli invertibili di $\mathbb{Z}/n\mathbb{Z}$, abbiamo $G \simeq U$. In particolare, se $n = p$ un primo dispari, G è ciclico di ordine $p-1$. Di conseguenza G ha un unico sottogruppo di indice 2 ed $\mathbb{F}$ ha un unico sottocampo $\mathbb{K}$ di grado 2. Questo campo è descritto nella seguente proposizione.

Proposizione 5.2.3 *Siano p un primo dispari e $\mathbb{F} = \mathbb{Q}[\omega]$ la p-esima estensione ciclotomica. Allora il sottocampo quadratico $\mathbb{K}$ di $\mathbb{F}$ è $\mathbb{Q}[\sqrt{p}]$ se $p \equiv 1 \pmod 4$ e $\mathbb{Q}[\sqrt{-p}]$ se $p \equiv 3 \pmod 4$.*

Dimostrazione. Scriviamo $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$ con d intero libero da quadrati. Se q è un primo che divide $\Delta_{\mathbb{K}}$ allora è ramificato in $\mathbb{K}$ e quindi in $\mathbb{F}$. D'altra parte p è l'unico primo ramificato in $\mathbb{F}$ e ne deduciamo che $d = \pm p$. Se $d \equiv 2, 4 \pmod 4$ il discriminante di $\mathbb{K}$ è $4d$ e, visto che 2 non è ramificato, deve essere $d \equiv 1 \pmod 4$. Dunque $d = p$ se $p \equiv 1 \pmod 4$, mentre $d = -p$ quando $p \equiv 3 \pmod 4$. □

il prossimo teorema è una interessante conseguenza di questo fatto.

Teorema 5.2.4 *Sia $\mathbb{K}$ una estensione quadratica si $\mathbb{Q}$. Allora esiste una estensione ciclotomica $\mathbb{F}$ tale che $\mathbb{K} \leq \mathbb{F}$.*

DIMOSTRAZIONE. Fattorizziamo $|d|$ come $p_1 p_2 \cdots p_k$ e poniamo $n = 4|d|$. Sia $\mathbb{F}$ la n-esima estensione ciclotomica. Se ω_j è una radice p_j-esima primitiva di di 1, è evidente che $\omega_j \in \mathbb{F}$ e quindi $\mathbb{F}$ contiene $\sqrt{p_j}$ o $\sqrt{-p_j}$. Visto che 4 divide n l'elemento i è in $\mathbb{F}$ e dunque $\mathbb{F}$ contiene sia $\sqrt{p_j}$ che $\sqrt{-p_j}$. Allora $\mathbb{F}$ contiene $\sqrt{\pm|d|}$ ed uno di questi è $\sqrt{d}$. Pertanto $\mathbb{K}$ è sottocampo di $\mathbb{F}$. □

Vale la pena osservare che, usando un argomento lievemente più elaborato, si dimostra che è possibile scegliere $n = |\Delta_{\mathbb{F}}|$. Questo migliora lievemente quanto provato nel teorema, nel caso in cui $d \equiv 1 \pmod 4$. Questo teorema è un caso particolare di un risultato assai più generale. Ricordiamo che una estensione si dice *abeliana* se è di Galois ed il suo gruppo di Galois è abeliano.

Teorema 5.2.5 (Kronecker-Weber) *Ogni estensione abeliana di $\mathbb{Q}$ è contenuta in una estensione ciclotomica.*

5.3 Teorema di Fermat per primi regolari

Un primo p si dice *regolare* se p non divide l'ordine del gruppo delle classi della p-esima estensione ciclotomica. Vale il seguente teorema

Teorema 5.3.1 (Kummer 1847) *Se p è un primo regolare l'equazione diofantea $x^p + y^p = z^p$ non ha soluzioni (a, b, c) con $abc \neq 0$.*

La dimostrazione di questo fatto esula dai fini di questo corso, ma vedremo comunque la dimostrazione di quello che viene comunemente detto il *primo caso* del teorema di Kummer. Considereremo sempre estensioni ciclotomiche proprie, ovvero di grado almeno 2 su $\mathbb{Q}$.

Se ω è radice n-esima primitiva ed $\mathbb{F} = \mathbb{Q}[\omega]$, poniamo $\varepsilon = \omega + \overline{\omega} = \omega + \omega^{-1}$. Il sottocampo $\mathbb{F}^+$ è contenuto in $\mathbb{R} \cap \mathbb{F}$ e quindi $|\mathbb{F} : \mathbb{F}^+| \geq 2$. Ma il polinomio $x^2 - \varepsilon x + 1 = (x - \omega)(x - \overline{\omega})$ appartiene ad $\mathbb{F}[\varepsilon][x]$ e allora $|\mathbb{F} : \mathbb{F}^+| = 2$. Ne segue che l'unico sottocampo contenente propriamente $\mathbb{F}^+$ è $\mathbb{F}$. Deduciamo da questo che $\mathbb{F}^+$ è il massimo sottocampo reale di $\mathbb{F}$. Infatti, se $\mathbb{K} \leq \mathbb{R} \cap \mathbb{F}$ e $\mathbb{K}$ non è contenuto in $\mathbb{F}^+$ allora il campo generato da $\mathbb{K}$ ed $\mathbb{F}^+$ contiene strettamente $\mathbb{F}^+$, e deve quindi coincidere con $\mathbb{F}$. D'altra parte, essendo $\mathbb{K}$ ed $\mathbb{F}^+$ sottocampi di $\mathbb{R}$ il campo da loro generato è anch'esso contenuto in $\mathbb{R}$, una contraddizione. In particolare $\mathbb{F}^+ = \mathbb{R} \cap \mathbb{F}$.

Lemma 5.3.2 *Siano $n = 2^k m$ un numero naturale dove m è dispari ed $\mathbb{F}$ è la n-esima estensione ciclotomica. Posto G il gruppo delle radici dell'unità contenute in $\mathbb{F}$ si ha*

1. *se $k = 0$, G è ciclico di ordine $2n$, generato da $-\omega$;*
2. *se $k \geq 1$, G è ciclico di ordine n generato da ω.*

DIMOSTRAZIONE. In ogni caso G è un gruppo ciclico generato da una radice di 1, diciamola ω. Se l è l'ordine di ω abbiamo che n divide l visto che $\mathbb{F}$ contiene radici n-esime primitive. Si deve inoltre avere $\varphi(l) = \varphi(n)$. Se $k = 0$ l'unica possibilità è $l = 2m$. Se invece n è pari si verifica immediatamente, usando la formula che esprime $\varphi(n)$ in termini della fattorizzazione di n, che $\varphi(l) > \varphi(n)$ se n divide l propriamente. La tesi segue da queste due osservazioni. □

Lemma 5.3.3 *Sia a un intero algebrico tale che, per ogni zero z del suo polinomio minimo su $\mathbb{Q}$, si abbia $\|z\| = 1$. Allora a è una radice di 1.*

DIMOSTRAZIONE. Osserviamo che, se $\sigma_1, \ldots, \sigma_n$ sono le immersioni di $\mathbb{Q}[a]$ e $a_i = \sigma_i(a)$, il polinomio minimo di a è $f = \prod_{i=1}^{n}(x - a_i) = \sum_{i=0}^{n-1} b_i x^i + x^n$. Dato che a è un intero algebrico tutti i b_i sono interi. Lo stesso argomento usato nella dimostrazione del Teorema 2.5.1 mostra che esiste un intero M, dipendente solo da n, tale che $|b_i| \leq M$ per ogni i. Il polinomio f appartiene allora all'insieme finito

$$\Omega = \left\{ \sum_{i=0}^{n} c_i x^i \mid |c_i| \leq M \,\forall\, i \right\}.$$

Consideriamo ora una qualsiasi potenza a^k. Abbiamo ancora un intero algebrico appartenente a $\mathbb{Q}[a]$ e quindi il suo polinomio minimo ha grado limitato da n. Inoltre gli zeri di tale polinomio sono immagini di a^k tramite le immersioni di $\mathbb{Q}[a^k]$ che, a loro volta, sono restrizioni delle immersioni di $\mathbb{Q}[a]$. Di conseguenza la loro norma è 1 e possiamo applicare il ragionamento precedente per dedurre che il polinomio minimo di ciascun elemento a^k appartiene ad Ω. Allora

$$\{\, a^k \mid k \in \mathbb{N} \,\} \subseteq Z = \{\, z \mid g(z) = 0 \text{ per qualche } g \in \Omega \,\}$$

Ma Z è finito quindi esistono $k > m$ tali che $a^k = a^m$. Semplificando per a^m otteniamo $a^{k-m} = 1$, provando che a è una radice di 1. □

Se $\mathbb{F}$ è la n-esima estensione ciclotomica, tutte le sue immersioni sono complesse e quindi il gruppo U delle unità di $\mathcal{O}_{\mathbb{F}}$ è isomorfo a $C \oplus \mathbb{Z}^{\frac{\varphi(n)}{2}-1}$ dove C è ciclico di ordine n o $2n$.

Il sottocampo $\mathbb{F}^+$ è una estensione normale di $\mathbb{Q}$ (vedi Corollario 5.1.7) e quindi le sue immersioni sono automorfismi e si ottengono come restrizioni degli automorfismi di $\mathbb{F}$. Pertanto tutte le sue immersioni sono reali ed il gruppo U^+ (gli elementi invertibili di $\mathcal{O}_{\mathbb{F}^+}$) è isomorfo a $C_2 \oplus \mathbb{Z}^{\frac{\varphi(n)}{2}-1}$.

Evidentemente U^+ è sottogruppo di U e la prossima proposizione descrive in modo preciso quale sia il legame tra gli elementi di questi due gruppi, nel caso in cui n sia potenza di un primo dispari.

Proposizione 5.3.4 *Siano $n = p^k$ con p un primo dispari ed $\mathbb{F} = \mathbb{Q}[\omega]$ con ω radice n-esima primitiva di 1. Se $\alpha \in U$ esistono $m \in \mathbb{Z}$ ed $u \in U^+$ tali che $\alpha = \omega^m u$.*

DIMOSTRAZIONE. L'elemento $a = \alpha/\overline{\alpha}$ appartiene ad U e $\|a\| = 1$. Il coniugio di $\mathbb{C}$ si restringe ad un automorfismo τ di $\mathbb{F}$ e, visto che il gruppo di Galois dell'estensione è abeliano, per ogni

suo elemento σ e per ogni $a \in \mathbb{F}$, abbiamo

$$\sigma(\overline{a}) = \sigma(\tau(a)) = (\sigma\tau)(a) = (\tau\sigma(a)) = \tau(\sigma(a)) = \overline{\sigma(a)}.$$

Di conseguenza $\sigma(a) = \sigma(\alpha)/\overline{\sigma(\alpha)}$ e dunque $\|\sigma(a)\| = 1$. Possiamo applicare i lemmi 5.3.3 e 5.3.2 per dedurre che $\alpha = \pm\omega^l\,\overline{\alpha}$ per qualche intero l. Supponiamo, per assurdo, che valga $\alpha = -\omega^l\,\overline{\alpha}$. Se consideriamo questa uguaglianza modulo $\pi = 1 - \omega$, otteniamo $\alpha \equiv -\overline{\alpha} \pmod{\pi}$. Dato che $\alpha \in \mathbb{Z}[\omega]$ possiamo anche scrivere $\alpha = \sum_{i=0}^{\varphi(n)-1} a_i\omega^i$ e quindi $\alpha \equiv \sum_{i=0}^{\varphi(n)-1} a_i \pmod{\pi}$. L'ideale (π) può essere generato da un qualsiasi elemento $1 - \omega^i$ e, in particolare $(\pi) = (1 - \omega^{-1})) = (\overline{\pi})$. Possiamo allora applicar eil coniugio alla relazione appena trovate per ottenere

$$\overline{\alpha} \equiv \sum_{i=0}^{\varphi(n)-1} a_i \pmod{\pi}$$

da cui segue $\alpha \equiv \overline{\alpha} \pmod{\pi}$. Da queste relazioni si ottiene $2\alpha \equiv 0 \pmod{\pi}$ e dunque (π) divide l'ideale $(2\alpha) = (2)$. Sappiamo però (vedi Proposizione 5.0.1) che (π) è l'unico fattore primo di (p) e quindi non può dividere (2). Pertanto $\alpha = \omega^l\,\overline{\alpha}$. L'elevamento al quadrato è un automorfismo del gruppo $\langle\omega\rangle$ e quindi anche ω^l si può scrivere come $(\omega^m)^2 = \omega^{2m}$. Poniamo $u = \omega^m\,\overline{\alpha}$. Dato che $\alpha = \omega^k u$ ci resta solo da provare che $u \in U^+$ e per farlo ci basterà osservare che u coincide col suo coniugato. Infatti

$$\overline{u} = \overline{\omega^m\,\overline{\alpha}} = \overline{\omega^m}\,\alpha = \omega^{-m}\,\alpha = \omega^{-m}\,\omega^{2m}\,\overline{\alpha} = \omega^{2m}\,\overline{\alpha} = u$$

concludendo la dimostrazione. □

Lemma 5.3.5 *Siano p un primo ed ω una radice p-esima primitiva. Allora per ogni $\delta \in \mathbb{Z}[\omega]$ si ha $\delta^p \in \mathbb{Z} + p\mathbb{Z}[\omega]$.*

Dimostrazione. L'anello $\mathbb{Z}[\omega]/(p)$ ha caratteristica p, quindi elevare alla p è un morfismo. Se $\delta = \sum_{i=0}^{p-2} a_i\omega^i$ abbiamo

$$(\delta + (p))^p = \left(\sum_{i=0}^{p-2} a_i\omega^i + (p)\right)^p = \sum_{i=0}^{p-2} {a_i}^p\omega^{ip} + (p) = \sum_{i=0}^{p-2} {a_i}^p + (p)$$

e quindi $\delta^p \in \mathbb{Z} + p\mathbb{Z}[\omega]$. □

Possiamo ora dimostrare il primo caso del Teorema di Kummer.

Teorema 5.3.6 *Sia p un primo regolare. Allora l'equazione diofantea $x^p + y^p = z^p$ non ha soluzioni (a, b, c) con $p \nmid abc$.*

Dimostrazione. È preferibile considerare l'equazione $x^p + y^p + z^p = 0$, che presenta una simmetria che può essere sfruttata nella dimostrazione. Chiaramente il nostro teorema è vero se e solo se questa equazione non ha soluzioni (a, b, c) con $p \nmid abc$. Dimostreremo il teorema per assurdo assumendo l'esistenza di una tale soluzione (a, b, c). Dividendo, se necessario, per i

fattori comuni, possiamo anche supporre $MCD(a,b,c)=1$. Notiamo che questa ipotesi implica che a, b e c sono *a due a due* coprimi.

