Appunti di Teoria dei Numeri (algebra III)

Fabrizio Andreatta & Massimo Bertolini

9 gennaio 2017

1 Campi di numeri

Definizione 1.1. Un *campo di numeri* (detto anche campo di numeri algebrici) è un sottocampo K di $\mathbb{C}$ tale che $[K : \mathbb{Q}]$ sia finito.

Osservazione 1.2.

1) Se K è un campo di numeri, allora $K \subset \bar{\mathbb{Q}}$.

2) Inoltre, $\bar{\mathbb{Q}}$ è uguale al composto L di tutti i campi di numeri, cioè il più piccolo sottocampo di $\mathbb{C}$ contenente tutti i campi di numeri. L'inclusione $L \subset \bar{\mathbb{Q}}$ è chiara. Viceversa, se α è un elemento di $\bar{\mathbb{Q}}$, allora $\mathbb{Q}[\alpha]$ è un campo di numeri e quindi $L \supset \bar{\mathbb{Q}}$.

Esempio 1.3.

1) Sia $d \in \mathbb{Z} - \{0, 1\}$ un intero privo di fattori quadratici. Il *campo quadratico* $\mathbb{Q}[\sqrt{d}]$ è un campo di numeri.

2) Sia $\zeta_m = e^{2\pi i/m}$. L'*m-esimo campo ciclotomico* $\mathbb{Q}[\zeta_m]$ è un campo di numeri.

3) Dato $a \in \mathbb{Z}$ e $m \in \mathbb{N}$, i campi $\mathbb{Q}[a^{1/m}]$ e $\mathbb{Q}[a^{1/m}, \zeta_m]$ sono campi di numeri.

Teorema 1.4 (Teorema dell'elemento primitivo)**.** *Sia K/F un'estensione finita di sottocampi di $\mathbb{C}$. Esiste $\alpha \in K$ tale che $K = F[\alpha]$.*

Dim. Vedi [Mi], cap. 5. □

Corollario 1.5. *Se K è un campo di numeri, esiste $\alpha \in K$ tale che $K = \mathbb{Q}[\alpha]$.*

Esercizio 1.6.

1) Sia $K = \mathbb{Q}[2^{1/2}, 3^{1/2}]$. Trovare $\alpha \in K$ tale che $K = \mathbb{Q}[\alpha]$.

2) Sia $K = \mathbb{Q}[2^{1/2}, 3^{1/3}] \subset \mathbb{R}$. Trovare $\alpha \in K$ tale che $K = \mathbb{Q}[\alpha]$.

3) Sia $K = \mathbb{Q}[3^{1/2}, 5^{1/2}, (-7)^{1/2}]$. Trovare $\alpha \in K$ tale che $K = \mathbb{Q}[\alpha]$.

Teorema 1.7 (Grado dei campi ciclotomici)**.** *Sia $K = \mathbb{Q}[\zeta_m]$ l'm-esimo campo ciclotomico e sia $f_m(x)$ il polinomio minimo di ζ_m. Allora*

$$f_m(x) = \prod_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} (x - \zeta_m^k).$$

In particolare, $[K : \mathbb{Q}] = \varphi(m)$, dove $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$ indica la funzione di Eulero.

Dim. Vedi [Mi], cap. 5. □

Corollario 1.8. *Vi è un isomorfismo canonico*

$$\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times.$$

Dim. Un elemento σ in $\mathrm{Gal}(K/\mathbb{Q})$ è determinato dal suo valore $\sigma(\zeta_m)$. Poiché $\sigma(\zeta_m)$ è una radice primitiva m-esima di 1 (cioè ha ordine m), si ha $\sigma(\zeta_m) = \zeta_m^{k_\sigma}$, dove $k_\sigma \in (\mathbb{Z}/m\mathbb{Z})^\times$ è un'unità modulo m. Ne viene che $\sigma \mapsto k_\sigma$ è un omomorfismo iniettivo (canonico) di gruppi aventi, grazie al Teorema 1.7, lo stesso ordine. Dunque è un isomorfismo. □

Esercizio 1.9.

1) Se $m = \prod_{i=1}^k p_i^{a_i}$, dove p_i è primo e $a_i \in \mathbb{N}$, dimostrare che

$$\varphi(m) = \prod_{i=1}^k \varphi(p^{a_i}) = \prod_{i=1}^k (p_i - 1)p^{a_i - 1}.$$

[Suggerimento: applicare il Teorema Cinese del Resto a $\mathbb{Z}/m\mathbb{Z}$.]

2) Calcolare f_m (detto *m-esimo polinomio ciclotomico*) per $m \leq 21$. [Suggerimento: notare la formula induttiva

$$f_m(x) = \frac{x^m - 1}{\prod_{d|m, d \neq m} f_d(x)},$$

dove il prodotto è effettuato sui divisori positivi d di m, con $1 \leq d < m$.]

3) Descrivere la struttura di $\mathrm{Gal}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ per $m \leq 21$.

2 Interi algebrici

Definizione 2.1. Un numero complesso α è detto *intero algebrico* se soddisfa un polinomio monico a coefficienti in $\mathbb{Z}$.

Indichiamo con

$$\bar{\mathbb{Z}} = \{\alpha \in \mathbb{C} : \alpha \text{ è un intero algebrico}\}$$

l'insieme degli interi algebrici. Si noti l'inclusione $\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}$. Dato un campo di numeri K, indichiamo con $\mathcal{O}_K = K \cap \bar{\mathbb{Z}}$ l'insieme degli interi algebrici contenuti in K. Vedremo tra breve che $\mathcal{O}_K$ è un sottoanello di $\mathbb{C}$, detto *anello degli interi (algebrici)* di K.

Lemma 2.2. *Il polinomio minimo $p(x)$ in $\mathbb{Q}[x]$ di un intero algebrico α ha coefficienti in $\mathbb{Z}$.*

Dim. Sia $q(x)$ in $\mathbb{Z}[x]$ il polinomio monico a coefficienti in $\mathbb{Z}$ di grado minimo soddisfatto da α. Basta dimostrare che $q(x)$ è irriducibile. In caso contrario, vi è una fattorizzazione $q(x) = q_1(x)q_2(x)$, con $q_i(x) \in \mathbb{Q}[x]$ monico di grado ≥ 1. Per il lemma di Gauss, $q_i(x)$ appartiene a $\mathbb{Z}[x]$. Inoltre, α è radice di $q_1(x)$ o $q_2(x)$, contravvenendo la minimalità di $q(x)$. □

Corollario 2.3. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Dim. Dato α in $\mathcal{O}_{\mathbb{Q}}$, il suo polinomio minimo $x - \alpha$ ha coefficienti in $\mathbb{Z}$ grazie al Lemma 2.2. (L'inclusione opposta $\mathbb{Z} \subset \mathcal{O}_K$ è ovvia.) □

Proposizione 2.4. *Sia α in $\mathbb{C}$. Le seguenti condizioni sono equivalenti.*

1. *L'elemento α appartiene a $\bar{\mathbb{Z}}$.*
2. *Il gruppo additivo dell'anello $\mathbb{Z}[\alpha]$ (delle espressioni polinomiali in α a coefficienti in $\mathbb{Z}$) è un gruppo abeliano finitamente generato.*
3. *L'elemento α appartiene ad un sottoanello A di $\mathbb{C}$ il cui gruppo additivo è finitamente generato.*
4. *Esiste un sottogruppo non nullo finitamente generato di $\mathbb{C}$ tale che $\alpha A \subset A$.*

Dim. Vediamo che $1 \Rightarrow 2$. Sappiamo che vale la relazione

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Segue che α^n appartiene al gruppo generato da $1, \alpha, \ldots, \alpha^{n-1}$. Induttivamente, si vede che α^k appartiene allo stesso gruppo per ogni $k \geq n$. In conclusione $\{1, \ldots, \alpha^{n-1}\}$ generano $\mathbb{Z}[\alpha]$ come gruppo additivo.
Le implicazioni $2 \Rightarrow 3 \Rightarrow 4$ sono ovvie.
Dimostriamo infine che $4 \Rightarrow 1$. Supponiamo che A sia generato dai numeri complessi $(\alpha_1, \ldots, \alpha_n)$. La condizione $\alpha A \subset A$ implica che $\alpha\alpha_i = \sum_{j=1}^n a_{ij}\alpha_j$, per $i = 1, \ldots, n$, con $a_{ij} \in \mathbb{Z}$. In altre parole, vale la relazione matriciale

$$\alpha \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \tag{1}$$

dove $M = [a_{ij}]$ è una matrice $n \times n$ a coefficienti in $\mathbb{Z}$. Si noti che il vettore $(\alpha_i) \in \mathbb{C}^n$ è diverso da zero, poiché il gruppo A è non nullo per ipotesi. L'equazione (1) implica che α è un autovalore associato all'autovettore (α_i). Segue che α soddisfa il polinomio caratteristico $\det(xI - M)$, che è monico (di grado n) a coefficienti in $\mathbb{Z}$. □