Sia ω una radice p-esima primitiva di 1 e lavoriamo in $\mathbb{Z}[\omega]$, l'anello degli interi di $\mathbb{F}=\mathbb{Q}[\omega]$. L'ipotesi che p sia regolare dice che, se G è il gruppo delle classi di $\mathbb{F}$, p non divide il suo ordine. In particolare G non possiede elementi non banali di ordine p. In $\mathbb{Z}[\omega]$ possiamo scrivere

$$a^p+b^p=\prod_{i=0}^{p-1}(a+\omega^i b)$$

e questo prodotto è uguale a $-c^p$. Passando agli ideali abbiamo l'uguaglianza

$$\prod_{i=0}^{p-1}(a+\omega^i b)=(c)^p$$

e mostreremo che, se $i\neq j$, i due ideali $(a+\omega^i b)$ e $(a+\omega^j b)$ sono coprimi. Intanto osserviamo che ogni primo che divide uno di questi fattori divide anche l'ideale (c). Se ci fosse un primo $\mathcal{P}$ che li divise entrambi, questo ne dividerebbe la somma e quindi l'elemento $\omega^i b-\omega^j b=(a+\omega^i b)-(a+\omega^j b)$ apparterrebbe a $\mathcal{P}$. Dato che ω^i è un invertibile, anche $b-\omega^{j-i}b=b(1-\omega^{j-i})$ sarebbe in $\mathcal{P}$. L'ideale $\mathcal{P}$ è primo e, visto che divide $(b(1-\omega^{j-i}))=(b)(1-\omega^{j-i})$, ne divide uno dei fattori. Se $\mathcal{P}$ divide (b) otteniamo una contraddizione osservando che $\mathcal{P}$ contiene $(b)+(c)$ e quest'ultimo ideale è $\mathbb{Z}[\omega]$ essendo b e c interi coprimi. Allora $\mathcal{P}$ divide $(1-\omega^{j-i})$ che, per la Proposizione 5.0.1 è primo. Ne segue $\mathcal{P}=(1-\omega)=(\pi)$. Ma se (π) divide $(c)^p$ otteniamo, considerando le norme, $p|c^{p(p-1)}$, e da questo si ricava che p divide c, una contraddizione. Il fatto che i fattori $(a+\omega^i b)$ siano a due a due coprimi, assieme all'unicità della fattorizzazione, ci assicura che ciascuno di questi è una potenza p-esima. Scriviamo $(a+\omega^i b)=\mathcal{A}_i{}^p$ e osserviamo che, passando alle classi in G, queste equazioni diventano

$$1=[(a+\omega^i b)]=[\mathcal{A}_i{}^p]=[\mathcal{A}_i]^p.$$

Abbiamo osservato in precedenza che G non ha elementi di ordine p e questo implica $[\mathcal{A}_i]=1$, ovvero tutti gli ideali $\mathcal{A}_i$ sono principali. Concentriamo la nostra attenzione su $\mathcal{A}_1$ e scriviamo $(a+b\omega)=(\delta)^p=(\delta^p)$. C'è quindi una unità $\alpha\in\mathbb{Z}[\omega]$ tale che $a+\omega b=\alpha\delta^p$. Usando la Proposizione 5.3.4 possiamo trovare elemento u nel gruppo delle unità di $\mathcal{O}_{\mathbb{F}^+}$ per cui $a+\omega b=\omega^m u\delta^p$ per un opportuno intero m. Il Lemma 5.3.5 ci assicura l'esistenza di un intero a tale che $\delta^p\equiv a \pmod p$, per cui

$$a+\omega b\equiv ua\omega^m \pmod p.$$

Moltiplicando per ω^{-m} (che è invertibile) si ottiene

$$\omega^{-m}(a+\omega b)\equiv ua \pmod p$$

e coniugando

$$\omega^m(a+\omega^{-1}b)\equiv ua \pmod p.$$

Da queste due congruenze ricaviamo

$$\omega^{-m}a + \omega^{1-m}b - \omega^m a - \omega^{m-1}b \equiv 0 \pmod{p}.$$

Se p divide m questa congruenza diventa

$$\omega b - \omega^{-1}b = b\omega^{-1}(\omega^2 - 1) = b\omega^{-1}(1+\omega)(\omega - 1) \equiv 0 \pmod{p}.$$

e ricaviamo, usando il fatto che $\omega^{-1}(1+\omega)$ è invertibile, $b(1-\omega) \equiv 0 \pmod{p}$. Tornando agli ideali abbiamo $(p) = (1-\omega)^{p-1} \mid (b)(1-\omega)$ e da questo $(1-\omega)^{p-2} \mid (b)$. Prendendo le norme otteniamo $N((1-\omega)^{p-2}) = p^{p-2} \mid N(b) = b^{p-1}$ e questa è una contraddizione. Allo stesso modo si prova che $m - 1 \not\equiv 0 \pmod{p}$. La congruenza trovata equivale all'uguaglianza $\omega^{-m}a + \omega^{1-m}b - \omega^m a - \omega^{m-1}b = p\beta$dove $\beta \in \mathbb{Z}[\omega]$ è un opportuno elemento. Vediamo che gli esponenti $\pm m, \pm(1-m)$ non sono divisibili per p. Se gli elementi $\omega^{-m}, \omega^{1-m}, \omega^{m-1}, \omega^{m-1}$ sono tutti distinti, allora $p \geq 5$ perché $\pm m, \pm(m-1)$ rappresentano quattro classi di congruenza modulo p, nessuna delle quali è 0. Sfruttiamo il fatto che ogni sottoinsieme proprio di $\{1, \omega, \ldots, \omega^{p-1}\}$ è indipendente su $\mathbb{Z}$, per dedurre che anche gli elementi $\omega^{-m}, \omega^{1-m}, \omega^{m-1}, \omega^{m-1}$ sono indipendenti su $\mathbb{Z}$. Poiché β si scrive come

$$\beta = \frac{a}{p}\omega^{-m} + \frac{b}{p}\omega^{1-m} - \frac{a}{p}\omega^m - \frac{b}{p}\omega^{m-1}$$

allora a/p e b/p devono essere interi, contraddicendo l'ipotesi che p non divida abc. Pertanto almeno due degli interi $\pm m, \pm(1-m)$ devono essere congrui modulo p. Se $m \not\equiv -m \pmod{p}$ otteniamo $p \mid 2m$ e quindi $p \mid m$, eventualità che abbiamo escluso. Allo stesso modo vediamo che $(m-1) \not\equiv -(m-1) \pmod{p}$. Rimane come unica possibilità $m \equiv -(m-1) \pmod{p}$, ovvero $2m \equiv 1 \pmod{p}$. Moltiplicando per ω^m otteniamo

$$\omega^m p\beta = a + \omega b - \omega^{2m}a - \omega^{2m-1}b = a + \omega b - \omega a - b = (1-\omega)(a-b)$$

e prendendo gli ideali

$$(p\beta) = (p)(\beta) = (1-\omega)(a-b).$$

Passando alle norme si ottiene che p^{p-1} divide $(a-b)^{p-1}p$ da cui segue che p divide $a-b$, per cui $a \equiv b \pmod{p}$. Usando la simmetria dell'equazione $x^p + y^p + z^p = 0$ si ottiene anche $a \equiv c \pmod{p}$, e da questo si ricava

$$0 = a^p + b^p + c^p \equiv 3a^p \pmod{p}.$$

Allora $p \mid 3a^p$ e pertanto $p = 3$. Osserviamo che gli unici cubi modulo 9 sono $-1, 0, 1$ e quindi $a^3 + b^3 + c^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{9}$, perché nelle nostre ipotesi a^3, b^3, c^3 non possono essere congrui a 0. Ma per nessuna scelta dei segni la quantità $\pm 1 \pm 1 \pm 1$ è congrua a 0 modulo 9. Questa contraddizione conclude la dimostrazione del teorema. □

5.4 Due teoremi sui discriminanti

In questa sezione dimostriamo due teoremi sui discriminanti che, pur non essendo rilevanti per il seguito della trattazione, sono di notevole interesse. Il primo di questi è noto come *Teorema di Stickelberger*.

Teorema 5.4.1 *Se $\mathbb{F}$ è un campo di numeri allora $\Delta_{\mathbb{F}} \equiv 0, 1 \pmod 4$.*

DIMOSTRAZIONE. Se n è il grado di $\mathbb{F}$ fissiamo $\sigma_1, \ldots, \sigma_n$ le immersioni di $\mathbb{F}$ ed una base $a_1, \ldots, a_n$ per $\mathcal{O}_{\mathbb{F}}$. Se $A = (\sigma_i(a_j))$ abbiamo $\Delta_{\mathbb{F}} = \det(A)^2$. Usiamo la formula di Laplace per il determinante e otteniamo

$$\det(A) = \sum_{\pi \in S_n} sgn(\pi) \prod_{i=1}^{n} \sigma_i(a_{\pi(i)}).$$

Se $\mathbb{F} = \mathbb{Q}[a]$ prendiamo $\mathbb{K}$ il campo di spezzamento (in $\mathbb{C}$) f il polinomio minimo di a, in modo che $\mathbb{K}|\mathbb{Q}$ è di Galois con gruppo di Galois G. Dato che ciascuna immersione σ_i ha immagine in $\mathbb{K}$ ($\sigma_i(a)$ è sempre uno zero di f), per ogni $\tau \in G$ possiamo considerare la funzione $\tau sigma_i$, e questa è ancora un'immersione di $\mathbb{F}$. Inoltre, se $\tau\sigma_i = \tau sigma_j$, ricaviamo facilmente, usando il fatto che τ ha un'inversa in G, che $\sigma_i = \sigma_j$. Di conseguenza tutte le immersioni di $\mathbb{F}$ si ottengono in questo modo. Pertanto, per ogni i esiste un unico j tale che $\tau\sigma_i = \sigma_j$. Per quanto detto la funzione ε che ad i associa l'unico indice j per cui $\tau\sigma_i = \sigma_j$, è un elemento di S_n. Applicando τ ad uno degli addendi nell'espansione di Laplace del determinante di M otteniamo

$$\tau\left(sgn(\pi)\prod_{i=1}^{n}\sigma_i(a_{\pi(i)})\right) = sgn(\pi)\prod_{i=1}^{n}\tau(\sigma_i(a_{\pi(i)})) = sgn(\pi)\prod_{i=1}^{n}\tau\sigma_i(a_{\pi(i)}) =$$
$$sgn(\pi)\prod_{i=1}^{n}\sigma_{\varepsilon(i)}(a_{\pi(i)}) = sgn(\varepsilon)sgn(\pi\varepsilon^{-1})\prod_{i=1}^{n}\sigma_i(a_{\pi\varepsilon^{-1}(i)}) = sgn(\varepsilon)sgn(\eta)\prod_{i=1}^{n}\sigma_i(a_{\eta(i)})$$

se $\eta = \pi\varepsilon^{-1}$.

Poniamo

$$P = \sum_{\pi \in A_n} sgn(\pi)\prod_{i=1}^{n}\sigma_i(a_{\pi(i)}) \quad \text{e} \quad -D = \sum_{\pi \notin A_n} sgn(\pi)\prod_{i=1}^{n}\sigma_i(a_{\pi(i)})$$

Supponiamo $\varepsilon \notin A_n$. Si ha

$$\tau(-D) = \sum_{\pi \notin A_n}\tau\left(sgn(\pi)\prod_{i=1}^{n}\sigma_i(a_{\pi(i)})\right) = sgn(\varepsilon)\sum_{\pi \notin A_n} sgn(\pi\varepsilon^{-1})\prod_{i=1}^{n}\sigma_i(a_{\pi\varepsilon^{-1}(i)}) =$$
$$sgn(\varepsilon)\sum_{\eta \in A_n} sgn(\eta)\prod_{i=1}^{n}\sigma_i(a_{eta(i)}) = -P$$

e quindi $\tau(D) = P$. Analogamente si prova che $\tau(P) = D$ e, se $\varepsilon \in A_n$, τ fissa P e D. Di conseguenza τ fissa $P + D$ e PD. Dato che questo accade per ogni elemento di G ne deduciamo che $P + D$ e PD sono razionali. Inoltre, essendo interi algebrici, devono essere in $\mathbb{Z}$. Allora

$$\Delta_{\mathbb{F}} = (P - D)^2 = (P + D)^2 + 4PD \equiv (P + D)^2 \pmod 4.$$

Dato che gli unici quadrati modulo 4 sono 0 e 1, il teorema è dimostrato. □

Il prossimo teorema che intendiamo dimostrare, ci darà una formula per il calcolo del discriminante di una qualsiasi estensione ciclotomica. Osserviamo che, se $\mathbb{F}_n$ indica l'estensione di $\mathbb{Q}$ con una radice n-esima primitiva di 1, si ha $\mathbb{F}_{2m} = \mathbb{F}_m$ ogni volta che m è dispari. Pertanto sarà sufficiente studiare estensioni $\mathbb{F}_n$ dove n non è congruo a 2 modulo 4. È necessario definire il *prodotto di Kronecker* tra matrici ed evidenziarne una sua proprietà .

Siano $\mathbb{F}$ un campo e A, B due matrici quadrate a coefficienti in $\mathbb{F}$ di dimensioni rispettivamente n ed m. Se $A = (a_{ij})$ definiamo il prodotto di Kronecker $A \otimes B$ come

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & a_{n2}B \dots & a_{nn}B \end{pmatrix}.$$

Useremo il fatto che $\det(A \otimes B) = (\det(A))^m (\det(B))^n$.