Esercizio 2.5. Ricordiamo che dato un gruppo abeliano A, un sottoinsieme $\{a_1, \ldots, a_n\}$ di A è detto una $\mathbb{Z}$-base di A se per ogni $\alpha \in A$ esistono unici $\beta_1, \ldots, \beta_n \in \mathbb{Z}$ tali che

$$a = \beta_1 a_1 + \cdots + \beta_n a_n.$$

Mostrare che dato un intero algebrico α con polinomio minimo $f_\alpha(X) \in \mathbb{Q}[X]$ l'insieme $\{1, \ldots, \alpha^{n-1}\}$ è una $\mathbb{Z}$-base del gruppo additivo soggiacente all'anello $\mathbb{Z}[\alpha]$.

Corollario 2.6. *$\bar{\mathbb{Z}}$ e $\mathcal{O}_K$ sono sottoanelli di $\mathbb{C}$ (e di $\bar{\mathbb{Q}}$).*

Dim. L'affermazione su $\mathcal{O}_K$ segue da quella per $\bar{\mathbb{Z}}$. Dati α e β in $\bar{\mathbb{Z}}$, grazie alla condizione 2 della Proposizione 2.4, abbiamo

$$\mathbb{Z}[\alpha] = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m, \quad \mathbb{Z}[\beta] = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n.$$

Segue che $\mathbb{Z}[\alpha, \beta]$ è generato da $\alpha_i\beta_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$. Poiché $\alpha \pm \beta$ e $\alpha\beta$ appartengono a $\mathbb{Z}[\alpha, \beta]$, il Corollario 2.6 è conseguenza della condizione 3 della Proposizione 2.4. □

Esercizio 2.7.

1) Osservato che il numero complesso $\alpha = (-5)^{1/2} + 7^{1/2}$ è un intero algebrico, calcolare un polinomio monico con coefficienti in $\mathbb{Z}$ di cui α è radice.

2) Osservato che il numero reale $\alpha = 3^{1/2} + 5^{1/3}$ è un intero algebrico, calcolare un polinomio monico con coefficienti in $\mathbb{Z}$ di cui α è radice.

3) Calcolare il polinomio minimo di $3^{1/2} \cdot 5^{1/3}$.

4) Calcolare il polinomio minimo di $3^{1/2} + (-5)^{1/2} + 11^{1/2}$.

Esempio 2.8.

1) Se $K = \mathbb{Q}[\sqrt{d}]$, con $d \in \mathbb{Z} - \{0, 1\}$ privo di fattori quadratici, allora $\mathbb{Z}[\sqrt{d}]$ è contenuto in $\mathcal{O}_K$. Infatti, $\sqrt{d}$ appartiene a $\mathcal{O}_K$ poiché soddisfa $x^2 - d$; inoltre, poiché $\mathcal{O}_K$ è un sottoanello unitario di $\mathbb{C}$, deve contenere l'anello $\mathbb{Z}[\sqrt{d}]$ generato da $\sqrt{d}$. La Proposizione 2.9 descrive $\mathcal{O}_K$.

2) Se $K = \mathbb{Q}[\zeta]$, con $\zeta = e^{2\pi i/m}$, è l'm-esimo campo ciclotomico, si ha che $\mathbb{Z}[\zeta]$ è contenuto in $\mathcal{O}_K$. Infatti, ζ appartiene a $\mathcal{O}_K$ poiché soddisfa $x^m - 1$; inoltre, poiché $\mathcal{O}_K$ è un sottoanello unitario di $\mathbb{C}$, deve contenere l'anello generato da ζ. Vedremo più avanti che $\mathcal{O}_K$ è sempre uguale a $\mathbb{Z}[\zeta]$.

Proposizione 2.9. *Sia $K = \mathbb{Q}[\sqrt{d}]$ un campo quadratico, dove $d \in \mathbb{Z} - \{0, 1\}$ è un intero privo di fattori quadratici. Allora*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : \ a, b \in \mathbb{Z}\} & \text{se } d \equiv 2, 3 \pmod 4 \\ \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{\frac{a+b\sqrt{d}}{2} : \ a, b \in \mathbb{Z}, \ a \equiv b \pmod 2\} & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

Dim. Dato $\alpha \in K$, scriviamo $\alpha = a + b\sqrt{d}$, con a, b in $\mathbb{Q}$. Se $b = 0$, allora α appartiene a $\mathcal{O}_K$ se e solo se α appartiene a $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Se $b \neq 0$, il polinomio minimo di α è uguale a $x^2 - 2ax + (a^2 - db^2)$. Grazie al Lemma 2.2, otteniamo che

$$\alpha \in \mathcal{O}_K \quad \Leftrightarrow \quad 2a \in \mathbb{Z} \ \text{ e } \ a^2 - db^2 \in \mathbb{Z}. \tag{2}$$

Supponiamo che α è un elemento di $\mathcal{O}_K$. Si noti che se a appartiene a $\mathbb{Z}$, necessariamente b appartiene a $\mathbb{Z}$, poiché d è privo di fattori quadratici. Se invece $a \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$, allora si ha che $2a \equiv 1 \pmod 2$ e quindi $4a^2 \equiv 1 \pmod 4$. Poiché $4a^2 - 4db^2 \equiv 0 \pmod 4$, otteniamo che $4db^2 \equiv 1 \pmod 4$ e quindi $b \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$. Segue come sopra che $4b^2 \equiv 1 \pmod 4$ da cui $4db^2 \equiv d \pmod 4$ e quindi $d \equiv 1 \pmod 4$. In conclusione, si ha che $\mathcal{O}_K \subset \mathbb{Z}[\sqrt{d}]$ a meno che $d \equiv 1 \pmod 4$. Poiché $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$ grazie all'Esempio 2.8, otteniamo l'uguaglianza quando $d \equiv 2, 3 \pmod 4$. Se $d \equiv 1 \pmod 4$, i calcoli precedenti mostrano che $\mathcal{O}_K \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. L'inclusione opposta si verifica immediatamente usando le condizioni (2). □

3 Traccia, norma e discriminante

Introduciamo alcuni strumenti teorici utili, in particolare, per calcolare l'anello $\mathcal{O}_K$ degli interi algebrici di un campo di numeri.

Sia K/F un'estensione di campi di numeri (non necessariamente di Galois). Sappiamo che vi sono $n = [K : F]$ F-omomorfismi distinti

$$\sigma_1, \ldots, \sigma_n \colon K \longrightarrow \mathbb{C}$$

ed inoltre fattorizzano attraverso la chiusura Galoisiana E di $F \subset K$ in $\mathbb{C}$. Definisco $\underline{\sigma} \colon K \to \mathbb{C}^n$ l'omomorfismo di anelli $x \mapsto \big(\sigma_1(x), \ldots, \sigma_n(x)\big)$

Esercizio 3.1. Scriviamo $K = F(\alpha_1, \ldots, \alpha_h)$ e sia $f_{\alpha_i}(X) \in F[X]$ il polinomio minimo di α_i. Sia $f(X) := f_{\alpha_1}(X) \cdots f_{\alpha_h}(X)$ e definiamo $E \subset \mathbb{C}$ come il campo generato da F e da tutte le radici complesse di $f(X)$. Mostrare che

1) l'estensione $F \subset E$ è di Galois e contiene K;

2) ogni F-omomorfismo $\sigma \colon K \to \mathbb{C}$ fatorizza attraverso E.

Definizione 3.2. Data una n-pla $(\alpha_1, \ldots, \alpha_n)$ di elementi di K denoto con $A(\alpha_1, \ldots, \alpha_n)$ la matrice $[\sigma_i(\alpha_j)]_{1\leq i,j\leq n} \in \mathrm{M}_{n\times n}(\mathbb{C})$.

Il *discriminante* di $(\alpha_1, \ldots, \alpha_n)$ è definito da

$$\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n) = (\det A(\alpha_1, \ldots, \alpha_n))^2.$$

Osservazione 3.3. Dalle proprietà del determinante segue che $\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n)$ non dipende dall'ordine dei σ_i e degli α_j.

Proposizione 3.4.

1) Abbiamo $\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n) \in F$.

2) L'insieme $\{\alpha_1, \ldots, \alpha_n\}$ *è una* F*-base di* K *se e solo se* $\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n) \neq 0$ *se e solo se i vettori* $\underline{\sigma}(\alpha_1), \ldots, \underline{\sigma}(\alpha_n) \in \mathbb{C}^n$ *sono una* $\mathbb{C}$*-base.*

Dim.

1) Osserviamo che $\sigma_1, \ldots, \sigma_n$ fattorizzano attraverso una chiusura Galoisiana E di $F \subset K$. Sia G il gruppo di Galois $\mathrm{Gal}(E/F)$. Allora $\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n) \in F$ se e solo se $\sigma\big(\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n)\big) = \mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n)$ per ogni $\sigma \in G$.

Ma $\sigma\big(\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n)\big) = (\det[\sigma \circ \sigma_i(\alpha_j)]_{1\leq i,j\leq n})^2$. Poichè $\sigma_i \mapsto \sigma \circ \sigma_i$ induce una permutazione degli F-omomorfismi da K ad E, la matrice $[\sigma \circ \sigma_i(\alpha_j)]_{1\leq i,j\leq n}$ è ottenuta dalla matrice $[\sigma_i(\alpha_j)]_{1\leq i,j\leq n}$ permutando le righe e dunque le due matrici hanno uguale determinate a meno di segno. Prendendone il quadrato tale ambiguità scompare.

2) Abbiamo che $\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n) \neq 0$ se e solo se la matrice $A(\alpha_1, \ldots, \alpha_n) \in M_{n\times n}(E)$ ha rango massimo, ovvero le sue colonne $\underline{\sigma}(\alpha_1)^t, \ldots, \underline{\sigma}(\alpha_n)^t$ sono una base di $\mathbb{C}^n$ come $\mathbb{C}$-spazio vettoriale o equivalentemente di E^n come E-spazio vettoriale. Questo mostra la seconda equivalenza.

Visto che $\underline{\sigma}$ è un omomorfismo iniettivo di F-spazi vettoriali, $\{\alpha_1, \ldots, \alpha_n\}$ è una F-base di K se e solo se le colonne di $A(\alpha_1, \ldots, \alpha_n)$ sono linearmente indipendenti su F. Per concludere dobbiamo mostrare che questa è condizione necessaria e sufficiente affinchè siano linearmente indipendenti su E. Che sia condizione necessaria è chiaro. Per la sufficienza supponiamo che le colonne siano linearmente dipendenti su E ovvero che esista $a := (a_1, \ldots, a_n) \in E^n$ non nulla tale che $A(\alpha_1, \ldots, \alpha_n) \cdot a^t = 0$. Prendiamo a tale che il numero di entrate non nulle sia il minimo possibile. A meno di rinumerare gli α_i e riscalare a possiamo supporre che $a_1 = 1$. Per ogni automorfismo σ di E abbiamo che $\sigma(a) := \big(\sigma(a_1), \ldots, \sigma(a_n)\big)$ soddisfa ancora $A(\alpha_1, \ldots, \alpha_n) \cdot \sigma(a)^t = 0$. Infatti per ogni i abbiamo $\sum_j \sigma_i(\alpha_j)a_j = 0$ e quindi

$$\sum_j \big(\sigma \circ \sigma_i\big)(\alpha_j)\sigma(a_j) = \sigma\big(\sum_j \sigma_i(\alpha_j)a_j\big) = \sigma(0) = 0.$$

Ma $\sigma_i \mapsto \sigma\circ\sigma_i$ induce una biezione sugli F-omomorfismi di K in E. Dunque anche $A(\alpha_1, \ldots, \alpha_n)\cdot\sigma(a)^t = 0$ e $A(\alpha_1, \ldots, \alpha_n)\cdot\big(a-\sigma(a)\big)^t = 0$. Segue dalla minimalità

nella scelta di a che $a = \sigma(a)$. Valendo questo per ogni $\sigma \in G$ concludiamo che $a \in F^n$ e che $\sigma_1\big(\sum_i a_i\alpha_i\big) = \sum_i a_i\sigma_1(\alpha_i) = 0$ ovvero, essendo σ_1 iniettivo, che $\sum_i a_i\alpha_i = 0$, il che implica che $\{\alpha_1, \ldots, \alpha_n\}$ non è una F-base di K. □

Definiamo ora polinomio caratteristico, traccia e norma di un elemento di K relativamente ad F.

Definizione 3.5.

1) Denotiamo con $f^{\text{char}}_{\alpha,K/F}(X) \in F[X]$ il *polinomio caratteristico* dell'endomorfismo di K come F-spazio vettoriale definito dalla moltplicazione per α, che associa a $x \in K$ l'elemento $\alpha x \in K$.

2) La *traccia* di un elemento α di K è definita da

$$T_{K/F}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha).$$

3) La *norma* di un elemento α di K è definita da

$$N_{K/F}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

La dimostrazione del lemma seguente è immediata.

Lemma 3.6.

1. $T_{K/F}(\alpha + \beta) = T_{K/F}(\alpha) + T_{K/F}(\beta)$ e $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$ per ogni α e β in K.

2. $T_{K/F}(\alpha\beta) = \alpha T_{K/F}(\beta)$ e $N_{K/F}(\alpha\beta) = \alpha^n N_{K/F}(\beta)$ per ogni α in F e β in K.

Proposizione 3.7.

1. Per ogni α in K abbiamo $f^{\text{char}}_{\alpha,K/F}(X) = \prod_{i=1}^n \big(X - \sigma_i(\alpha)\big)$.

2. Per ogni α in K, $T_{K/F}(\alpha)$ è $-$ il coefficiente di X^{n-1} in $f^{\text{char}}_{\alpha,K/F}(X)$ e $N_{K/F}(\alpha)$ è $(-1)^n$ il coefficiente costante di $f^{\text{char}}_{\alpha,K/F}(X)$. In particolare, $T_{K/F}(\alpha)$ e $N_{K/F}(\alpha)$ appartengono a F.

3. Per ogni α in $\mathcal{O}_K$, abbiamo che $f^{\text{char}}_{\alpha,K/F}(X) \in \mathcal{O}_F[X]$. In particolare, $T_{K/F}(\alpha)$ e $N_{K/F}(\alpha)$ appartengono a $\mathcal{O}_F$.

Dim.

1. Sia $\mathcal{A} := \{\alpha_1, \ldots, \alpha_n\}$ una F-base di K. La matrice ${}_{\mathcal{A}}M_{\mathcal{A}}(\alpha)$ di moltiplicazione per α sull' F-spazio vettoriale K rispetto alla base $\mathcal{A}$ ha come colonna i-esima $(a_{1i}, \ldots, a_{ni})$ la n-upla tale che $\alpha\alpha_i = \sum_j a_{ji}\alpha_j$.

In particolare $\sigma_h(\alpha\alpha_i) = \sigma_h(\alpha)\sigma_h(\alpha_i) = \sum_j a_{ji}\sigma_h(\alpha_j)$ ovvero, in forma matriciale, posso calcolare $A(\alpha\alpha_1, \ldots, \alpha\alpha_n)$ come

$$A(\alpha\alpha_1, \ldots, \alpha\alpha_n) = \text{diag}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\big) \cdot A(\alpha_1, \ldots, \alpha_n)$$

oppure

$$A(\alpha\alpha_1, \ldots, \alpha\alpha_n) = A(\alpha_1, \ldots, \alpha_n) \cdot {}_{\mathcal{A}}M_{\mathcal{A}}(\alpha).$$

Qui $\mathrm{diag}(x_1, \ldots, x_n)$ denota la matrice diagonale con entrate $x_1, \ldots, x_n$. Segue dalla proposizione 3.4 che la matrice $A(\alpha_1, \ldots, \alpha_n)$ a coefficienti in $\mathbb{C}$ è invertibile e quindi

$$A(\alpha_1, \ldots, \alpha_n)^{-1} \cdot \mathrm{diag}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) \cdot A(\alpha_1, \ldots, \alpha_n) = {}_{\mathcal{A}}M_{\mathcal{A}}(\alpha).$$

La prima affermazione segue dal fatto che il polinomio caratteristico di una matrice è uguale a quello di una qualsiasi matrice ad essa coniugata per il teorema di Binet.