Teorema 5.4.2 *Siano ω una radice n-esima primitiva di 1 ed $\mathbb{F} = \mathbb{Q}[\omega]$. Se $n \geq 3$ ed $n \not\equiv 2 \pmod 4$ allora*

$$\Delta_{\mathbb{F}} = (-1)^{\varphi(n)/2} n^{\varphi(n)} \prod_{\substack{p \mid n \\ p \text{ primo}}} p^{-\frac{\varphi(n)}{p-1}}.$$

Dimostrazione. La Proposizione 5.1.4 mostra che il teorema è vero se $n = p^k$ per qualche primo p. Lavoriamo allora per induzione su n e supponiamo il risultato vero per ogni intero minore di n. Se n è potenza di un primo si usa la Proposizione 5.1.4 e si conclude. Supponiamo dunque che n si possa scrivere come $n = lm$ con $(l, m) = 1$ ed $l, m < n$. Definiamo $\varepsilon = \omega^l$, $\zeta = \omega^m$ e poniamo $\mathbb{K} = \mathbb{Q}[\varepsilon]$, $\mathbb{L} = \mathbb{Q}[\zeta]$. Siano $\sigma_1, \dots, \sigma_{\varphi(m)}$ le immersioni di $\mathbb{K}$ mentre indichiamo con $\tau_1, \dots, \tau_{\varphi(l)}$ quelle di $\mathbb{L}$. La dimostrazione del Lemma 5.2.1 mostra che $\mathbb{Z}[\omega] = \mathbb{Z}[\varepsilon]\mathbb{Z}[\zeta]$ e quindi, se scegliamo $\{ a_1, \dots, a_{\varphi(m)} \}$ e $\{ b_1, \dots, b_{\varphi(l)} \}$ basi rispettivamente di $\mathbb{Z}[\varepsilon]$ e $\mathbb{Z}[\zeta]$, l'insieme $\{ a_i b_j \mid i = 1, \dots \varphi(m)\ j = 1, \dots \varphi(l) \}$ è una base per $\mathbb{Z}[\omega]$. Se $M_1 = (\sigma_i(a_r))$ ed $M_2 = (\tau_j(b_s))$ abbiamo $\Delta_{\mathbb{K}} = \det(M_1)^2$, $\Delta_{\mathbb{L}} = \det(M_2)^2$. Se η è una immersione di $\mathbb{F}$ allora le sue restrizioni a $\mathbb{K}$ ed $\mathbb{L}$ sono immersioni σ_i, τ_j. Viceversa, visto che $|\mathbb{F} : \mathbb{Q}| = |\mathbb{K} : \mathbb{Q}|\ |\mathbb{L} : \mathbb{Q}|$ per ogni coppia σ_i, τ_j esiste un'unica immersione η di $\mathbb{F}$ tale che $\eta_{|\mathbb{K}} = \sigma_i$ e $\eta_{|\mathbb{L}} = \tau_j$. Indichiamo questa immersione con η_{ij}. Se M è la matrice $M = (\eta_{ij}(a_r b_s))$ (righe e colonne sono indiciate da coppie di indici) allora $\Delta_{\mathbb{F}} = \det(M)^2$. Dato che

$$\eta_{ij}(a_r b_s) = \eta_{ij}(a_r)\eta_{ij}(b_s) = \sigma_i(a_r)\tau_j(b_s)$$

abbiamo che la matrice M si ottiene da $M_1 \otimes M_2$ permutando opportunamente righe e colonne. Di conseguenza

$$\det(M) = \pm \det(M_1 \otimes M_2) = \pm (\det(M_1))^{\varphi(l)} (\det(M_2))^{\varphi(m)}$$

e quindi

$$\Delta_{\mathbb{F}} = (\Delta_{\mathbb{K}})^{\varphi(l)} (\Delta_{\mathbb{L}})^{\varphi(m)}.$$

L'ipotesi induttiva ci permette quindi di scrivere

$$\Delta_{\mathbb{F}} = \left((-1)^{\varphi(m)/2} n^{\varphi(m)} \prod_{\substack{p|m \\ p \text{ primo}}} p^{-\frac{\varphi(m)}{p-1}}\right)^{\varphi(l)} \left((-1)^{\varphi(l)/2} n^{\varphi(l)} \prod_{\substack{p|l \\ p \text{ primo}}} p^{-\frac{\varphi(l)}{p-1}}\right)^{\varphi(m)}.$$

Osservando che $\varphi(l)\varphi(m) = \varphi(n)$ e che, se un primo p divide n, allora divide solo uno tra l ed m, otteniamo

$$\Delta_{\mathbb{F}} = (-1)^{\varphi(n)} n^{\varphi(n)} \prod_{\substack{p|n \\ p \text{ primo}}} p^{-\frac{\varphi(n)}{p-1}}.$$

Ricordiamo che $\varphi(u)$ è dispari se e solo se $u = 2$ e quindi, nel nostro caso $\varphi(n) = \varphi(l)\varphi(m)$ è multiplo di 4. Pertanto $(-1)^{\varphi(n)} = (-1)^{\varphi(n)/2}$ e quindi

$$\Delta_{\mathbb{F}} = (-1)^{\varphi(n)/2} n^{\varphi(n)} \prod_{\substack{p|n \\ p \text{ primo}}} p^{-\frac{\varphi(n)}{p-1}}$$

come richiesto. □

Capitolo 6

La funzione zeta di Dedekind e la *Class number formula*

In questo capitolo introdurremo alcuni strumenti analitici che risultano di enorme utilità nello studio dei campi di numeri. In particolare discuteremo la *funzione zeta di Dedekind* di un campo di numeri e la utilizzeremo per trovare una formula che esprime, nel caso di estensioni abeliane di $\mathbb{Q}$, l'ordine del gruppo delle classi. La trattazione segue, nella sostanza, quella del capitolo 7 di [5], aggiungendo però alcuni dettagli alle dimostrazioni. Il lettore potrebbe trovare utile anche il capitolo VI di [10].

6.1 Serie di Dirichlet

In questa sezione richiameremo alcuni risultati sulla convergenza di serie e prodotti infiniti. Le proprietà fondamentali di cui faremo uso si possono trovare in qualsiasi testo di analisi complessa (ad esempio [1]).

Definizione 6.1.1 *Siano* $\{ a_n \mid n \in \mathbb{N}^* \}$ *una successione di numeri reali ed* s *una variabile complessa. La serie*

$$\sum_{n \in \mathbb{N}^*} \frac{a_n}{n^s}$$

si dice una serie di Dirichlet (ordinaria).

Un esempio di serie di Dirichlet è la funzione zeta di Riemann

$$\zeta(s) = \sum_{n \in \mathbb{N}^*} \frac{1}{n^s}.$$

Per ogni numero reale r poniamo $S(r) = \{ s \mid \mathrm{Re}(s) > r \} \subseteq \mathbb{C}$. Il prossimo lemma è di fondamentale importanza.

Lemma 6.1.2 *Sia* $\{ a_n \mid n \in \mathbb{N}^* \}$ *una successione reale e supponiamo che la funzione* $A(t) = \sum_{n \le t} a_n$ *sia* $O(t^r)$ *per qualche* $r > 0$. *Allora la serie di Dirichlet* $f(s) = \sum_{n \in \mathbb{N}^*} a_n n^{-s}$ *converge, nel semipiano* $S(r)$, *ad una funzione olomorfa.*

Dimostrazione. Basterà dimostrare che $f(s)$ converge uniformemente su ogni compatto di $S(r)$. Dato che la natura della serie non cambia se omettiamo un numero finito di termini, possiamo assumere che, per un opportuno $B > 0$, si abbia $A(t) \le Bt^r$ per ogni $t \in \mathbb{R}^+$. Fissati due naturali $m < M$ mostriamo che $\sum_{n=m}^{M} \frac{a_n}{n}^{-s}$ è infinitesima al crescere di m ed M. Scrivendo $a_n = A(n) - A(n-1)$ abbiamo

$$\sum_{n=m}^{M} \frac{a_n}{n^s} = \sum_{n=m}^{M} \frac{A(n)}{n^s} - \sum_{n=m}^{M} \frac{A(n-1)}{n^s} = \frac{A(M)}{M^s} - \frac{A(m-1)}{m^s} + \sum_{n=m}^{M-1} A(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right).$$

Sfruttando l'ipotesi sulla funzione $A(t)$ otteniamo

$$\left|\sum_{n=m}^{M} \frac{a_n}{n^s}\right| \le B\left(\frac{M^r}{|M^s|} + \frac{(m-1)^r}{|m^s|} + \sum_{n=m}^{M-1} n^r \left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right|\right).$$

Indicando con x la parte reale di s e sfruttando l'uguaglianza

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} = s\int_n^{n+1} \frac{1}{t^{s+1}} dt$$

ricaviamo

$$\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \le |s| \int_n^{n+1} \frac{1}{|t^{s+1}|} dt = |s| \int_n^{n+1} \frac{1}{t^{x+1}} dt \le \frac{|s|}{n^{x+1}}.$$

Questa disuguaglianza ci permette di ottenere la maggiorazione

$$\left|\sum_{n=m}^{M} \frac{a_n}{n^s}\right| \le B\left(M^{r-x} + m^{r-x} + |s| \sum_{n=m}^{M-1} n^{r-x-1}\right)$$

Fissiamo un compatto C contenuto in $S(r)$. Esistono numeri reali positivi ε e K tali che

- $|s| \le K$ per ogni $s \in C$ e
- $\mathrm{Re}(s) - r \ge \varepsilon$ per ogni $s \in C$.

e questo ci permette di ottenere

$$\left|\sum_{n=m}^{M} \frac{a_n}{n^s}\right| \le B\left(\frac{1}{M^\varepsilon} + \frac{1}{m^\varepsilon} + K \sum_{n=m}^{M-1} \frac{1}{n^{1+\varepsilon}}\right) \le B\left(\frac{2}{m^\varepsilon} + K \sum_{n=m}^{M-1} \frac{1}{n^{1+\varepsilon}}\right).$$

Usiamo ora il fatto che

$$\sum_{n=m}^{M-1} \frac{1}{n^{1+\varepsilon}} \le \int_{m-1}^{\infty} \frac{1}{t^{1+\varepsilon}} dt = \frac{1}{\varepsilon(m-1)^{1+\varepsilon}}$$

per scrivere

$$\left|\sum_{n=m}^{M}\frac{a_n}{n^s}\right| \leq B\left(\frac{2}{m^\varepsilon}+\frac{K}{\varepsilon(m-1)^{1+\varepsilon}}\right) = R(C,m).$$

La costante $R(C,m)$ dipende solo dal compatto C e da m e, se m ed M tendono ad infinito, $R(C,m)$ tende a 0. Questo prova che $f(s)$ converge uniformemente sui compatti di $R(s)$ e quindi il suo limite è una funzione olomorfa su $S(r)$. □

Una conseguenza di questo lemma è che la funzione zeta di Riemann $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ è olomorfa nel semipiano $S(1)$. Vedremo adesso che la zeta di Riemann ammette una estensione meromorfa ad $S(0)$ con un solo polo di ordine 1 nel punto $s = 1$.

Definiamo $f(s) = -\sum_{n=1}^{\infty}\frac{(-1)^n}{n^s}$. Il Lemma 6.1.2 ci assicura che $f(s)$ è olomorfa in $S(0)$. Abbiamo

$$\zeta(s)(1-2^{1-s}) = \sum_{n=1}^{\infty}\frac{1}{n^s} - \sum_{n=1}^{\infty}\frac{2}{(2n)^s} = \sum_{n=1}^{\infty}\frac{1}{n^s} - \sum_{n\text{ pari}}\frac{2}{n^s} = \sum_{n=1}^{\infty} = \frac{(-1)^{n+1}}{n^s} = f(s).$$

La funzione $1-2^{1-s}$ si annulla nell'insieme $\mathcal{Z} = \{\, s_k = 1 + 2k\pi i/\ln(2) \mid k \in \mathbb{Z}\,\}$ e

$$\frac{f(s)}{1-2^{1-s}}.$$

è olomorfa in $S(0)\setminus\mathcal{Z}$. Nel punto 1 la funzione $\frac{f(s)}{1-2^{1-s}}$ ha un polo di ordine 1, perché f è definita in 1 mentre $(1-s)/1-2^{1-s}$ ha limite finito al tendere di s ad 1. Per vedere che negli altri punti di $\mathcal{Z}$ la funzione $f(s)/(1-2^{1-s})$ è definita, usiamo un argomento indiretto. Poniamo

$$a_n = \begin{cases} 1 & \text{se } n \equiv 1,2 \pmod 3 \\ -2 & \text{se } n \equiv 0 \pmod 3 \end{cases}$$

e

$$g(s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s}.$$

Analogamente a quanto fatto prima si controlla che $g(s) = \zeta(s)(1-3^{1-s})$. L'unico zero comune a $1-2^{1-s}$ e $1-3^{1-s}$ e il punto $s = 1$. Fissiamo un $s_k \neq 1$ ed un suo intorno destro U che non contenga zeri di $1-3^{1-s}$. In $U\setminus\{s_k\}$ la funzione $\zeta(s)$ è definita dalla sua serie di Dirichlet, ed abbiamo

$$\zeta(s) = \frac{f(s)}{1-2^{1-s}} = \frac{g(s)}{1-3^{1-s}} \quad \text{per ogni } s \in U\setminus\{s_k\}.$$

Allora

$$\lim_{s\to {s_k}^+}\frac{f(s)}{1-2^{1-s}} = \lim_{s\to {s_k}^+}\frac{g(s)}{1-3^{1-s}}$$

è finito perché $1-3^{1-s}$ non ha zeri in prossimità di s_k. Se $\frac{f(s)}{1-2^{1-s}}$ avesse un polo in s_k (o una singolarità non eliminabile), il limite destro non sarebbe finito. Ne deduciamo che $\frac{f(s)}{1-2^{1-s}}$ è meromorfa in $S(0)\setminus\{1\}$ e definiamo una estensione di $\zeta(s)$ ponendo

$$\zeta(s) = \frac{f(s)}{1-2^{1-s}} \quad \text{per ogni } s \in S(0)\setminus\{1\}.$$

Dovendo discutere la convergenza di prodotti infiniti, è utile il seguente lemma. Per enunciarlo è bene definire gli insiemi

$$\mathcal{N} = \{r \in \mathbb{N}^{\mathbb{N}} \mid r(i) = 0 \text{ eccetto che per un numero finito di indici } i\}$$

e, per ogni $m \in \mathbb{N}$,

$$\mathcal{N}(m) = \mathbb{N}^{\{0,1,\dots,m\}}.$$

Lemma 6.1.3 *Sia $\{a_0, a_1, \dots\}$ una successione di numeri complessi con $|a_n| < 1$ per ogni n e tali che $\sum_{n=0}^{\infty} |a_n| < \infty$. Allora $\prod_{n=0}^{\infty}(1 - a_n)$ converge assolutamente ad un numero complesso diverso da 0 e*

$$\prod_{n=0}^{\infty}(1 - a_n)^{-1} = \sum_{r \in \mathcal{N}} a(r)$$

dove $a(r) = \prod_{n=0}^{\infty} {a_i}^{r(i)}$. La convergenza è assoluta e quindi l'ordine dei fattori è ininfluente.

Dimostrazione Le nostre ipotesi implicano che $\prod_{n=0}^{\infty}(1 - a_n)$ converge assolutamente ad un limite diverso da 0, e che l'ordine dei fattori è ininfluente (vedi [1] pag. 189-191). Fissato m vale l'uguaglianza

$$\prod_{n=0}^{m}(1 - a_n)^{-1} = \sum_{r \in \mathcal{N}(m)} \prod_{i=0}^{m} {a_i}^{r(i)}$$

ottenuta osservando che $(1 - a_n)^{-1} = \sum_{i=0}^{\infty} a_n^i$ ed eseguendo il prodotto di Cauchy di queste serie. Per concludere basta notare che il lato sinistro di questa uguaglianza ha come limite $\prod_{n=0}^{\infty}(1 - a_n)^{-1}$ al tendere di m all'infinito, e quindi lo stesso vale per il lato destro che, invece, tende a $\sum_{r \in \mathcal{N}} a(r)$. La convergenza è assoluta visto che è possibile ripetere questo argomento per la successione $\{|a_n| \mid n \in \mathbb{N}\}$. □

Scegliendo la successione a_n in modo particolare, si possono ottenere serie di Dirichlet con proprietà molto utili. Ricordiamo che $f : \mathbb{N} \longrightarrow \mathbb{C}$ si dice *strettamente moltiplicative* se $f(nm) = f(n)f(m)$ per ogni $n, m \in \mathbb{N}$.