2. Questo segue immediatamente.

3. Osservo che se $\alpha \in \mathcal{O}_K$ allora ciascun $\sigma_i(\alpha) \in \mathcal{O}_E$ e quindi $f^{\mathrm{char}}_{\alpha,K/F}(X)$ ha coefficienti in $\mathcal{O}_E \cap F = \mathcal{O}_F$. □

Il seguente lemma presenta ulteriori importanti proprietà della norma.

Lemma 3.8.

1. Sia α in $\mathcal{O}_K$. Allora $N_{K/F}(\alpha) \in \alpha\mathcal{O}_K$.

2. Dato $\alpha \in K$ abbiamo $N_{K/F}(\alpha) = 0$ se e solo se $\alpha = 0$.

3. Dato $\alpha \in \mathcal{O}_K$ allora α è invertibile in $\mathcal{O}_K$ se se solo se $N_{K/F}(\alpha)$ è invertibile in $\mathcal{O}_F$.

Dim. Per definizione $N_{K/F}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.

1) Se $\sigma_1 \colon K \to E$ è l'inclusione naturale e poniamo $\beta = \prod_{i=2}^{n} \sigma_i(\alpha)$, allora $N_{K/F}(\alpha) = \alpha\beta$. Se $\alpha \neq 0$, segue che $\beta = N_{K/F}(\alpha)\alpha^{-1} \in K$ infatti $N_{K/F}(\alpha) \in F$. Inoltre ciascun $\sigma_i(\alpha) \in \mathcal{O}_E$ e quindi $\beta \in K \cap \mathcal{O}_E = \mathcal{O}_K$.

2) chiaro.

3) Usando la notazione di (1) ho che $\alpha\beta = N_{K/F}(\alpha)$. Quindi se $N_{K/F}(\alpha)$ è invertibile in $\mathcal{O}_F$ lo è anche in $\mathcal{O}_K$ e $\beta N_{K/F}(\alpha)^{-1} \in \mathcal{O}_K$ è l'inverso di α. Viceversa se α è invertibile in $\mathcal{O}_K$ esiste $\gamma \in \mathcal{O}_K$ tale che $\alpha\gamma = 1$. Applicando la moltiplicatività della norma otteniamo $N_{K/F}(\alpha)N_{K/F}(\gamma) = N_{K/F}(1) = 1$ con $N_{K/F}(\gamma) \in \mathcal{O}_F$ e dunque $N_{K/F}(\alpha) \in \mathcal{O}_F$ risulta invertibile in $\mathcal{O}_F$. □

Per il teorema dell'elemento primitivo sappiamo che $K = F[\alpha]$. In questo caso $f^{\mathrm{char}}_{\alpha,K/F}(X)$ è il polinomio minimo di α per questioni di gradi.

Proposizione 3.9. *Sia $K = F[\alpha]$ e sia $(1, \alpha, \ldots, \alpha^{n-1})$ la F-base di K associata ad α. Indichiamo con $f(x) \in F[x]$ il polinomio minimo di α su F e con $f'(x)$ la sua derivata. Allora*

$$\mathrm{disc}_{K/F}(1, \alpha, \ldots, \alpha^{n-1}) = \epsilon \cdot N_{K/F}(f'(\alpha)),$$

dove $\epsilon = 1$ se $n \equiv 0, 1 \pmod 4$ e $\epsilon = -1$ altrimenti.

Dim. Sia $A = [\sigma_i(\alpha^{j-1})]$ la matrice $n \times n$ che interviene nella definizione di $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$. Posto $\alpha_i = \sigma_i(\alpha)$, si noti che $A = [\alpha_i^{j-1}]$ è una matrice di Vandermonde. Di conseguenza, notando che $\epsilon = (-1)^{n(n-1)/2}$, si ha

$$\begin{aligned} \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) &= \det(A)^2 \\ &= \prod_{1 \le r < s \le n} (\alpha_s - \alpha_r)^2 \\ &= \epsilon \cdot \prod_{1 \le r \ne s \le n} (\alpha_r - \alpha_s). \end{aligned}$$

Basta ora dimostrare che

$$N_{K/\mathbb{Q}}(f'(\alpha)) = \prod_{1 \le r \ne s \le n} (\alpha_r - \alpha_s).$$

Abbiamo

$$\begin{aligned} N_{K/\mathbb{Q}}(f'(\alpha)) &= \prod_{r=1}^{n} \sigma_r(f'(\alpha)) \\ &= \prod_{r=1}^{n} f'(\alpha_r). \end{aligned}$$

Infine, la formula $f(x) = \prod_{s=1}^{n}(x - \alpha_s)$ implica che

$$f'(\alpha_r) = \prod_{s=1, r \ne s}^{n} (\alpha_r - \alpha_s).$$

□

Applichiamo la Proposizione 3.9 ai campi ciclotomici.

Corollario 3.10. *Sia p un primo dispari e sia $K = \mathbb{Q}[\zeta]$, con $\zeta = e^{2\pi i/p}$, il p-esimo campo ciclotomico. Allora*

$$\mathrm{disc}(1, \zeta, \ldots, \zeta^{p-2}) = \epsilon \cdot p^{p-2},$$

dove $\epsilon = 1$ se $p \equiv 1 \pmod 4$ e $\epsilon = -1$ se $p \equiv 3 \pmod 4$.

Dim. Per il Teorema 1.7, $[K : \mathbb{Q}] = p - 1$ e quindi $(1, \zeta, \ldots, \zeta^{p-2})$ è una $\mathbb{Q}$-base per K. Il polinomio minimo di ζ è dato da

$$\phi(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

La relazione $x^p - 1 = (x-1)\phi(x)$ implica che $p\,x^{p-1} = \phi(x) + (x-1)\phi'(x)$ e quindi

$$\phi'(\zeta) = \frac{p\zeta^{p-1}}{\zeta - 1} = \frac{p}{\zeta(\zeta - 1)}.$$

Posto $N = N_{K/\mathbb{Q}}$, la moltiplicatività della norma (Lemma 3.6) implica che

$$N(\phi'(\zeta)) = \frac{N(p)}{N(\zeta)N(\zeta-1)}.$$

Infine,

$$N(p) = p^{p-1}, \quad N(\zeta) = (-1)^{p-1} \cdot (\text{termine costante di } \phi(x)) = 1,$$

$$N(\zeta - 1) = N(-(1-\zeta)) = (-1)^{p-1}N(1-\zeta) = \phi(1) = p.$$

□

Applichiamo ora il Corollario 3.10 ad un problema già affrontato con mezzi diversi.

Corollario 3.11. *Sia $K = \mathbb{Q}[\zeta]$ il p-esimo campo ciclotomico, con $p \geq 3$ primo. Allora K contiene un unico sottocampo quadratico, uguale a $\mathbb{Q}[\sqrt{p}]$ se $p \equiv 1 \pmod 4$ e a $\mathbb{Q}[\sqrt{-p}]$ se $p \equiv 3 \pmod 4$.*

Dim. Il gruppo di Galois $\mathrm{Gal}(K/\mathbb{Q})$ è isomorfo a $\mathbb{F}_p^\times$ e quindi è ciclico di ordine $p-1$. Segue che $\mathrm{Gal}(K/\mathbb{Q})$ contiene un unico sottogruppo di indice 2, che fissa l'unico sottocampo quadratico di K. Inoltre, $\mathrm{disc}(1, \zeta, \ldots, \zeta^{p-2}) = \delta^2$, dove

$$\delta = \det[\sigma_i(\zeta^{j-1})]$$

è il determinante di una matrice a coefficienti in K. Segue che δ appartiene a K. Poiché $\delta^2 = \epsilon p^{p-1}$ per il Corollario 3.10, otteniamo che $\sqrt{\epsilon p}$ appartiene a K. □

Esercizio 3.12. Dato $d \in \mathbb{Z} - \{0, 1\}$ privo di fattori quadratici, si definisca $D = d$ se $d \equiv 1 \pmod 4$ e $D = 4d$ se $d \equiv 2, 3 \pmod 4$. Si dimostri che $\mathbb{Q}[\sqrt{d}]$ è contenuto nel D-esimo campo ciclotomico $\mathbb{Q}[e^{2\pi i/D}]$. [Suggerimento: si fattorizzi d (a meno del segno) come prodotto di primi; si osservi poi che $\mathbb{Q}[\sqrt{p}]$ è contenuto in $\mathbb{Q}[e^{2\pi i/4p}]$ se p è un primo $\equiv 3 \pmod 4$ ...]