Lemma 6.1.4 *Sia f una funzione strettamente moltiplicativa con $|f(n)| \leq 1$ per ogni n. Posto $g(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ abbiamo che $g(s)$ converge assolutamente su $S(1)$ ad una funzione olomorfa e, se $\mathbb{P}$ indica l'insieme dei primi di $\mathbb{N}$, si ha*

$$g(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - f(p)/p^s}.$$

Dimostrazione. Scegliamo una enumerazione $\{p_n \mid n \in \mathbb{N}\}$ per i primi e, fissato $s \in S(1)$, poniamo $a_n = f(p_n)/p_n^s$. Per ogni $n \in \mathbb{N}$ esiste un unico $r \in \mathcal{N}$ tale che $n = \prod_{i=1}^{\infty} {p_i}^{r(i)}$ e quindi

$$\sum_{r \in \mathcal{N}} \prod_{i=0}^{\infty} {a_i}^{r(i)} = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Abbiamo inoltre

$$\sum_{n=0}^{\infty}|a_n| \leq \sum_{n=0}^{\infty}\left|\frac{1}{n^s}\right| = \sum_{n=0}^{\infty}\frac{1}{n^{\mathrm{Re}(s)}} = \zeta(\mathrm{Re}(s)).$$

Il risultato segue ora dal fatto che è possibile applicare il Lemma 6.1.3. □ Se scegliamo come f la funzione costantemente uguale ad 1, otteniamo

$$\zeta(s) = \prod_{p\in\mathbb{P}}\frac{1}{1-\frac{1}{p^s}} \quad \text{su } S(1).$$

Questo tipo di fattorizzazioni si dicono *fattorizzazioni di Eulero*.

6.2 Distribuzione degli ideali

Prima di proseguire è necessario richiamare alcuni risultati, di cui ometteremo la dimostrazione, che riguardano la *distribuzione* degli ideali in un campo di numeri. Servono alcune definizioni. Per la prima ci rifacciamo alla notazione introdotta nella dimostrazione del Teorema 4.1.3.

Definizione 6.2.1 *Siano $\mathbb{F}$ un campo di numeri, diverso da $\mathbb{Q}$ o da una sua estensione quadratica immaginaria, di grado $n = s+2t$ ed $u_1, u_2, \ldots, u_{s+t-1}$ elementi del gruppo delle unità U di $\mathcal{O}_\mathbb{F}$ le cui immagini in $U/T(U)$ sono un insieme libero di generatori. Se M è la matrice le cui colonne sono i vettori $\psi(u_i)$ ed indichiamo con $A_1, A_2, \ldots, A_{s+t}$ le sue righe, abbiamo $\sum_{i=1}^{s+t} A_i = 0$. Quindi, se M_i è la matrice ottenuta da M cancellando la riga A_i, abbiamo $|det(M_i)| = |det(M_j)|$ per ogni scelta di i e j. Questo valore non dipende dagli elementi $u_1, \ldots, u_{s+r-1}$ e viene detto il* regolatore *di $\mathbb{F}$ ed indicato con $R(\mathbb{F})$. Se $\mathbb{F}$ è $\mathbb{Q}$ o una sua estensione quadratica immaginaria, il suo regolatore si pone uguale ad 1.*

Definizione 6.2.2 *Sia $\mathbb{F}$ un campo di numeri di grado $n = s+2t$ ed indichiamo con w l'ordine del gruppo delle radici dell'unità appartenenti a $\mathcal{O}_\mathbb{F}$. Definiamo il numero κ come*

$$\kappa = \frac{2^{s+t}\pi^t R(\mathbb{F})}{w\sqrt{|\Delta_\mathbb{F}|}}.$$

Il prossimo teorema è fondamentale per comprendere il dominio di convergenza di certe serie di Dirichlet. La dimostrazione è omessa ma chi fosse interessato può consultare [5], Teorema 39 e suo corollario.

Teorema 6.2.3 *Sia $\mathbb{F}$ un campo di numeri di grado n. Se $i(t)$ indica il numero di ideali di $\mathcal{O}_\mathbb{F}$ di norma minore o uguale a t, si ha*

$$i(t) = h\kappa t + \varepsilon(t)$$

dove h è l'ordine del gruppo delle classi di $\mathbb{F}$ ed $\varepsilon(t) \in O(t^{1-1/n})$.

6.3 Funzioni zeta di Dedekind

Sia $\mathbb{F}$ un campo e indichiamo con j_n il numero di ideali di $\mathcal{O}_\mathbb{F}$ di norma n. Definiamo la *funzione zeta di Dedekind di* $\mathbb{F}$ come

$$\zeta_\mathbb{F}(s) = \sum_{n=1}^{\infty} \frac{j_n}{n^s}.$$

Il Teorema 6.2.3 ed il Lemma 6.1.2 ci permettono di dire che $\zeta_\mathbb{F}(s)$ è olomorfa in $S(1)$. Anche in questo caso un esempio è fornito dalla zeta di Riemann, in quanto risulta $\zeta(s) = \zeta_\mathbb{Q}(s)$.

Dato che la convergenza in $S(1)$ è assoluta, c'è un altro modo interessante per riscrivere $\zeta_\mathbb{F}(s)$. Indichiamo con $\mathcal{I}$ l'insieme degli ideali non nulli di $\mathcal{O}_\mathbb{F}$. Allora

$$\zeta_\mathbb{F}(s) = \sum_{I \in \mathcal{I}} \frac{1}{N(I)^s}.$$

La convergenza assoluta ci assicura che questa serie non dipende dall'ordine degli addendi. Il vantaggio di questa scrittura è che possiamo ottenere una fattorizzazione di Eulero anche per queste funzioni. Se $x = \mathrm{Re}(s)$ allora $|u^s| = |u|^x$ per ogni numero complesso u quindi, se $s \in S(1)$ e $\mathcal{P}$ indica l'insieme degli ideali primi di $\mathcal{O}_\mathbb{F}$,

$$\sum_{P \in \mathcal{P}} |N(P)^{-s}| = \sum_{P \in \mathcal{P}} |N(P)|^{-x} \leq \sum_{I \in \mathcal{I}} |N(I)|^{-x} = \zeta_\mathbb{F}(x) < +\infty.$$

Applicando i lemmi 6.1.3 e 6.1.4 e otteniamo

Proposizione 6.3.1 *Sia $\mathbb{F}$ un campo di numeri e indichiamo con $\mathcal{P}$ l'insieme degli ideali primi di $\mathcal{O}_\mathbb{F}$. Allora in $S(1)$ si ha la fattorizzazione di Eulero*

$$\zeta_\mathbb{F}(s) = \prod_{P \in \mathcal{P}} \left(1 - \frac{1}{N(P)^s}\right)^{-1}$$

Vediamo ora che, analogamente a quanto fatto per la zeta di Riemann, è possibile definire estensioni meromorfe anche per le funzioni zeta di Dedekind.

Fissato un campo di numeri $\mathbb{F}$ riscriviamo la funzione $\zeta_\mathbb{F}(s)$ come

$$\zeta_\mathbb{F}(s) = \sum_{n=1}^{\infty} \frac{j_n - h\kappa + h\kappa}{n^s} = \sum_{n=1}^{\infty} \frac{j_n - h\kappa}{n^s} + h\kappa\zeta(s)$$

e osserviamo che $A(n) = \sum_{m \leq n}(j_m - h\kappa) = i(n) - h\kappa n = \varepsilon(n) \in O(t^{1-1/|\mathbb{F}:\mathbb{Q}|})$. Ancora il lemma 6.1.2 ci dice che la serie di Dirichlet $\sum_{n=1}^{\infty} \frac{j_n - h\kappa}{n^s}$ converge ad una funzione olomorfa su $S(1 - 1/|\mathbb{F} : \mathbb{Q}|)$. In questo semipiano possiamo usare l'estensione della $\zeta(s)$ descritta in precedenza, ed estendere quindi $\zeta_\mathbb{F}(s)$ ad una funzione meromorfa su $S(1 - 1/|\mathbb{F} : \mathbb{Q}|)$ con un polo di ordine 1 in $s = 1$.

Accade spesso di voler *misurare la densità* di certi insiemi di primi, ma questo concetto è piuttosto vago. Esistono infatti diverse possibili definizioni ed una di queste coinvolge una generalizzazione della funzione zeta di Dedekind.

Se $\mathcal{A}$ è un insieme di ideali primi (non banali) di $\mathcal{O}_\mathbb{F}$, indichiamo con $\mathsf{G}(\mathcal{A})$ il semigruppo generato da $\mathcal{A}$, ovvero l'insieme degli ideali di $\mathcal{O}_\mathbb{F}$ nella cui fattorizzazione compaiono solo primi di $\mathcal{A}$. Definiamo quindi

$$\zeta_{\mathbb{F},\mathcal{A}}(s) = \sum_{I \in \mathsf{G}(\mathcal{A})} \frac{1}{N(I)^s}.$$

Anche a questa funzione possiamo applicare gli argomenti visti sopra per vedere che la serie converge (assolutamente) in $S(1)$ dove si ha

$$\zeta_{\mathbb{F},\mathcal{A}}(s) = \sum_{I \in \mathsf{G}(\mathcal{A})} \frac{1}{N(I)^s} = \prod_{P \in \mathcal{A}} \frac{1}{1 - \frac{1}{N(P)^s}}.$$

Definizione 6.3.2 *Diremo che $\mathcal{A}$ ha* densità polare m/n *se la funzione $\zeta^n_{\mathbb{F},\mathcal{A}}(s)$ ammette una estensione meromorfa in un intorno di $s = 1$, con un polo di ordine m in 1.*

Se $\mathcal{A}$ è finito è possibile trovare un intorno U di 1 in cui $N(P)^s \neq 1$ per ogni $P \in \mathcal{A}$, e quindi $\zeta^n_{\mathbb{F},\mathcal{A}}(s)$ è olomorfa in U per ogni n. Di conseguenza la densità polare di $\mathcal{A}$ è 0, come del resto era ragionevole supporre. Esistono comunque insiemi piuttosto ampi di primi, la cui densità polare è nulla. Un importante esempio è il seguente.

Proposizione 6.3.3 *Supponiamo che, per ogni $P \in \mathcal{A}$, $N(P)$ non sia un primo. Allora la densità polare di $\mathcal{A}$ è zero.*

Dimostrazione. Ogni primo razionale p si fattorizza nel prodotto di al più $k = |\mathbb{F} : \mathbb{Q}|$ ideali primi di $\mathcal{O}_\mathbb{F}$. Possiamo allora costruire degli insiemi $\mathcal{B}_i \subseteq \mathcal{A}$ in modo che

- $\mathcal{A} = \bigcup_{i=1}^k \mathcal{B}_i$;
- $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$ se $i \neq j$;
- se $P, Q \in \mathcal{B}_i$ sono distinti, allora $N(P)$ e $N(Q)$ sono potenze di primi diversi.

Ovviamente qualcuno di questi insiemi potrebbe essere vuoto. Abbiamo dunque che $\zeta_{\mathbb{F},\mathcal{A}}(s) = \prod_{i=1}^k \zeta_{\mathbb{F},\mathcal{B}_i}(s)$ dove, se $\mathcal{B}_i = \emptyset$, si intende $\zeta_{\mathbb{F},\mathcal{B}_i}(s) = 1$. Fissiamo $\mathcal{B} = \mathcal{B}_i$ e scriviamo

$$\zeta_{\mathbb{F},\mathcal{B}}(s) = \prod_{P \in \mathcal{B}} \left(1 - \frac{1}{N(P)^s}\right)^{-1}$$

e ciascun fattore è relativo ad un diverso primo razionale p.

Espandendo in serie uno dei fattori abbiamo

$$\left(1 - \frac{1}{N(P)^s}\right)^{-1} = \sum_{r=0}^{\infty} \frac{1}{N(P)^{rs}} = \sum_{r=0}^{\infty} \frac{1}{p^{mrs}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

dove $a_n = 0$ se n non è una potenza di p^m, e vale 1 altrimenti. Se scriviamo la funzione $\eta(s) = \zeta(ms)$ come

$$\eta(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

abbiamo che $b_n = 0$ se n non è una potenza m-esima, mentre vale 1 altrimenti. Di conseguenza $B(t) = \sum_{n \leq t} b_n = |\{i \mid i^m \leq t\}| \in O(t^{1/m})$. Per ogni t vale dunque la disuguaglianza

$$A(t) = \sum_{n \leq t} a_n \leq B(t)$$

e questo prova, grazie al Lemma 6.1.2, che $\left(1 - \frac{1}{N(P)^s}\right)^{-1}$ è una funzione olomorfa in $S(1/m)$. In particolare, essendo $m \geq 2$, è definita in $s = 1$. Se ne deduce che ciascun fattore $\zeta_{\mathbb{F},\mathcal{B}_i}(s)$ è olomorfo in $S(1/2)$ e pertanto $\zeta_{\mathbb{F},\mathcal{A}}(s)$ è olomorfa in $S(1/2)$ provando che $\mathcal{A}$ ha densità polare 0. □

Vediamo come valutare la densità polare di alcuni insiemi di primi.

Proposizione 6.3.4 *Siano $\mathbb{F} \leq \mathbb{K}$ campi di numeri con $\mathbb{K}|\mathbb{F}$ una estensione normale. Se $\mathcal{A}$ è l'insieme dei primi di $\mathcal{O}_\mathbb{F}$ che si spezzano completamente in $\mathcal{O}_\mathbb{K}$, allora la sua densità polare è $1/|\mathbb{K} : \mathbb{F}|$.*

Dimostrazione. Poniamo $n = |\mathbb{K} : \mathbb{F}|$. Se $\mathcal{B}$ è l'insieme dei primi di $\mathcal{O}_\mathbb{K}$ che stanno sopra a qualche primo di $\mathcal{A}$ abbiamo che, se $Q \in \mathcal{B}$ e $P = Q \cap \mathcal{O}_\mathbb{F}$, allora $P \in \mathcal{A}$ e $N(Q) = N(P)$. Inoltre ci sono esattamente n primi distinti di $\mathcal{O}_\mathbb{K}$ sopra P. Possiamo allora ripartire $\mathcal{B}$ nell'unione disgiunta di n insiemi $\mathcal{B}(i)$ in modo tale che, se $Q, R \in \mathcal{B}(i)$, allora $Q \cap \mathcal{O}_\mathbb{F} \neq R \cap \mathcal{O}_\mathbb{F}$. In questo modo le funzioni $\eta_i : \mathcal{B}(i) \longrightarrow \mathcal{A}$ definite da $\eta_i(Q) = Q \cap \mathcal{O}_\mathbb{F}$ sono biiezioni e vale $N(\eta_i(Q)) = N(Q)$ per ogni Q. Queste osservazioni ci dicono che

$$\zeta_{\mathbb{K},\mathcal{B}}(s) = \prod_{i=1}^{n} \zeta_{\mathbb{K},\mathcal{B}(i)}(s) = \zeta^n_{\mathbb{F},\mathcal{A}}(s)$$

e dunque, per concludere, sarà sufficiente mostrare che $\zeta_{\mathbb{K},\mathcal{B}}(s)$ ha un polo di ordine 1 in $s = 1$. Siano $\mathcal{R}$ l'insieme dei primi di $\mathcal{O}_\mathbb{K}$ sopra ai primi di $\mathcal{O}_\mathbb{F}$ che si ramificano, e $\mathcal{T}$ l'insieme dei primi fuori da $\mathcal{B} \cup \mathcal{R}$. L'insieme $\mathcal{R}$ è finito e quindi $\zeta_{\mathbb{K},\mathcal{R}}(s)$ è analitica in un intorno di 1. Se $Q \in \mathcal{T}$ allora la sua norma non è un primo, visto che Q deve avere indice di inerzia almeno 2 e quindi, per la dimostrazione della Proposizione 6.3.3, anche $\zeta_{\mathbb{K},\mathcal{T}}(s)$ è analitica in un intorno di 1. D'altra parte $\zeta_\mathbb{K}(s)$ ha un polo di ordine 1 in $s = 1$ e, visto che

$$\zeta_\mathbb{K}(s) = \zeta_{\mathbb{K},\mathcal{B}}(s)\zeta_{\mathbb{K},\mathcal{R}}(s)\zeta_{\mathbb{K},\mathcal{T}}(s)$$

deduciamo che $\zeta_{\mathbb{K},\mathcal{B}}(s)$ deve avere un polo di ordine 1 in $s = 1$. □

In particolare abbiamo che l'insieme dei primi che si spezzano completamente è infinito. Questa proposizione ha un corollario interessante alla cui dimostrazione facciamo precedere un lemma che ci saà necessario in seguito. Per enunciarlo è necessario stabilire alcune notazioni. Sia ω una radice m-esima primitiva di 1 e poniamo $\mathbb{K} = \mathbb{Q}[\omega]$. Il gruppo di Galois di questa estensione è isomorfo ad U_m ed ogni $\overline{a} = a + m\mathbb{Z}$ si identifica con l'elemento del gruppo di Galois che manda ω in ω^a.

Lemma 6.3.5 *Siano $\mathbb{K} = \mathbb{Q}[\omega]$ la m-esima estensione ciclotomica ed $\mathbb{F}$ un suo sottocampo. Se p è un primo non ramificato in $\mathbb{K}$ indichiamo con f_p l'indice di inerzia $f(P \mid p)$ per ogni primo P di $\mathcal{O}_\mathbb{F}$ sopra p. Allora, se $H = \mathcal{G}al(\mathbb{K} \mid \mathbb{F})$, si ha che f_p è l'ordine dell'elemento $\overline{p}H$ in U_m/H.*

Dimostrazione. Sia $(p) = Q_1 \cdots Q_k$ la fattorizzazione in $\mathcal{O}_\mathbb{F}$. Dato che l'stensione è abeliana, esiste un elemento ϕ che è l'elemento di Frobenius per ciascuno dei primi Q_i. Come prima cosa mostriamo che $\phi = \overline{p}$. Gli automorfismi $\phi, \overline{p}$ agiscono su $\mathbb{Z}[\omega]/(p)$ e $\tau = \overline{p}\phi^{-1}$ è l'dentità perché fissa la classe di ω. Allora $\tau \in E(Q_i)$ per ogni i perché $\mathcal{O}_\mathbb{K}/Q_i$ è un quoziente di $\mathbb{Z}[\omega]/(p)$. D'altra parte questi sottogruppi sono banali perché p non si ramifica e quindi $\phi = \overline{p}$. In particolare $\overline{p} \in D(Q)$ per ogni primo Q sopra p. Fissato il primo Q poniamo $P = Q \cap \mathcal{O}_\mathbb{F}$. Questo è un primo sopra p ed il suo indice di inerzia è f_p. Il gruppo U_m/H è isomorfo al gruppo di Galois di $\mathbb{F}|\mathbb{Q}$ e un suo generico elemento σH agisce su $\mathbb{F}$ tramite la restrizione di σ. Quindi, se f è l'ordine di $\overline{p}H$, abbiamo che $\overline{p}^f$ induce l'identità su $\mathbb{F}$, mentre $\overline{p}^e$ agisce in modo non banale se f non divide e. Il sottoanello $\mathcal{O}_\mathbb{F}/P \simeq \mathcal{O}_\mathbb{F} + Q/Q \leq \mathcal{O}_\mathbb{K}/Q$ è un campo con p^{f_p} elementi, quindi $\overline{p}^{f_p}$ induce l'dentità su $\mathcal{O}_\mathbb{F}/P$. Di conseguenza $\overline{p}^{f_p} \in E(P)$, ma questo è il sottogruppo banale perché p non è ramificato. Questo significa che $\overline{p}^{f_p}$ agisce banalmente su $\mathcal{O}_\mathbb{F}$ (e quindi su $\mathbb{F}$) o, in altri termini, $\overline{p}^{f_p} \in H$ e pertanto $f | f_p$. Viceversa $\overline{p}^f$ fissa $\mathcal{O}_\mathbb{F}$ e è perciò l'identità su $\mathcal{O}_\mathbb{F}/P$, il sottocampo di $\mathcal{O}_\mathbb{K}/Q$ con p^{f_p} elementi. Ma una potenza del morfismo di Frobenius fissa questo sottocampo, se e solo se l'esponente è multiplo di f_p. Assieme a quanto visto sopra otteniamo $f = f_p$. □

Il corollario della Proposizione 6.3.4 è il seguente.

Corollario 6.3.6 *Siano m un numero naturale e U_m il gruppo degli elementi invertibili di $\mathbb{Z}/m\mathbb{Z}$. Fissato $H \leq U_m$ sia $\mathcal{A} = \{p \mid p \text{ e primo e } \overline{p} = p + m\mathbb{Z} \in H\}$. Allora la densità polare $\mathcal{A}$ è $|H| / \varphi(m) = 1/|U_m : H|$.*

Dimostrazione. Sia ω una radice m-esima primitiva di 1, poniamo $\mathbb{K} = \mathbb{Q}[\omega]$ ed $\mathbb{F} = \mathrm{Inv}_\mathbb{K}(H)$. Il Lemma 6.3.5 dice che, per primi p non ramificati, $p \in \mathcal{A}$ se e solo se i suoi fattori primi in $\mathbb{O}_\mathbb{F}$ hanno indice di inerzia 1, ovvero se e solo se p si spezza completamente in $\mathcal{O}_\mathbb{F}$. Per la Proposizione 6.3.4, la densità polare di $\mathcal{A}$ è $1/|\mathbb{K} : \mathbb{Q}| = |H| / \varphi(m) = 1/|U_m : H|$. □

Da questo corollario otteniamo una forma debole, ma lo stesso interessante, del teorema di Dirichlet sulla distribuzione di primi nelle successioni aritmetiche.

Corollario 6.3.7 *Sia $m \geq 2$ un numero naturale. Allora esistono infiniti numeri primi p tali che $p \equiv 1 \pmod{m}$.*

Dimostrazione. Si usa il Corollario 6.3.6 scegliendo $H = 1$. L'nsieme dei primi congrui a 1 modulo m ha quindi densità analitica $1/\varphi(m)$ e, in particolare, deve essere infinito. □

Possiamo infine applicare questo risultato per provare che il problema inverso della teoria di Galois ha soluzione positiva per i gruppi abeliani finiti.

Teorema 6.3.8 *Sia G un gruppo abeliano finito. Allora esiste una estensione normale $\mathbb{F}|\mathbb{Q}$ tale che $\mathcal{G}al(\mathbb{F}|\mathbb{Q}) \simeq G$.*

DIMOSTRAZIONE. Il gruppo G è un prodotto diretto di ciclici

$$G \simeq \oplus_{i=1}^{k} C_i$$

con C_i ciclico di ordine n_i. Per ciascun indice i esistono, per il Corollario 6.3.7, infiniti primi congrui ad 1 modulo n_i. Possiamo allora scegliere dei primi q_i per $i = 1, \ldots, k$ in modo tale che

(*i*) $q_i \equiv 1 \pmod{n_i}$ per ogni $i = 1, \ldots, k$ e

(*ii*) $q_i \neq q_j$ se $i \neq j$.

Per il Teorema Cinese dei Resti $\mathbb{Z}/m\mathbb{Z} \simeq \oplus_{i=1}^{k} \mathbb{Z}/q_i\mathbb{Z}$ e quindi $U_m \simeq \oplus_{i=1}^{k} U_{q_i}$. Inoltre ciascun U_{q_i} è ciclico di ordine $q_i - 1$ e per ogni i c'è un sottogruppo $A_i \leq U_i$ con U_i/A_i ciclico di ordine n_i. Poniamo $m = \prod_{i=1}^{k} q_i$ e consideriamo $\mathbb{K}$ la m-esima estensione ciclotomica. Il gruppo di Galois di questa estensione si può identificare con U_m. Posto $A = \oplus_{i=1}^{k} A_i$ si ottiene

$$U_m/A \simeq \oplus_{i=1}^{k} U_i/A_i \simeq \oplus_{i=1}^{k} C_i \simeq G.$$

Se $\mathbb{F} = \mathrm{Inv}_{\mathbb{K}}(A)$ abbiamo che $\mathbb{F}|\mathbb{Q}$ è un'estensione normale, ed il suo gruppo di Galois è isomorfo a $U_m/A \simeq G$. □

6.4 Funzioni L e *Class number formula*

Per un campo di numeri $\mathbb{F}$ di grado n abbiamo una estensione a $S(1-1/n)$ della sua funzione zeta di Dedekind data da

$$\zeta_{\mathbb{F}}(s) = \sum_{n=1}^{\infty} \frac{j_n - h\kappa}{n^s} + h\kappa\zeta(s)$$

dove la serie di Dirichlet che compare in questa scrittura converge in $S(1-1/n)$. Allora è finito il

$$\lim_{s \to 1} \frac{\zeta_{\mathbb{F}}(s)}{\zeta(s)} = \rho$$

e l'ordine del gruppo delle classi di $\mathbb{F}$ è dato da $h = \rho/\kappa$. Il numero κ si può calcolare tramite la formula nella Definizione 6.2.2 e cercheremo ora di trovare una espressione per il numero ρ che, in conseguenza, ci darà una formula per esprimere h. Troveremo questa formula nel caso in cui $\mathbb{F}$ sia una estensione abeliana di $\mathbb{Q}$ ma sarà necessario assumere il seguente teorema.

Teorema 6.4.1 (Teorema di Kronecker-Weber) *Se $\mathbb{F}|\mathbb{Q}$ è un'estensione abeliana, allora esiste una estensione ciclotomica $\mathbb{K}$ tale che $\mathbb{F} \leq \mathbb{K}$.*

La dimostrazione di questo teorema va oltre gli scopi di queste note ma, se il lettore non intende usare strumenti di cui non conosce la dimostrazione, può limitarsi a pensare al caso delle

estensioni quadratiche, per le quali abbiamo provato il Teorema 5.2.4. Useremo anche diversi fatti riguardanti caratteri di gruppi abeliani per i quali rimandiamo il lettore all'Appendice.

Sia allora $\mathbb{F}$ una estensione abeliana di $\mathbb{Q}$. Possiamo assume i seguenti fatti:

1. $\mathbb{F}$ è sottocampo della m-esima estensione ciclotomica $\mathbb{K} = \mathbb{Q}[\omega]$ con $\omega = e^{2\pi i/m}$;
2. i primi ramificati in $\mathbb{F}$ sono tutti e soli quelli che dividono m.

In queste ipotesi il gruppo di Galois G di $\mathbb{F}|\mathbb{Q}$ è isomorfo ad un quoziente U_m/H ed $\mathbb{F} = \mathrm{Inv}_{\mathbb{K}}(H)$. Pertanto il gruppo $\widehat{G}$ si può identificare con un sottogruppo di $\widehat{U_m}$ (vedi 6.4.15).

Se χ è un carattere del gruppo U_m, possiamo estendere χ ad una funzione moltiplicativa, che indicheremo ancora con χ, ponendo

$$\chi(n) = \begin{cases} \chi(\overline{n}) & \text{se } (n,m) = 1 \\ 0 & \text{se } (n,m) \neq 1. \end{cases}$$

Queste funzioni saranno dette *caratteri modulo* m. Il *carattere banale* sarà quello che estende $1 \in \widehat{U}_m$. Per ciascuno di questi caratteri abbiamo la corrispondente *funzione L di Dirichlet* definita da

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Usando i risultati della sezione precedente abbiamo che $L(s,\chi)$ converge assolutamente ad una funzione olomorfa su $S(1)$ e, in questo dominio, ha una fattorizzazione di Eulero

$$L(s,\chi) = \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Se poniamo $A(t) = \sum_{n \leq t} \chi(n)$ possiamo provare che questa funzione è limitata in modulo quando $\chi \neq 1$. Infatti, se $I \subseteq \mathbb{Z}$ è un intervallo di ampiezza m, abbiamo che I è un sistema di rappresentanti per $\mathbb{Z}/m\mathbb{Z}$. Quindi

$$\sum_{n \in I} \chi(n) = \sum_{\substack{n \in I \\ (n,m)=1}} \chi(n) = \sum_{g \in U_m} \chi(g) = 0$$

per la Proposizione 6.4.12. Da questo deduciamo $|A(t)| \leq |\sum_{n=0}^{m-1} \chi(n)| \leq \varphi(n)$ e, per il Lemma 6.1.2, la serie che definisce $\zeta_{\mathbb{F}}(s)$ converge in $S(0)$ ad una funzione olomorfa. In particolare $L(s,\chi)$ è definita in $s = 1$ quando $\chi \neq 1$.

Possiamo subito notare un legame tra $L(s,1)$ e la zeta di Riemann. Nel dominio $S(1)$

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p|m} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \nmid m} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p|m} \left(1 - \frac{1}{p^s}\right)^{-1} L(s,1).$$

In particolare la funzione zeta di Riemann coincide (su $S(1)$) con $L(s,1)$, a meno di un fattore analitico.

Cercheremo di calcolare il numero ρ usando le funzioni $L(s,\chi)$ e per farlo sarà necessario trovare una scrittura alternativa per la zeta di Dedekind di $\mathbb{F}$.

Sia p un primo che non divide m (e quindi non ramificato in $\mathbb{K}$). Allora $p\mathcal{O}_{\mathbb{F}}$ è prodotto di r_p fattori primi, ciascuno con indice di inerzia f_p. Inoltre $f_p r_p = |G|$. Sia $\overline{p} \in U_m$ l'automorfismo di $\mathbb{K}$ che manda ω in ω^p. Il Lemma 6.3.5 mostra che f_p è l'ordine di $\overline{p}H$ in $G = U_m/H$ e quindi $r_p = |G|/f_p$. Infine, se $\chi \in \widehat{G}$, possiamo pensarlo come un elemento del sottogruppo $K(G) \leq \widehat{U}_m$ ed ha quindi senso scrivere $L(s,\chi)$. Con queste notazioni abbiamo

Lemma 6.4.2 *In $S(1)$ si ha*

$$\zeta_{\mathbb{F}}(s) = \prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p} \quad e \quad \prod_{\chi\in\widehat{G}} L(s,\chi) = \prod_{p\nmid m} \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}.$$

Dimostrazione. Per provare la prima uguaglianza definiamo, per ogni primo $p \in \mathbb{N}$, l'insieme $\mathcal{F}(p)$ dei primi di $\mathcal{O}_{\mathbb{F}}$ sopra p, ed indichiamo con r_p la sua cardinalità. Ogni primo in $\mathcal{F}(p)$ ha norma p^{f_p}. Sfruttando la fattorizzazione di Eulero e la possibilità di cambiare l'ordine dei fattori abbiamo

$$\zeta_{\mathbb{F}}(s) = \prod_{P\in\mathcal{P}} \left(1 - \frac{1}{N(P)^s}\right)^{-1} = \prod_{p\in\mathbb{P}} \prod_{P\in\mathcal{F}(p)} \left(1 - \frac{1}{N(P)^s}\right)^{-1} =$$

$$= \prod_{p\in\mathbb{P}} \prod_{P\in\mathcal{F}(p)} \left(1 - \frac{1}{p^{f_p s}}\right)^{-1} = \prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}$$

in $S(1)$.