4 Struttura additiva di $\mathcal{O}_K$

Sia K un campo di numeri. Intendiamo descrivere la struttura di $\mathcal{O}_K$ come gruppo additivo.

Definizione 4.1. Un gruppo abeliano A si dice *libero di rango $n \geq 0$* se A è isomorfo al gruppo additivo

$$\mathbb{Z}^n = \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}.$$

Esercizio 4.2. Due gruppi abeliani liberi sono isomorfi se e solo se hanno lo stesso rango. [Suggerimento: $(\mathbb{Z}/2\mathbb{Z})^n$ non è isomorfo a $(\mathbb{Z}/2\mathbb{Z})^m$ se $n \neq m$.]

Lemma 4.3. *Esiste una F-base $\{\alpha_1, \ldots, \alpha_n\}$ di K i cui elementi appartengono a $\mathcal{O}_K$.*

Dim. Se $\alpha \in K$ è un numero algebrico, allora α soddisfa un polinomio a coefficienti in $\mathbb{Z}$ (non necessariamente monico!)

$$a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0, \quad \text{con} \quad a_m \neq 0.$$

Segue (moltiplicando per a_m^{m-1}) che $a_m\alpha$ soddisfa il polinomio monico a coefficienti in $\mathbb{Z}$

$$x^m + a_{m-1}x^{m-1} + \ldots + a_m^{m-2}a_1 x + a_m^{m-1}a_0$$

e dunque $a_m\alpha$ appartiene ad $\mathcal{O}_K$. Di conseguenza, per ottenere la F-base richiesta è sufficiente moltiplicare gli elementi di una F-base arbitraria per un opportuno elemento non nullo di $\mathbb{Z}$. □

Proposizione 4.4. *Sia $\{\alpha_1, \ldots, \alpha_n\}$ una F-base per K costituita da interi algebrici e sia $d = \mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n)$ il suo discriminante. Allora*

1. *d appartiene a $\mathcal{O}_F - \{0\}$,*
2. *ogni intero algebrico α in $\mathcal{O}_K$ si scrive nella forma*

$$\alpha = \frac{m_1\alpha_1 + \ldots + m_n\alpha_n}{d},$$

dove i m_j appartengono a $\mathcal{O}_F$ e sono unici.

Dim.

Siano σ_i, $i = 1, \ldots, n$ gli omomorfismi di K in $\mathbb{C}$. Poiché (α_i) è una F-base di K, segue dalla proposizione 3.4 che la matrice $A = [\sigma_i(\alpha_j)]$ è invertibile. Posto $\delta = \det(A)$, si ha per costruzione $d = \delta^2$. Sappiamo quindi che $d \in F$ è non nullo. Inoltre, le componenti di A sono interi algebrici e dunque δ è un intero algebrico. Segue che d appartiene a $F \cap \bar{\mathbb{Z}} = \mathcal{O}_F - \{0\}$.

Dato $\alpha \in \mathcal{O}_K$, scriviamo $\alpha = \alpha_1 x_1 + \cdots + \alpha_n x_n$, con $x_i \in F$. Otteniamo il sistema lineare di n equazioni in n incognite

$$\sigma_i(\alpha_1)x_1 + \cdots + \sigma_i(\alpha_n)x_n = \sigma_i(\alpha), \quad i = 1, \ldots, n.$$

Per la regola di Kramer ho un'unica soluzione

$$x_j = \delta_j/\delta,$$

dove δ_j è il determinante della matrice ottenuta da A sostituendo la sua j-esima colonna con la colonna $(\sigma_i(\alpha))$ dei termini noti. Sappiamo che

$$\delta^2 = d, \quad \text{e} \quad \delta, \delta_j \in \bar{\mathbb{Z}}.$$

Segue che $m_j = dx_j = \delta_j \cdot \delta$ appartiene a $\bar{\mathbb{Z}} \cap F = \mathcal{O}_F$. Infine, m_j^2/d è uguale a $(dx_j)^2/d = dx_j^2 = d\delta_j^2/\delta^2 = \delta_j^2$. Di nuovo otteniamo che m_j^2/d appartiene a $\bar{\mathbb{Z}} \cap F = \mathcal{O}_F$. □

Teorema 4.5. *Sia $n = [K : \mathbb{Q}]$. Allora $\mathcal{O}_K$ è un gruppo abeliano libero di rango n.*

Dim. Sia $\mathcal{A}$ l'insieme delle n-uple $(\alpha_1, \ldots, \alpha_n)$ di elementi di $\mathcal{O}_K$ che formano una $\mathbb{Q}$-base di K. Grazie al Lemma 4.3 l'insieme $\mathcal{A}$ è non vuoto. Definiamo l'insieme

$$\{|\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)| \text{ t.c. } (\alpha_1, \ldots, \alpha_n) \in \mathcal{A}$$

Grazie alla Proposizione 4.4 si tratta di un insieme di numeri naturali, non nulli. Fissiamo $(\alpha_1, \ldots, \alpha_n) \in \mathcal{A}$ tale che $|\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)| = \min(I)$, realizza il minimo di I. Affermo che $\{\alpha_1, \ldots, \alpha_n\}$ è una $\mathbb{Z}$-base di $\mathcal{O}_K$ (Esercizio 2.5), dimostrando la tesi. Basta mostare che genera $\mathcal{O}_K$ in quanto $\{\alpha_1, \ldots, \alpha_n\}$ è linearmente indipendente su $\mathbb{Q}$ essendo una $\mathbb{Q}$-base di K.

Sia $\beta \in \mathcal{O}_K$ e scriviamo $\beta = a_1\alpha_1 + \ldots + a_n\alpha_n$ con $a_1, \ldots, a_n \in \mathbb{Q}$. Sia $J = \{i = 1, \ldots, n | a_i \notin \mathbb{Z}\}$. Devo mostrare che $J = \emptyset$. Supponiamo di no. Per ogni i scriviamo $b_i = a_i$ se a_i è un intero e poniamo b_i come il più grande intero $\leq a_i$ se $a_i \notin \mathbb{Z}$ ovvero $i \in J$. In particolare $a_i - b_i = 0$ se $i \notin J$ e $0 < a_i - b_i < 1$ se $i \in J$. Allora $\beta' = \sum_{i=1}^n (a_i - b_i)\alpha_i = \beta - \sum_{i=1}^n b_i\alpha_i$ è un elemento di $\mathcal{O}_K$ in quanto il sottogruppo generato da $\alpha_1, \ldots, \alpha_n$ è contenuto in $\mathcal{O}_K$. Inoltre $\beta' \neq 0$ visto che J è non vuoto. Supponiamo, a meno di rinumerare gli α_i, che $1 \in J$. Allora $|\mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \alpha_2, \ldots, \alpha_n)| = b_1^2 |\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)|$, per la definizione del discriminante come quadrato del determinate della matrice $A(\beta_1, \alpha_2, \ldots, \alpha_n)$ e perchè il determinante è n-lineare. Ma allora, visto che $0 < b_1 < 1$, segue che $0 \neq |\mathrm{disc}_{K/\mathbb{Q}}(\beta_1, \alpha_2, \ldots, \alpha_n)| < |\mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)|$ contraddicendo la minimalità di quest'ultimo. □

□

Definizione 4.6. Una *base intera* per $\mathcal{O}_K$ è una $\mathbb{Z}$-base di $\mathcal{O}_K$ ovvero un insieme di elementi $\{\alpha_1, \ldots, \alpha_n\}$ tale che

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Esempio 4.7. Sia dato $d \in \mathbb{Z} - \{0, 1\}$ privo di fattori quadratici e sia $K = \mathbb{Q}[\sqrt{d}]$ il campo quadratico corrispondente. Allora

$$\begin{cases} \{1, \sqrt{d}\} & \text{se } d \equiv 2, 3 \pmod 4 \\ \{1, \frac{1+\sqrt{d}}{2}\} & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

è una base intera per $\mathcal{O}_K$.