Il gruppo $\widehat{G}$ è isomorfo a $\widehat{U_m/H}$ e, usando la Proposizione 6.4.15 possiamo identificarlo col sottogruppo $K(G) = \{\chi \in \widehat{U}_m | \, H \leq \ker(\chi)\}$. Per $g = \overline{p}H \in G$ possiamo usare questa identificazione ed il Lemma 6.4.13 per ottenere

$$\prod_{\chi\in\widehat{G}} \left(1 - \frac{\chi(g)}{p^s}\right) = \prod_{\chi\in K(G)} \left(1 - \frac{\chi(p)}{p^s}\right)$$

Se T indica il gruppo delle radici f_p-esime di 1, ogni $\chi(g)$ appartiene a T e, visto che ogni carattere di $\langle g\rangle$ si estende in $|G|/f_g = r_p$ modi distinti ad un carattere di G, per ogni elemento $\varepsilon \in T$ esistono r_p caratteri distinti χ tali che $\varepsilon = \chi(g)$. L'uguaglianza ottenuta si può elaborare ulteriormente ricavando

$$\prod_{\chi\in K(G)} \left(1 - \frac{\chi(p)}{p^s}\right) = \prod_{\varepsilon\in T} \prod_{\substack{\chi(g)=\varepsilon \\ \chi\in K(G)}} \left(1 - \frac{\varepsilon}{p^s}\right) = \prod_{\varepsilon\in T} \left(1 - \frac{\varepsilon}{p^s}\right)^{r_p} = \left(\prod_{\varepsilon\in T} \left(1 - \frac{\varepsilon}{p^s}\right)\right)^{r_p}.$$

Il polinomio $g(x) = x^{f_p} - (1/p^s)^{f_p}$ si fattorizza in $\mathbb{C}$ come

$$g(x) = \prod_{\varepsilon\in T} \left(x - \frac{\varepsilon}{p^s}\right)$$

e dunque

$$\prod_{\chi\in\widehat{G}}\left(1-\frac{\chi(g)}{p^s}\right)=g(1)^{r_p}=\left(1-\frac{1}{p^{f_p s}}\right)^{r_p}.$$

Usando questa uguaglianza possiamo valutare il prodotto delle funzioni $L(s,\chi)$ sfruttando ancora una volta la possibilità di cambiare l'ordine dei fattori. Otteniamo

$$\prod_{\chi\in\widehat{G}}L(s,\chi)=\prod_{\chi\in\widehat{G}}\prod_{p\nmid m}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}=\prod_{p\nmid m}\prod_{\chi\in\widehat{G}}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}=\prod_{p\nmid m}\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}$$

come volevamo dimostrare. □

Questa proposizione ha una conseguenza per quello che riguarda il calcolo di dell'ordine del gruppo delle classi di $\mathbb{F}$.

Teorema 6.4.3 *Sia* $\rho=\lim_{s\to1}\zeta_{\mathbb{F}}(s)/\zeta(s)$. *Allora*

$$\rho=\prod_{p\,|\,m}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^{f_p}}\right)^{-r_p}\prod_{\substack{\chi\in\widehat{G}\\ \chi\neq1}}L(1,\chi).$$

Dimostrazione. Dal Lemma 6.4.2 ricaviamo

$$\zeta_{\mathbb{F}}(s)=\prod_{p\,|\,m}\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}\prod_{p\nmid m}\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}=\prod_{p\,|\,m}\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}\prod_{\chi\in\widehat{G}}L(s,\chi)$$

e ricordiamo che abbiamo anche ottenuto l'uguaglianza

$$\zeta(s)=\prod_{p\,|\,m}\left(1-\frac{1}{p^s}\right)^{-1}L(s,1).$$

Combinando queste due relazioni

$$\frac{\zeta_{\mathbb{F}}(s)}{\zeta(s)}=\prod_{p\,|\,m}\left(1-\frac{1}{p^s}\right)\left(1-\frac{1}{p^{f_p s}}\right)^{-r_p}\prod_{\substack{\chi\in\widehat{G}\\ \chi\neq1}}L(s,\chi).$$

Il risultato segue dal fatto che questa funzione è analitica in un intorno di 1 e quindi il limite coincide con il suo valore in $s=1$. □

Abbiamo quindi ricondotto il nostro problema a quello del calcolo di $L(1,\chi)$ nel caso dei caratteri non banali. Per farlo occorrono due nuove definizioni. Sia z un numero complesso con $|z|<1$. Definiamo il logaritmo di $1-z$ come

$$\log(1-z)=-\sum_{n=1}^{\infty}\frac{z^n}{n}.$$

Un confronto con la serie geometrica mostra che questa serie converge assolutamente e, in alcuni casi, abbiamo convergenza anche quando $|z|=1$. In particolare, se $z^m=1$ e $z\neq1$, sappiamo

che $\sum_{i=0}^{m-1} z^i = 0$, da cui ricaviamo $|\sum_{n\le t} z^n| \le m-1$ per ogni $t \ge 0$. Il Lemma 6.1.2 ci assicura che la serie $g(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^s}$ converge in $S(0)$ ad una funzione analitica e pertanto esiste $\log(1-z) = -g(z)$. Fissiamo ora $\omega = e^{2\pi i/m}$ e scegliamo $\chi \in \widehat{U}_m$. Come sempre il simbolo $\overline{a}$ indicherà la classe $a + m\mathbb{Z}$. Per ogni $k = 0, 1, \dots, m-1$ definiamo la *somma di Gauss*

$$\tau_k(\chi) = \sum_{\overline{a} \in U_m} \chi(\overline{a}) \omega^{ak}.$$

Notiamo che la definizione è buona perché, se $\overline{a} = \overline{b}$, anche $\omega^a = \omega^b$.

Proposizione 6.4.4 *Se $\chi \in \widehat{U}_m$ è un carattere non banale ed $\omega = e^{2\pi i/m}$ si ha*

$$L(1, \chi) = -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \log(1 - \omega^k).$$

Dimostrazione. Lavoriamo nel semipiano $S(1)$, dove la serie che definisce $L(s, \chi)$ converge assolutamente, permettendoci quindi di modificare l'ordine di sommatoria. Per prima cosa si ottiene

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{\overline{a} \in U_m} \chi(a) \sum_{\overline{n} = \overline{a}} \frac{1}{n^s}.$$

Notiamo che ω^{a-n} è 1 se e solo se $\overline{n} = \overline{a}$ e quindi

$$\sum_{k=0}^{m-1} \omega^{(a-n)k} = \begin{cases} 0 & \text{se} \quad \overline{n} \neq \overline{a} \\ m & \text{se} \quad \overline{n} = \overline{a}. \end{cases}$$

Utilizzando questo fatto

$$\begin{aligned} \sum_{\overline{a} \in U_m} \chi(a) \sum_{\overline{n} = \overline{a}} \frac{1}{n^s} &= \sum_{\overline{a} \in U_m} \chi(a) \sum_{n=1}^{\infty} \frac{\frac{1}{m} \sum_{k=0}^{m-1} \omega^{(a-n)k}}{n^s} = \\ &= \frac{1}{m} \sum_{\overline{a} \in U_m} \chi(a) \sum_{k=0}^{m-1} \omega^{ak} \sum_{n=1}^{\infty} \frac{\omega^{-nk}}{n^s} = \\ &= \sum_{k=0}^{m-1} \sum_{\overline{a} \in U_m} \chi(a) \omega^{ak} \sum_{n=1}^{\infty} \frac{\omega^{-nk}}{n^s} = \\ &= \sum_{k=0}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{(\omega^{-k})^n}{n^s}. \end{aligned}$$

Come osservato sopra, la serie $g(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^s}$ converge in $S(0)$ e quindi $g(\omega^{-k}) = -\log(1 - \omega^{-k})$ e si ottiene

$$\frac{1}{m} \sum_{k=0}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{(\omega^{-k})^n}{n^s} = -\frac{1}{m} \sum_{k=0}^{m-1} \tau_k(\chi) \log(1 - \omega^{-k}).$$

Osservando che $\tau_0(\chi) = 0$ abbiamo la tesi. □

L'espressione ottenuta si può semplificare riducendola al caso di un particolare tipo di caratteri.

Definizione 6.4.5 *Siano m un numero naturale, d un suo divisore e $\pi : U_m \longrightarrow U_d$ la restrizione della proiezione $\pi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$. Diciamo che $\phi \in \widehat{U}_d$ induce $\chi \in \widehat{U}_m$ se $\chi = \phi \circ \pi$.*

La stessa definizione si applica quando ϕ, χ sono caratteri modulo d e modulo m. Un carattere $\chi \in \widehat{U}_m$ che non sia indotto da alcun carattere si dice *primitivo*. Caratteri primitivi esistono, come mostra il seguente esempio.

Esempio 6.4.6 *Il gruppo U_{12} è isomorfo al prodotto diretto $U_4 \times U_3$ e quindi è un gruppo di Klein, generato dalle classi $\overline{5}, \overline{7}$. Esiste allora un unico morfismo $\chi \in \widehat{U}_m$ che soddisfa $\chi(\overline{5}) = -1 = \chi(\overline{7})$. Supponendo χ indotto da $\phi \in \widehat{U}_4$ avremmo*

$$-1 = \chi(\overline{5}) = \phi \circ \pi(\overline{5}) = \phi(5 + 4\mathbb{Z}) = \phi(1 + 4\mathbb{Z}) = 1$$

una contraddizione. Allo stesso modo, calcolando $\chi(\overline{7})$, si mostra che χ non può essere indotto da un carattere modulo 3 o modulo 6.

Può essere utile osservare che la proiezione da U_m in U_d è suriettiva. Scriviamo $m = ab$ con $(a, b) = 1$ in modo che a e d siano divisi dagli stessi primi (b potrebbe quindi essere 1). Se $k + d\mathbb{Z} \in U_d$ sappiamo che esiste x tale che

$$\begin{cases} x \equiv k \pmod{a} \\ x \equiv 1 \pmod{b}. \end{cases}$$

Questo intero è necessariamente coprimo con m e quindi $x+m\mathbb{Z} \in U_m$. Chiaramente $\pi(x+m\mathbb{Z}) = k + d\mathbb{Z}$.

Il prossimo lemma ci fa intuire l'utilità dei caratteri primitivi.

Lemma 6.4.7 *Sia χ un carattere modulo m indotto dal carattere $\phi \in \widehat{U}_d$. Allora*

$$L(1, \chi) = L(1, \phi) \prod_{\substack{p \mid m \\ p \nmid d}} \left(1 - \frac{\phi(p)}{p}\right).$$

Dimostrazione. In $S(1)$ possiamo scrivere

$$L(s, \chi) = \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{p \nmid m} \left(1 - \frac{\phi(\pi(p))}{p^s}\right)^{-1} = \prod_{p \nmid m} \left(1 - \frac{\phi(p)}{p^s}\right)^{-1}.$$

Dato che

$$\{p \in \mathbb{P} \mid p \nmid d\} = \{p \in \mathbb{P} \mid p \nmid m\} \cup \{p \in \mathbb{P} \mid p \mid m \text{ e } p \nmid d\}$$

otteniamo

$$\prod_{p \nmid m} \left(1 - \frac{\phi(p)}{p^s}\right)^{-1} = L(s, \phi) \prod_{\substack{p \mid m \\ p \nmid d}} \left(1 - \frac{\phi(p)}{p^s}\right).$$

Poniamo $f(s) = \prod_{\substack{p\,|\,m \\ p\nmid d}} \left(1 - \frac{\phi(p)}{p^s}\right)$ e notiamo che questa è una funzione olomorfa in $S(0)$. Possiamo usare il fatto che $L(s,\phi)$ è olomorfa in $S(0)$ per ottenere che $g(s) = L(s,\phi)f(s)$ è olomorfa in $S(0)$. Quindi anche $h(s) = L(s,\chi) - g(s)$ è una funzione olomorfa in $S(0)$. D'altra parte questa funzione è nulla in $S(1)$ e questo implica che $g(s)$ è costantemente uguale ad 0 in $S(0)$. In particolare l'uguaglianza

$$L(s,\chi) = L(s,\phi) \prod_{\substack{p\,|\,m \\ p\nmid d}} \left(1 - \frac{\phi(p)}{p^s}\right)$$

vale in $S(0)$ e di conseguenza

$$L(1,\chi) = L(1,\phi) \prod_{\substack{p\,|\,m \\ p\nmid d}} \left(1 - \frac{\phi(p)}{p}\right)$$

come volevamo dimostrare. □

Questo lemma ci dice che, volendo calcolare i valori $L(1,\chi)$, è sufficiente farlo nel caso di caratteri primitivi. Il prossimo lemma va in questa direzione.

Lemma 6.4.8 *Sia $\chi \in \widehat{U}_m$ un carattere primitivo. Allora*

$$\tau_k(\chi) = \begin{cases} \overline{\chi}(k)\tau(\chi) & \text{quando } (k,m) = 1 \\ 0 & \text{quando } (k,m) \neq 1 \end{cases}$$

dove $\tau(\chi) = \tau_1(\chi)$ e $\overline{\chi}$ indica il coniugato del carattere χ.