Lemma 4.8. *Due basi intere per $\mathcal{O}_K$ hanno lo stesso discriminante.*

Dim. Indicate le basi con $\mathcal{A} = (\alpha_i)$ e $\mathcal{B} = (\beta_i)$, abbiamo che

$$(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)\, M$$

dove $M = {}_{\mathcal{A}}M(\mathrm{Id}_{\mathcal{B}}$ è la matrice $n \times n$ a coefficienti in $\mathbb{Z}$ di cambiamento di base da $\mathcal{B}$ a $\mathcal{A}$. Scambiando il ruolo delle basi, otteniamo che M è invertibile e dunque $\det(M) = \pm 1$. Inoltre, posto $A = [\sigma_j(\alpha_i)]$ e $B = [\sigma_j(\beta_i)]$, vale la relazione

$$B = AM.$$

Segue che $\det(B) = \pm \det(A)$. Poiché $\mathrm{disc}(\mathcal{A}) = \det(A)^2$ e $\mathrm{disc}(\mathcal{B}) = \det(B)^2$, otteniamo l'uguaglianza dei discriminanti. □

Definizione 4.9. Chiamiamo *discriminante* di $\mathcal{O}_K$, indicato con $\mathrm{disc}(\mathcal{O}_K)$, il discriminante di una qualunque base intera di $\mathcal{O}_K$. (Si ricordi che $\mathrm{disc}(\mathcal{O}_K)$ appartiene a $\mathbb{Z}$, grazie alla Proposizione 4.4.)

Esercizio 4.10. L'insieme $(\alpha_1, \ldots, \alpha_n) \subset \mathcal{O}_K$ è una base intera per $\mathcal{O}_K$ se e solo se $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(\mathcal{O}_K)$.

Esercizio 4.11. Con notazioni come in Esempio 4.7, dimostrare che

$$\mathrm{disc}(\mathcal{O}_K) = \begin{cases} 4d & \text{se } d \equiv 2, 3 \pmod 4 \\ \\ d & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

(Di conseguenza, $\mathrm{disc}(\mathcal{O}_K)$ è uguale alla quantità D definita in Esercizio 3.12.)

Il prossimo risultato è utile per il calcolo dell'anello degli interi algebrici di certi campi di numeri.

Teorema 4.12. *Siano K ed L campi di numeri aventi grado su $\mathbb{Q}$ uguale a m ed n, rispettivamente. Sia M il campo composto KL. Supponiamo che*

$$[M : \mathbb{Q}] = mn.$$

Allora vale l'inclusione

$$\mathcal{O}_M \subset (1/d)\mathcal{O}_K\mathcal{O}_L,$$

dove $d = (\mathrm{disc}(\mathcal{O}_K), \mathrm{disc}(\mathcal{O}_L))$ è il massimo comun divisore di $\mathrm{disc}(\mathcal{O}_K)$ e $\mathrm{disc}(\mathcal{O}_L)$ e $\mathcal{O}_K\mathcal{O}_L$ è il sottoanello di KL generato da $\mathcal{O}_K$ e $\mathcal{O}_L$ (cioè l'anello i cui elementi sono somme finite del tipo $\sum \alpha\beta$, con α in $\mathcal{O}_K$ e β in $\mathcal{O}_L$).

Dim. Fissiamo basi intere $(\alpha_1, \ldots, \alpha_m)$ e $(\beta_1, \ldots, \beta_n)$ per $\mathcal{O}_K$ e $\mathcal{O}_L$, rispettivamente. Otteniamo che gli mn elementi $(\alpha_i\beta_j)$ di $\mathcal{O}_K\mathcal{O}_L$ formano

1. un sistema di generatori per $\mathcal{O}_K\mathcal{O}_L$,
2. una $\mathbb{Q}$-base per KL.

La prima affermazione segue dalla definizione di $\mathcal{O}_K\mathcal{O}_L$, mentre la seconda dipende dal fatto che $(\alpha_i\beta_j)$ è un sistema di generatori per il campo di numeri KL, il cui grado è mn per ipotesi. (Quanto detto implica che il gruppo additivo del sottoanello $\mathcal{O}_K\mathcal{O}_L$ di $\mathcal{O}_M$ è libero di rango mn e che $(\alpha_i\beta_j)$ è una $\mathbb{Z}$-base.)

Dato $\alpha \in \mathcal{O}_M$, lo scriviamo come

$$\alpha = \sum_{i,j} \frac{m_{i,j}}{r}\ \alpha_i\beta_j, \tag{3}$$

per unici $\frac{m_{i,j}}{r} \in \mathbb{Q}$ dove $m_{i,j}$ ed r appartengono a $\mathbb{Z}$ e $(r,\ m_{i,j})_{1\le i\le m, 1\le j\le n} = 1$. Dobbiamo mostrare che

$$r \mid \operatorname{disc}(\mathcal{O}_K) \quad \text{e} \quad r \mid \operatorname{disc}(\mathcal{O}_L).$$

Considerato il ruolo simmetrico di $\mathcal{O}_K$ e $\mathcal{O}_L$, ci basta controllare che r divide $\operatorname{disc}(\mathcal{O}_K)$. Siano $\sigma_k\colon K \longrightarrow \mathbb{C}$, $k = 1, \dots, m$ gli omomorfismi di K in $\mathbb{C}$. Poiché $[KL : L] = m$ per l'ipotesi $[KL : \mathbb{Q}] = mn$, il numero degli L-omomorfismi di KL in $\mathbb{C}$ è anch'esso m. L'applicazione che, dato un L-omomorfismo da KL in $\mathbb{C}$, associa la sua restrizione a K è iniettiva: se due restrizioni a K coincidono, devono coincidere su KL poiché coincidono su L per ipotesi. Quindi l'applicazione $\operatorname{Hom}_L(KL, \mathbb{C}) \to \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, che ad un L-omomorfismo $\tilde{\sigma}\colon KL \to \mathbb{C}$ associa la restrizione $\tilde{\sigma}|_K\colon K \to \mathbb{C}$ a K, è una biezione essendo una applicazione iniettiva fra due insiemi entrambi di cardinalità m. Concludo che per ogni $k = 1, \dots, m$ esiste un unico L-omomorfismo $\tilde{\sigma}_k\colon KL \to \mathbb{C}$ la cui restrizone a K coincide con σ_k.

Otteniamo l'uguaglianza delle matrici $\big(\sigma_k(\alpha_i)\big)_{k,i} = \big(\tilde{\sigma}_k(\alpha_i)\big)_{k,i}$ e l'uguaglianza $\operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_m) = \operatorname{disc}_{M/L}(\alpha_1, \dots, \alpha_m)$. Segue allora dalla Proposizione 4.4 che

$$\operatorname{disc}(\mathcal{O}_K)\alpha \in \mathcal{O}_L\alpha_1 + \cdots + \mathcal{O}_L\alpha_m = \sum_{1\le i\le m, 1\le j\le n} \mathbb{Z}\alpha_i\beta_j.$$

Quindi $(\operatorname{disc}(\mathcal{O}_K)m_{i,j})/r$ appartiene a $\mathbb{Z}$, cioè r divide $\operatorname{disc}(\mathcal{O}_K)m_{i,j}$ per ogni (i, j). Poiché per ipotesi $(m_{i,j}, r)_{i,j} = 1$, concludiamo che $r \mid \operatorname{disc}(\mathcal{O}_K)$. □

Il seguente corollario è immediato.

Corollario 4.13. *Se* $(\operatorname{disc}(\mathcal{O}_K), \operatorname{disc}(\mathcal{O}_L)) = 1$, *allora* $\mathcal{O}_M = \mathcal{O}_K\mathcal{O}_L$.

Esercizio 4.14. Sia K il *campo biquadratico* $\mathbb{Q}[\sqrt{-3}, \sqrt{11}]$. Calcolare $\mathcal{O}_K$.