Dimostrazione. Per prima cosa notiamo che $\overline{\chi} = \chi^{-1}$ per cui $\overline{\chi}(u) = \chi^{-1}(u) = \chi(u^{-1})$ per ogni $u \in U_m$. Se $(k,m) = 1$ la classe $\overline{k}$ è invertibile e quindi ogni $\overline{a} \in U_m$ si scrive in modo unico come $\overline{a} = \overline{b}\,\overline{k}^{-1}$. Scrivendo $\overline{k}^{-1} = \overline{r}$ si ricava

$$\overline{\chi}(k)\tau(\chi) = \overline{\chi}(k) \sum_{\overline{b}\in U_m} \chi(\overline{b})\omega^b = \sum_{\overline{b}\in U_m} \chi(\overline{k}^{-1})\chi(\overline{b})\omega^b = \sum_{\overline{b}\in U_m} \chi(\overline{b}\,\overline{k}^{-1})\omega^b.$$

In U_m abbiamo $\overline{br} = \overline{b}\,\overline{r} = \overline{b}\,\overline{k}^{-1}$ e quindi, se $\overline{a} = \overline{b}\,\overline{k}^{-1}$, allora $\omega^b = \omega^{ak}$. Usando questa osservazione otteniamo infine

$$\sum_{\overline{b}\in U_m} \chi(\overline{b}\,\overline{k}^{-1})\omega^b = \sum_{\overline{a}\in U_m} \chi(\overline{a})\omega^{ak} = \tau_k(\chi).$$

Possiamo anche notare che, in questa parte della dimostrazione, l'ipotesi di primitività del carattere non è necessaria. Per dimostrare la seconda parte poniamo $d = m/(k,m)$ e indichiamo con K il nucleo della proiezione $\pi : U_m \longrightarrow U_d$. Se $\ker(\chi) \geq K$ possiamo definire $\phi \in \widehat{U}_d$ identificando U_d con U_m/K e ponendo $\phi(uK) = \chi(u)$. Una facile verifica mostra però che $\chi = \phi \circ \pi$, una contraddizione. Esiste quindi $\overline{b} \in K$ su cui χ non è banale. L'intero b è congruo

ad 1 modulo d e quindi $(b-1)k$ è divisibile per m. Ne segue che $\omega^{kb} = \omega^k$ e, usando il fatto che $\{\overline{ab} \mid \overline{a} \in U_m\} = U_m$, otteniamo

$$\tau_k(\chi) = \sum_{\overline{a}\in U_m} \chi(\overline{ab})\omega^{abk} = \sum_{\overline{a}\in U_m} \chi(\overline{ab})\omega^{ak} = \chi(\overline{b}) \sum_{\overline{a}\in U_m} \chi(\overline{a})\omega^{ak} = \chi(\overline{b})\tau_k(\chi)$$

e questo implica $\tau_k(\chi) = 0$ perché $\chi(\overline{b}) \neq 1$. □

La formula per $L(1,\chi)$ nel caso di caratteri primitivi diventa

$$L(1,\chi) = \frac{1}{m}\sum_{k=1}^{m-1} \overline{\chi}(\overline{k})\tau(\chi)\log(1-\omega^{-k}) = \frac{\tau(\chi)}{m}\sum_{k=1}^{m-1} \overline{\chi}(\overline{k})\log(1-\omega^{-k}) =$$
$$\frac{\tau(\chi)}{m}\sum_{k=1}^{m-1} \overline{\chi}(\overline{-k})\log(1-\omega^{k}) = \frac{\chi(-1)\tau(\chi)}{m}\sum_{k=1}^{m-1} \overline{\chi}(\overline{k})\log(1-\omega^{k})$$

dove abbiamo usato il fatto che $\chi(-1) = \overline{\chi}(-1)$. Cerchiamo adesso di calcolare esplicitamente $\log(1-\omega^k)$. Se $\alpha = e^{i\pi/m} = \omega^{1/2}$, facciamo vedere che $1-\omega^k = -2i\alpha^k \sin(k\pi/m)$. Abbiamo

$$(1-\omega^k)\alpha^{-k} = (1-\omega^k)\omega^{-k/2} = \omega^{-k/2} - \omega^{k/2} = \overline{\omega^{k/2}} - \omega^{k/2} = -2i\,\mathrm{Im}(\omega^{k/2}) = -2i\sin(k\pi/m)$$

da cui la tesi. Da questo si ricava facilmente che

$$\log(1-\omega^k) = \log(2) + \log\left(\sin\left(\frac{k\pi}{m}\right)\right) + i\pi\left(\frac{k}{m} - \frac{1}{2}\right)$$

e, ricordando che $\sum_{\overline{k}\in U_m} \overline{\chi}(\overline{k}) = 0$, ricaviamo

$$L(1,\chi) = \frac{\chi(-1)\tau(\chi)}{m}\sum_{k=1}^{m-1} \overline{\chi}(\overline{k})\left(\log\left(\sin\left(\frac{k\pi}{m}\right)\right) + \frac{k\pi i}{m}\right).$$

Per qualsiasi carattere si ha $\chi(-1) = \pm 1$ e, a seconda dei casi, la formula per $L(1,\chi)$ si riduce ad una forma piú semplice. Se $\chi(-1) = 1$ diciamo che il carattere è *pari*, mentre è *dispari* se $\chi(-1) = -1$. Quando il carattere è pari $\chi(\overline{m-k}) = \chi(\overline{-k}) = \chi(\overline{k})$ e quindi

$$\begin{aligned}\sum_{k=1}^{m-1} \chi(\overline{k})k &= \sum_{k=1}^{m-1} \chi(\overline{m-k})(m-k) = \\ &= \sum_{k=1}^{m-1} \chi(\overline{-k})(m-k) = \\ &= \sum_{k=1}^{m-1} \chi(\overline{k})(m-k) = \\ &= m\sum_{k=1}^{m-1} \chi(\overline{k}) - \sum_{k=1}^{m-1} \chi(\overline{k})(k) = -\sum_{k=1}^{m-1} \chi(\overline{k})(k)\end{aligned}$$

da cui $\sum_{k=1}^{m-1} \chi(\overline{k})(k) = 0$.

Quando χ è dispari

$$\sum_{k=1}^{m-1}\chi(\overline{k})\log\left(\sin\left(\frac{k\pi}{m}\right)\right)=\sum_{k=1}^{m-1}\chi(\overline{m-k})\log\left(\sin\left(\frac{(m-k)\pi}{m}\right)\right)=$$
$$=\sum_{k=1}^{m-1}\chi(\overline{-k})\log\left(\sin\left(\pi-\frac{k\pi}{m}\right)\right)=$$
$$=-\sum_{k=1}^{m-1}\chi(\overline{k})\log\left(\sin\left(\frac{k\pi}{m}\right)\right)$$

e dunque

$$\sum_{k=1}^{m-1}\chi(\overline{k})\log\left(\sin\left(\frac{k\pi}{m}\right)\right)=0.$$

Dividendo i due casi possiamo riscrivere il valore di $L(1,\chi)$ come

$$L(1,\chi)=\begin{cases}-\frac{2\tau(\chi)}{m}\sum_{k=1}^{m-1}\overline{\chi}(\overline{k})\log\sin\left(\frac{k\pi}{m}\right) & \text{se } \chi \text{ è pari}\\ \frac{\pi i\tau(\chi)}{m^2}\sum_{k=1}^{m-1}\overline{\chi}(\overline{k})k & \text{se } \chi \text{ è dispari}\end{cases}$$

Un'altra semplificazione si ottiene dal fatto che ρ è un numero strettamente positivo e quindi è sufficiente conoscere i valori $|L(1,\chi)|$ per calcolarlo. Ci servirà allora trovare $|\tau(\chi)|$ e lo calcoliamo valutandone il quadrato, sempre nel caso di un carattere primitivo.

$$|\tau(\chi)|^2=\Big(\sum_{\overline{a}\in U_m}\chi(\overline{a})\omega^a\Big)\overline{\Big(\sum_{\overline{b}\in U_m}\chi(\overline{b})\omega^b\Big)}=\sum_{\overline{a},\overline{b}\in U_m}\chi(\overline{a})\chi(\overline{b}^{-1})\omega^{a-b}$$

e posto $\overline{a}\overline{b}^{-1}=\overline{c}$,

$$\sum_{\overline{a},\overline{b}\in U_m}\chi(\overline{a})\chi(\overline{b}^{-1})\omega^{a-b}=\sum_{\overline{b},\overline{c}\in U_m}\chi(\overline{c})\omega^{bc-b}.$$

Per ogni $\overline{c}$ e per ogni intero $b\in[1,m-1]$ non coprimo con m, abbiamo

$$\sum_{\overline{c}\in U_m}\chi(\overline{c})\omega^{bc-b}=\omega^{-b}\sum_{\overline{c}\in U_m}\chi(\overline{c})\omega^{bc}=\omega^{-b}\tau_b(\chi)=0$$

e possiamo allora scrivere

$$\sum_{\overline{b},\overline{c}\in U_m}\chi(\overline{c})\omega^{bc-b}=\sum_{b=0}^{m-1}\sum_{\overline{c}\in U_m}\chi(\overline{c})\omega^{bc-b}=\sum_{\overline{c}\in U_m}\chi(\overline{c})\sum_{b=0}^{m-1}(\omega^{c-1})^b.$$

Se $\overline{c}\neq 1$, l'elemento ω^{c-1} è una radice m-esima dell'unità diversa da 1 e di conseguenza $\sum_{b=0}^{m-1}(\omega^{c-1})^b=0$. Otteniamo allora

$$|\tau(\chi)|^2=\sum_{\overline{c}\in U_m}\chi(\overline{c})\sum_{b=0}^{m-1}(\omega^{c-1})^b=\sum_{b=0}^{m-1}1=m$$

e quindi $|\tau(\chi)| = \sqrt{m}$.

È possibile dimostrare che, quando χ è un carattere primitivo dispari, si ha

$$\sum_{k=1}^{m-1} \chi(\overline{k})k = \frac{m}{\overline{\chi}(\overline{2}) - 2} \sum_{1 \leq k < m/2} \chi(\overline{k}).$$

Mettendo assieme le ultime osservazioni fatte, si ottiene il seguente teorema

Teorema 6.4.9 *Sia χ un carattere modulo $m \geq 3$ primitivo. Allora*

$$|L(1,\chi)| = \begin{cases} \frac{2}{\sqrt{m}} \left| \sum_{1 \leq k < m/2} \chi(\overline{k}) \log \sin\left(\frac{k\pi}{m}\right) \right| & \text{se } \chi \text{ è pari} \\ \frac{\pi}{|\chi(\overline{2})-2|\sqrt{m}} \left| \sum_{1 \leq k < m/2} \chi(\overline{k}) \right| & \text{se } \chi \text{ è dispari} \end{cases}$$

Si noti che nelle formule compare il carattere χ al posto del suo coniugato. Il motivo di questa sostituzione è dovuto al fatto che, per ogni numero complesso α, $|\alpha| = |\overline{\alpha}|$.

6.4.1 Un esempio: campi quadratici.

Il caso più semplice che può presentarsi è quello delle estensioni quadratiche. Sia $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ con d intero libero da quadrati. Indichiamo con m il valore assoluto di $\Delta_{\mathbb{F}}$. L'osservazione seguente al teorema 5.2.4 ci assicura che $\mathbb{F}$ è contenuto nella m-esima estensione ciclotomica $\mathbb{K} = \mathbb{Q}[\omega]$. Con questa scelta i primi ramificati in $\mathbb{F}$ sono tutti e soli i primi che dividono m. Il gruppo di Galois G di $\mathbb{F}$ è ciclico di ordine 2 e quindi possiede un unico carattere non banale χ. Se $H = \mathcal{G}al(\mathbb{F}|\mathbb{Q})$ abbiamo $G \simeq U_m/H = \langle \sigma H \rangle$ dove σ è un automorfismo tale che $\sigma(\sqrt{d}) = -\sqrt{d}$. Per i nostri scopi è necessario capire, per ogni primo p che non divide m, quando $\overline{p}$ appartiene ad H. La Proposizione 6.3.5 ci dice che $\overline{p} \in H$ se e solo se il primo p si fattorizza in fattori con indice di inerzia 1, ovvero quando p si spezza completamente. Se $d \equiv 2, 3 \pmod 4$ il 2 è sempre ramificato e un primo p dispari si spezza se e solo se d è un residuo quadratico modulo p. Nell'altro caso è ancora vero che un primo dispari p si spezza solo quando d è un residuo quadratico modulo p, mentre 2 si spezza se e solo se $d \equiv 1 \pmod 8$. Possiamo descrivere il carattere χ nel modo seguente, elencandone i valori sulle classi $\overline{p} \in U_m$, al variare di p tra i primi che non dividono m:

$$\chi(\overline{2}) = \begin{cases} 1 & \text{se } d \equiv 1 \pmod 8 \\ -1 & \text{se } d \equiv 5 \pmod 8 \end{cases} \qquad \text{e} \qquad \chi(\overline{p}) = \left(\frac{d}{p}\right) \text{ se } p \text{ è dispari}$$

dove $\left(\frac{d}{p}\right)$ indica il *simbolo di Legendre*. Per poter applicare la formula trovata è necessario provare che χ è primitivo e capirne la parità . Iniziamo studiando la parità e partiamo dal caso $d \equiv 1 \pmod 4$. Se $n \in \mathbb{N}$ è dispari, usando il fatto che χ è moltiplicativo e la definizione del *simbolo di Jacobi*, si ricava $\chi(\overline{n}) = \left(\frac{d}{n}\right)$. Scrivendo $d = \epsilon m$ abbiamo

$$\epsilon = \begin{cases} 1 & \text{se } m \equiv 1 \pmod 4 \\ -1 & \text{se } m \equiv 3 \pmod 4. \end{cases}$$

Il teorema di reciprocità per il simbolo di Jacobi ci dice che

$$\left(\frac{d}{n}\right) = \left(\frac{\epsilon}{n}\right)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right).$$

Se $A = \{p \,|\, p \text{ è un primo, } p\,|n \text{ e } p \equiv 3 \pmod 4\}$ abbiamo

$$\left(\frac{\epsilon}{n}\right) = \prod_{p\in A}\left(\frac{\epsilon}{p}\right) = \prod_{p\in A}\epsilon^{\frac{p-1}{2}} = \epsilon^{|A|}.$$

Allo stesso modo $(-1)^{\frac{n-1}{2}} = (-1)^{|A|}$. Se $\epsilon = 1$ deve essere $m \equiv 1 \pmod 4$ e quindi

$$\left(\frac{d}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right) = \left(\frac{n}{m}\right)$$

mentre, nell'altro caso, si ottiene

$$\left(\frac{d}{n}\right) = \left(\frac{\epsilon}{n}\right)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}}(-1)^{\frac{n-1}{2}}\left(\frac{n}{m}\right) = \left(\frac{n}{m}\right).$$

Per quanto riguarda il primo 2 ricordiamo intanto che, per ogni naturale dispari r, vale $\left(\frac{2}{r}\right) = (-1)^{(r^2-1)/8}$. Usando questo fatto si controlla facilmente che $\chi(\overline{2}) = \left(\frac{2}{m}\right)$. Infine la moltiplicatività del carattere ci permette di concludere che $\chi(\overline{n}) = \left(\frac{n}{m}\right)$ per ogni naturale n coprimo con m. Sia ora $n \in \mathbb{Z}$ negativo. Sfruttando le note proprietà del simbolo di Jacobi otteniamo

$$\chi(\overline{n}) = \chi(\overline{-1}\,\overline{-n}) = \chi(\overline{(m-1)}\,\overline{-n}) = \left(\frac{m-1}{m}\right)\left(\frac{-n}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{-n}{m}\right) = \left(\frac{n}{m}\right).$$

A questo punto possiamo calcolare

$$\chi(\overline{-1}) = \left(\frac{-1}{m}\right) = \begin{cases} (-1)^{\frac{d-1}{2}} = 1 & \text{se } d > 0 \\ (-1)^{\frac{m-1}{2}} = -1 & \text{se } d < 0 \end{cases}$$

e dedurre che χ è pari quando $d > 0$ e dispari altrimenti. Quando $d \equiv 2, 3 \pmod 4$ allora $m = 4|d|$ e quindi

$$\chi(\overline{-1}) = \chi(\overline{m-1}) = \left(\frac{d}{m-1}\right) = \left(\frac{4d}{m-1}\right) = \left(\frac{\epsilon m}{m-1}\right) = \epsilon^{\frac{m-2}{2}}.$$

Certamente $\chi(\overline{-1}) = 1$ se $d > 0$ visto che in questo caso $\epsilon = 1$. Quando d è negativo basta osservare che $m - 1 \equiv 3 \pmod 4$ per concludere che $\chi(\overline{-1}) = -1$. Possiamo riassumere entrambi i casi dicendo che χ è pari se e solo se $d > 0$.