Teorema 4.15. *Sia* $K = \mathbb{Q}[\zeta]$, *con* $\zeta = e^{2\pi i/m}$, *l'*m*-esimo campo ciclotomico. Allora* $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Dim.

Passo 1: Sia $m = m_1 m_2$, con $(m_1, m_2) = 1$, e sia $K_i = \mathbb{Q}[\zeta_i]$, $i = 1, 2$, l'm_i-esimo campo ciclotomico. Se $\mathcal{O}_{K_i} = \mathbb{Z}[\zeta_i]$ per $i = 1, 2$, allora $\mathcal{O}_K = \mathbb{Z}[\zeta]$. Questa affermazione segue dal Corollario 4.13, osservando quanto segue:

1. $K = K_1 K_2$, poiché $\zeta_1 \zeta_2$ è una radice primitiva m-esima di 1, e vale l'uguaglianza $[K : \mathbb{Q}] = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]$ (**esercizio**);

2. $(\mathrm{disc}(\mathcal{O}_{K_1}), \mathrm{disc}(\mathcal{O}_{K_2})) = 1$: questa affermazione segue dal lemma seguente.

Lemma 4.16. *Se $K = \mathbb{Q}[\zeta]$ è l'm-esimo campo ciclotomico, allora* $\mathrm{disc}(\mathcal{O}_K)$ *divide $m^{\varphi(m)}$.*

Dim. Grazie all'Esempio 2.8, $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$. Abbiamo che $(1, \zeta, \ldots, \zeta^{\varphi(m)-1})$ è una base intera di $\mathbb{Z}[\zeta]$. Indichiamo per brevità il suo discriminante con $\mathrm{disc}(\zeta)$. Allora $\mathrm{disc}(\mathcal{O}_K)$ divide $\mathrm{disc}(\zeta)$ (**esercizio**: vedi la dimostrazione del Lemma 4.8). Posto $x^m - 1 = f(x)g(x)$, dove $f(x) = f_m(x)$ è l'm-esimo polinomio ciclotomico (cioè il polinomio minimo di ζ), differenziando e sostituendo x con ζ, si ottiene

$$m = \zeta f'(\zeta) g(\zeta).$$

Calcolando $N_{K/\mathbb{Q}}$ su questa uguaglianza, otteniamo grazie alla Proposizione 3.9

$$m^{\varphi(m)} = \pm \mathrm{disc}(\zeta) N_{K/\mathbb{Q}}(\zeta g(\zeta)).$$

Poiché $\zeta g(\zeta)$ è un intero in $\mathcal{O}_K$, segue che $N_{K/\mathbb{Q}}(\zeta g(\zeta))$ appartiene a $\mathbb{Z}$ grazie alla Proposizione 3.7. Otteniamo che $\mathrm{disc}(\zeta)$ divide $m^{\varphi(m)}$. □

Passo 2: Grazie al Passo 1, basta ora dimostrare il Teorema 4.15 nel caso in cui $m = p^h$ sia uguale alla potenza di un primo e quindi $\zeta = e^{2\pi i/p^h}$.

Premettiamo un lemma.

Lemma 4.17.

1. Abbiamo $\mathbb{Z}[\zeta] = \mathbb{Z}[1 - \zeta]$ e $\mathrm{disc}(\zeta) = \mathrm{disc}(1 - \zeta)$.

2.

$$\prod_{k \in (\mathbb{Z}/p^h\mathbb{Z})^\times} (1 - \zeta^k) = p.$$

Dim. Poiché $\zeta = 1 - (1 - \zeta)$, $\mathbb{Z}[\zeta]$ è uguale a $\mathbb{Z}[1 - \zeta]$. Da questa uguaglianza segue l'uguaglianza dei discriminanti (**esercizio**). (Si noti che queste affermazioni non dipendono dal fatto che m è una potenza di p.) Il prodotto nella seconda parte è uguale a $f_{p^h}(1)$, dove

$$f_{p^h}(x) = \frac{x^{p^h} - 1}{x^{p^{h-1}} - 1} = 1 + x^{p^{h-1}} + x^{2(p^{h-1})} + \cdots + x^{(p-1)p^{h-1}}$$

è il p^h-esimo polinomio ciclotomico. □

Posto $n = \varphi(p^h) = (p-1)p^{h-1}$ e $d = \mathrm{disc}(\zeta) = \mathrm{disc}(1-\zeta)$, la Proposizione 4.4 implica che ogni α in $\mathcal{O}_K$ si scrive nella forma

$$\alpha = \frac{m_1 + m_2(1-\zeta) + \cdots + m_n(1-\zeta)^{n-1}}{d} \ . \tag{4}$$

Dobbiamo dimostrare che $\mathcal{O}_K = \mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$. Se $\mathcal{O}_K \neq \mathbb{Z}[1-\zeta]$, esiste α come sopra tale che non tutti gli m_i sono divisibili per d. In questo caso, poichè d è una potenza di p grazie al Lemma 4.16, $\mathcal{O}_K$ contiene un elemento β della forma

$$\beta = \frac{m_i(1-\zeta)^{i-1} + \cdots + m_n(1-\zeta)^{n-1}}{p} \ , \tag{5}$$

dove m_i non è divisibile per p. Il Lemma 4.17 implica che $p/(1-\zeta)^n$ appartiene a $\mathbb{Z}[\zeta]$, notando che $1-\zeta^k$ è divisibile in $\mathbb{Z}[\zeta]$ per $1-\zeta$. Segue che $p/(1-\zeta)^i$ appartiene a $\mathbb{Z}[\zeta]$ e quindi $\beta p/(1-\zeta)^i$ appartiene a $\mathcal{O}_K$. Usando l'espressione (5) per β, otteniamo che $m_i/(1-\zeta)$ appartiene a $\mathcal{O}_K$. Questo è impossibile perchè $N_{K/\mathbb{Q}}(m_i) = m_i^n$ non è divisibile per p, mentre $N_{K/\mathbb{Q}}(1-\zeta) = p$ grazie al Lemma 4.17, da cui segue che $N_{K/\mathbb{Q}}(m_i/(1-\zeta))$ non appartiene a $\mathbb{Z}$, contro la Proposizione 3.7. □

5 Domini di Dedekind

Questo capitolo si occupa della struttura di anello di $\mathcal{O}_K$. L'osservazione preliminare è che in generale $\mathcal{O}_K$ non è un UFD.

Esempio 5.1. Sia $K = \mathbb{Q}[\sqrt{-5}]$ e sia $N = N_{K/\mathbb{Q}}$. Poiché $-5 \equiv 3 \pmod 4$, si ha $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Si consideri la fattorizzazione

$$2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}). \tag{6}$$

Abbiamo $N(2) = 4$, $N(3) = 9$ e $N(1 \pm \sqrt{-5}) = 6$. Se u è un'unità in $\mathcal{O}_K^\times$, allora

$$N(u) = 1.$$

Infatti, se u^{-1} appartiene a $\mathcal{O}_K$, $N(u)$ e $N(u^{-1})$ appartengono a $\mathbb{Z}$; inoltre, $1 = N(1) = N(uu^{-1})$. Segue che $N(u) = \pm 1$. Infine, si ha

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 \tag{7}$$

è ≥ 0 per ogni a, b in $\mathbb{Z}$. Sulla base di questa osservazione e tenuto conto della moltiplicatività della norma, per dimostrare che $\mathcal{O}_K$ non è un UFD basta osservare che $\mathcal{O}_K$ non contiene elementi di norma 2 e 3. Considerata (7), questa affermazione è conseguenza immediata del fatto evidente che le equazioni

$$a^2 + 5b^2 = 2, \quad a^2 + 5b^2 = 3$$

non hanno soluzioni in $\mathbb{Z}$. Segue allora che 2, 3 e $1 \pm \sqrt{-5}$ sono irriducibili e quindi (6) contraddice il principio di fattorizzazione unica.

Esercizio 5.2.

1) Dato un campo quadratico $K = \mathbb{Q}[\sqrt{d}]$, con $d \in \mathbb{Z} - \{0, 1\}$ privo di fattori quadratici, dimostrare che u è un'unità di $\mathcal{O}_K^\times$ se e solo se $u \in \mathcal{O}_K$ e $N_{K/\mathbb{Q}}(u) = \pm 1$.