Discuteremo la primitività di χ solo nel caso $d \equiv 1 \pmod 4$ sfruttando la formula esplicita che abbiamo ottenuto. Fissiamo un divisore positivo proprio k di m. L'intero m è libero da quadrati quindi possiamo trovare un primo q tale che $q|(m/k)$ e $(q, k) = 1$. Il primo q è dispari quindi esiste $a \in [1, q[$ che non sia un residuo quadratico modulo q. Se c è una soluzione del sistema

$$\begin{cases} x \equiv 1 \pmod{m/q} \\ x \equiv a \pmod q \end{cases}$$

abbiamo

$$\chi(\overline{c}) = \left(\frac{c}{m}\right) = \left(\frac{c}{q}\right)\left(\frac{c}{m/q}\right) = \left(\frac{a}{q}\right)\left(\frac{1}{m/q}\right) = -1.$$

Se χ fosse indotto da $\phi \in \widehat{U}_k$ avremmo invece

$$\chi(\overline{c}) = \phi(c + k\mathbb{Z}) = \phi(1 + k\mathbb{Z}) = 1$$

una contraddizione che dimostra che χ è primitivo. La dimostrazione del caso generale segue un'idea simile, ma la omettiamo.

Quando $d > 0$ indichiamo con u l'unità fondamentale di $\mathcal{O}_{\mathbb{F}}$ ovvero l'elemento positivo tale che $\langle -1, u\rangle$ sia il gruppo delle unità di $\mathcal{O}_{\mathbb{F}}$. Si verifica che $\kappa = 2\log(u)/\sqrt{m}$ se d è positivo, mentre vale $\pi/\sqrt{m}$ se d è negativo e diverso da $-1, -3$. Notiamo anche che, se $d = -1, -3$ l'anello degli interi è euclideo e quindi il gruppo delle classi è banale.

Possiamo allora enunciare il Teorema 6.4.9 nel caso di estensioni quadratiche.

Teorema 6.4.10 *Siano $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ con d intero libero da quadrati e diverso da -1 e -3, $m = |\Delta_{\mathbb{F}}|$ e $\chi \in \widehat{U}_m$ il carattere non banale del gruppo di Galois dell'estensione. Se h è l'ordine del gruppo delle classi di $\mathbb{F}$ si ha*

$$h = \frac{1}{\log u}\Big|\sum_{1\le k<m/2} \chi(\overline{k}) \log \sin \frac{k\pi}{m}\Big| \qquad \textit{se } d > 0 \textit{ e } u \textit{ è l' unità fondamentale}$$

e

$$h = \frac{1}{2 - \chi(\overline{2})}\Big|\sum_{1\le k<m/2} \chi(\overline{k})\Big| \qquad \textit{se } d < 0.$$

Come esempio studiamo il caso $d = -5$. Il discriminante del campo vale -20 ed $m = 20$. Il carattere χ deve essere calcolato sulle classi con rappresentante compreso tra 1 e 9. Le uniche su cui assume valore diverso da 0 sono quelle corrispondenti a $1, 3, 7, 9$ e quindi

$$h = \frac{1}{2}\left|1 + \left(\frac{-5}{3}\right) + \left(\frac{-5}{7}\right) + \left(\frac{-5}{9}\right)\right| = \frac{1}{2}(1 + 1 + 1 + 1) = 2.$$

Appendice. Caratteri di gruppi abeliani

Se G è un gruppo abeliano si pone $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$. Rispetto al prodotto puntuale $\widehat{G}$ è un gruppo, detto il *duale* di G. I suoi elementi sono i *caratteri* di G. Il carattere costantemente uguale ad 1 si dice il *carattere banale* e verrà indicato con 1. In questa sezione raccogliamo alcune delle proprietà fondamentali dei caratteri e dei duali.

Lemma 6.4.11 *Siano A, B gruppi.*

1. *Se A è ciclico finito allora $\widehat{A} \simeq A$.*
2. *$\widehat{A \oplus B} \simeq \widehat{A} \oplus \widehat{B}$.*
3. *Se A è finito allora $\widehat{\widehat{A}} \simeq A$.*

Dimostrazione. Se $A = \langle a \rangle$ ha ordine n e $\chi \in \widehat{A}$ allora $1 = \chi(a^n) = \chi(a)^n$ provando che $\chi(a) \in C_n = \langle e^{2\pi i/n} \rangle$ il gruppo delle radici n-esime di 1. Dato che ogni carattere è univocamente individuato da $\chi(a)$, la funzione $E : \widehat{A} \longrightarrow C_n$ definita da $E(\chi) = \chi(a)$ è un isomorfismo e quindi $\widehat{A} \simeq C_n \simeq A$.

In generale, per ogni gruppo C, $\mathrm{Hom}(A \oplus B, C) \simeq \mathrm{Hom}(A, C) \oplus \mathrm{Hom}(A, C)$ ed un isomorfismo è dato dalla mappa $\phi \longmapsto (\phi_{|A}, \phi_{|B})$, come si verifica facilmente. Infine, se A è finito, si può scrivere come somma diretta di ciclici $A = \oplus_{i=1}^k A_i$. Usando i punti precedenti otteniamo

$$\widehat{A} = \widehat{\oplus_{i=1}^k A_i} \simeq \oplus_{i=1}^k \widehat{A_i} \simeq \oplus_{i=1}^k A_i = A.$$

□

Come conseguenza abbiamo anche che, sempre per gruppi finiti, G è isomorfo a $\widehat{\widehat{G}}$. Questo isomorfismo si può descrivere in modo canonico. Per ogni $g \in G$ sia $\varepsilon_g : \widehat{G} \longrightarrow \mathbb{C}^*$ la funzione definita da $\varepsilon_g(\chi) = \chi(g)$. Si controlla immediatamente che $\varepsilon_g \in \widehat{\widehat{G}}$ e che la mappa che associa ad ogni g il carattere ε_g è un isomorfismo tra G e $\widehat{\widehat{G}}$.

Proposizione 6.4.12 *Siano G un gruppo abeliano finito, χ un suo carattere e $x \in G$. Allora*

$$\sum_{g \in G} \chi(g) = \begin{cases} 0 & \text{se } \chi \neq 1 \\ |G| & \text{se } \chi = 1 \end{cases} \qquad e \qquad \sum_{\phi \in \widehat{G}} \phi(x) = \begin{cases} 0 & \text{se } x \neq 1 \\ |G| & \text{se } x = 1 \end{cases}$$

DIMOSTRAZIONE. Se $\chi \neq 1$ c'è un $a \in G$ tale che $\chi(a) \neq 1$. Allora, osservando che ogni elemento di G si scrive in modo unico nella forma ag, otteniamo

$$\chi(a)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(a)\chi(g) = \sum_{g\in G}\chi(ag) = \sum_{g\in G}\chi(g)$$

e quindi $(\chi(a)-1)\sum_{g\in G}\chi(g) = 0$. Dato che $\chi(a) \neq 1$ deve essere $\sum_{g\in G}\chi(g) = 0$. Se $\chi = 1$ è ovvio che $\sum_{g\in G}\chi(g) = |G|$.

La seconda relazione si ottiene applicando la prima al gruppo $\widehat{G}$ ed al suo carattere $\varepsilon_x \in \widehat{\widehat{G}}$. □

Un importante proprietà dei caratteri è la seguente.

Proposizione 6.4.13 *Siano A un gruppo abeliano finito e B un suo sottogruppo. Allora ogni carattere di B si estende a $|A|/|B|$ distinti caratteri di A.*

Per la sua dimostrazione abbiamo bisogno di un lemma che è preferibile isolare.

Lemma 6.4.14 *Siano A un gruppo abeliano e B un suo sottogruppo ciclico. Supponiamo che, per ogni $1 \neq C \leq A$ si abbia $C \cap B \neq 1$. Allora A è ciclico.*

DIMOSTRAZIONE. Per ogni primo p che divide l'ordine di A, indichiamo con A_p il p-Sylow di A. Se ciascuno degli A_p è ciclico allora A è ciclico perché prodotto diretto di ciclici con ordini coprimi. Supponiamo per assurdo che, per almeno un primo p, A_p non sia ciclico. Allora A_p è isomorfo ad una somma diretta di ciclici dove compaiono almeno due fattori e possiamo scrivere $A_p = U \oplus V$ con U, V non banali. Per ipotesi $B \cap U$ e $B \cap V$ non sono banali e ciascuno di loro contiene un sottogruppo di ordine p. Se indichiamo tali sottogruppi con U_B, V_B abbiamo $U_B \cap V_B \leq U \cap V = 1$ e quindi, in particolare $U_B \neq V_B$. Questa è una contraddizione perché il gruppo ciclico B contiene un unico sottogruppo di ordine p. □

DIMOSTRAZIONE DELLA PROPOSIZIONE 6.4.13. Iniziamo provando l'esistenza di estensioni. Fissato un carattere $\chi \in \widehat{B}$ e detto K il suo nucleo, abbiamo che B/K è ciclico in quanto isomorfo a $\mathrm{Im}(\chi)$ un sottogruppo finito di $\mathbb{C}^*$. Poniamo $\overline{A} = A/K$ e indichiamo con $\overline{B}$ il suo sottogruppo B/K. Il carattere χ induce un carattere χ_0 di $\overline{B}$ definito da $\chi_0(bK) = \chi(b)$ (la verifica che questa sia una buona definizione è lasciata al lettore). Se ϕ_0 è una estensione di χ_0 ad $\overline{A}$ possiamo porre, per ogni $a \in A$, $\phi(a) = \phi_0(aK)$ ed osservare che ϕ è un carattere di A che estende χ. Pertanto è sufficiente concertarci su questa situazione e, senza perdere in generalità, si può assumere $K = 1$. Di conseguenza B è ciclico, diciamo di ordine m e, se $B = \langle b\rangle$, $\chi(b)$ è una radice m-esima primitiva di 1. L'insieme $\mathcal{C} = \{C \leq A \mid C \cap B = 1\}$ è non vuoto e possiamo dunque sceglierne un suo elemento massimale M. Con questa scelta ogni sottogruppo che contenga M propriamente deve intersecare B in modo non banale. Preso un sottogruppo non banale $R/M \leq A/M$ abbiamo

$$(R/M)\cap(BM/M) = (R\cap BM)/M = (R\cap B)M/M$$

e questo non è banale perché $R \cap B \neq 1$ visto che $R > M$. Per il Lemma 6.4.14 il gruppo A/M è ciclico, di ordine n, e ne scegliamo un generatore aM in modo che $(aM)^{n/m} = a^{n/m}M = bM$.

Possiamo ora prendere un numero complesso ε tale che $\varepsilon^{n/m} = \chi(b)$. Si controlla che tale complesso è una radice n-esima di 1 e quindi, ponendo $\psi(aM) = \varepsilon$, definiamo un carattere di A/M. A questo punto, se π indica la proiezione canonica di A su A/M, poniamo $\phi = \psi \circ \pi$. Questo è un morfismo da A in $\mathbb{C}^*$, quindi un elemento di $\widehat{A}$ e vogliamo vedere che è un'estensione di χ. A tal scopo sarà sufficiente mostrare che $\phi(b) = \chi(b)$. Usiamo la definizione:

$$\phi(b) = \psi(bM) = \psi((aM)^{n/m}) = \psi(aM)^{n/m} = \varepsilon^{n/m} = \chi(b)$$

come volevamo dimostrare. Una volta assodato che ogni carattere di B si estende, abbiamo che la funzione $\rho : \widehat{A} \longrightarrow \widehat{B}$ che associa ad ogni carattere la sua restrizione a B, è un morfismo suriettivo. L'ordine del nucleo ci dice in quanti modi ogni carattere di B si estende. Chiaramente $|\ker(\rho)| = |\widehat{A}|/|\widehat{B}| = |A|/|B|$ e questo conclude la dimostrazione. □ Chiudiamo la sezione con un ultimo fatto.

Proposizione 6.4.15 *Siano A un gruppo abeliano finito e B un suo sottogruppo. Se $G = A/B$ allora $\widehat{G}$ si può identificare con il gruppo*

$$K(G) = \{\chi \in \widehat{A} \mid \ker(\chi) \leq B\}.$$

Dimostrazione. Se π è la proiezione canonica di A su $G = A/B$, la funzione

$$\begin{aligned} f : \widehat{G} &\longrightarrow \widehat{A} \\ \chi &\longmapsto \chi \circ \pi \end{aligned}$$

è un morfismo ed è evidente che $\mathrm{Im}(f) = K(G)$. Viceversa, se $\chi \in K(G)$, possiamo definire la funzione $\phi_\chi : G = A/B \longrightarrow \mathbb{C}^*$ ponendo $\phi_\chi(aB) = \chi(a)$. Il lettore può controllare che questa è una buona definizione e che $\phi_\chi \in \widehat{G}$. La funzione

$$\begin{aligned} g : K(G) &\longrightarrow \widehat{G} \\ \chi &\longmapsto \phi_\chi \end{aligned}$$

è un morfismo di gruppi e $f \circ g = id_{K(G)}$, $g \circ f = id_{\widehat{G}}$. Ne segue che $\widehat{G}$ e $K(G)$ sono isomorfi, come richiesto. Inoltre ogni elemento χ di $\widehat{G}$ può essere interpretato come il carattere di A dato da $\chi \circ \pi$. □

Bibliografia

[1] Lars V. Ahlfors. *Complex analysis*. McGraw-Hill Book Co., New York, third edition, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics.

[2] H. Chatland and H. Davenport. Euclid's algorithm in real quadratic fields. *Canad. J. Math.*, 2:289–296, 1950.

[3] David A. Clark. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.*, 83(3-4):327–330, 1994.

[4] K. Inkeri. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Sci. Fennicae Ser. A. I. Math.-Phys.*, 1947(41):35, 1947.

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

[6] T. Nagell. The diophantine equation $x^2 + 7 = 2^n$. *Ark. Mat.*, 4:185–187, 1961.

[7] W. Narkiewicz. Euclidean algorithm in small abelian fields. *Funct. Approx. Comment. Math.*, 37(part 2):337–340, 2007.

[8] Pierre Samuel. About Euclidean rings. *J. Algebra*, 19:282–301, 1971.

[9] Daniel Segal. *Polycyclic groups*, volume 82 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1983.

[10] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[11] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. CRC Press, Boca Raton, FL, fourth edition, 2016.