2) Se $d < 0$ (in questo caso diciamo che K è una *campo quadratico immaginario o complesso*), dimostrare che $\mathcal{O}_K^\times = \{\pm 1\}$ a meno che non sia $d = -1$ o $d = -3$. Se $d = -1$, dimostrare che $\mathcal{O}_K^\times = \{\zeta \in \mathbb{C} : \zeta^4 = 1\}$. Se $d = -3$, dimostrare che $\mathcal{O}_K^\times = \{\zeta \in \mathbb{C} : \zeta^6 = 1\}$.

3) Mostrare con un esempio che se $d > 0$ (in questo caso diciamo che K è un *campo quadratico reale*)il gruppo $\mathcal{O}_K^\times$ può non essere di torsione. (E' un fatto non banale che $\mathcal{O}_K^\times$ non è mai di torsione se K è un campo quadratico reale.)

4) Dimostrare che nell'affermazione del punto 1 K può essere sostituito da un qualunque campo di numeri.

L'esempio precedente suggerisce di cercare un sostituto per la proprietà di fattorizzazione unica degli elementi valida per $\mathbb{Z} = \mathcal{O}_\mathbb{Q}$. Si noti che ogni ideale non nullo $n\mathbb{Z}$ di $\mathbb{Z}$ può essere fattorizzato in modo unico come prodotto di ideali massimali:

$$n\mathbb{Z} = p_1\mathbb{Z} \cdots p_k\mathbb{Z}.$$

Vedremo come l'analogo di questa proprietà si generalizzi a qualunque anello di numeri $\mathcal{O}_K$, come conseguenza del fatto che $\mathcal{O}_K$ è un dominio di Dedekind.

Definizione 5.3. Un dominio di integrità R è detto *dominio di Dedekind* se valgono le condizioni seguenti:

1. R è noetheriano cioè ogni ideale di R è finitamente generato,
2. ogni ideale primo non nullo di R è massimale,
3. R è integralmente chiuso nel suo campo delle frazioni.

La condizione 3 significa che ogni elemento del campo delle frazioni di R che soddisfa un polinomio monico a coefficienti in R appartiene ad R.

Teorema 5.4. *Ogni anello $\mathcal{O}_K$ è un dominio di Dedekind.*

Dim. Se I è un ideale di $\mathcal{O}_K$, si ha che il gruppo additivo di I è un sottogruppo del gruppo additivo di $\mathcal{O}_K$. Dato $\alpha \in I$ non nullo abbiamo che

1. $0 \neq N_{K/\mathbb{Q}}(\alpha) \in \mathcal{O}_K\alpha$ grazie al Lemma 3.8;
2. $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ grazie alla Proposizione 3.7.

Per il Teorema 4.5 l'anello $\mathcal{O}_K$, e quindi anche $N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K$, è un gruppo abeliano libero di rango $n = [K : \mathbb{Q}]$ e

$$\mathcal{O}_K/N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K \cong \left(\mathbb{Z}/N_{K/\mathbb{Q}}(\alpha)\mathbb{Z}\right)^n$$

è un gruppo finito. Visto che $N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K \subset \alpha\mathcal{O}_K \subset I$ anche $I/N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K$ è un gruppo finito in quanto sottogruppo di $\mathcal{O}_K/N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K$. Quindi anche I è un gruppo abeliano senza torsione in quanto contenuto in $\mathcal{O}_K$. Inoltre è fintamente generato: un insieme di generatori è dato ad esempio da un numero finito di generatori di $N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K$ come gruppo abeliano e da rappresentanti delle classi di $I/N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K$. Dunque a maggior ragione I è un ideale finitamente generato. Questo mostra che $\mathcal{O}_K$ soddisfa la condizione (1) della Definizione 5.3.

Riguardo alla condizione 2, sia $\mathcal{P}$ un ideale primo non nullo di $\mathcal{O}_K$. Occorre mostrare che $\mathcal{P}$ è massimale, cioè che $\mathcal{O}_K/\mathcal{P}$ è un campo. Sappiamo che $\mathcal{O}_K/\mathcal{P}$ è un dominio di integrità. Segue dal ragionamento al punto (1) che, dato $0 \neq \alpha \in \mathcal{P}$ l'anello $\mathcal{O}_K/\mathcal{P}$ è quoziente dell'anello finito $\mathcal{O}_K/N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K$ e quindi anche $\mathcal{O}_K/\mathcal{P}$ è finito. Concludiamo che $\mathcal{O}_K/\mathcal{P}$ è necessariamente un campo.

Infine verifichiamo la condizione 3. Si noti che K è il campo delle frazioni di $\mathcal{O}_K$ (vedere la dimostrazione del Lemma 4.3). Sia $\alpha = a/b$ con a, b in $\mathcal{O}_K$ un elemento di K. Supponiamo che α soddisfi il polinomio monico

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

a coefficienti a_i in $\mathcal{O}_K$. Segue che il gruppo additivo dell'anello $\mathcal{O}_K[\alpha]$ è finitamente generato su $\mathcal{O}_K$. Poiché $\mathcal{O}_K$ è finitamente generato su $\mathbb{Z}$ per il Teorema 4.5, segue che $\mathcal{O}_K[\alpha]$ è finitamente generato su $\mathbb{Z}$. La condizione 3 della Proposizione 2.4 garantisce che α appartiene a $\overline{\mathbb{Z}}$. Poichè α appartiene a K, segue che α appartiene a $\mathcal{O}_K$. □

Sia I un ideale non nullo di $\mathcal{O}_K$. Segue del Teorema 5.4 che l'anello quoziente $\mathcal{O}_K/I$ è finito. La sua cardinalità è chiamata la *norma* di I e viene denotata come $N_{K/\mathbb{Q}}(I)$.

Esercizio 5.5. * Mostrare che dato $0 \neq \alpha \in \mathcal{O}_K$ e definito I come l'ideale principale (α), allora $N_{K/\mathbb{Q}}(I) = |N_{K/\mathbb{Q}}(\alpha)|$ (SUGG: segue dalla Proposizione 3.7 che $N_{K/\mathbb{Q}}(\alpha)$ è, a meno di segno, il determinante della matrice dell'operatore moltiplicazione per α su $\mathcal{O}_K$ rispetto ad una base intera di $\mathcal{O}_K$. D'altra parte $N_{K/\mathbb{Q}}(I)$ è la cardinalità del quoziente $\mathcal{O}_K/\alpha\mathcal{O}_K$ di tale operatore.)

Esercizio 5.6. Sia R un anello commutativo con unità. Si dimostri che le seguenti condizioni sono equivalenti:

1) R è noetheriano (cioè ogni suo ideale è finitamente generato).

2) Ogni successione crescente

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

di ideali di R è definitivamente costante.

3) Ogni insieme non vuoto $\mathcal{S}$ di ideali di R ha un elemento massimale (cioè esiste $M \in \mathcal{S}$ – non necessariamente unico – tale che $M \subset I \in \mathcal{S}$ implica $M = I$).

(Suggerimento: per 1) $\Rightarrow$ 2), considerare l'ideale $\cup_n I_n$; per 2) $\Rightarrow$ 3), costruire un'opportuna successione crescente di ideali; per 3) $\Rightarrow$ 1), dato un ideale I, considerare l'insieme degli ideali finitamente generati contenuto in I.)

L'obiettivo che ci poniamo ora è dimostrare che in un dominio di Dedekind ogni ideale non nullo è prodotto di ideali primi non nulli (cioè massimali).

Terminologia e notazioni: Nella parte rimanente di questo capitolo, R indicherà sempre un dominio di Dedekind. Inoltre, per *ideale* intenderemo sempre un ideale proprio non nullo; per *primo* indenderemo sempre un ideale proprio, primo e non nullo.

Lemma 5.7. *Ogni ideale di R contiene un prodotto di primi.*

Dim. Sia $\mathcal{S}$ l'insieme degli ideali di R che non contengono un prodotto di primi. Se $\mathcal{S}$ è non vuoto, allora $\mathcal{S}$ contiene un elemento massimale M. L'ideale M non è primo, poiché appartiene a $\mathcal{S}$. Segue che esistono elementi $a, b \in R - M$ tali che $ab \in M$. Gli ideali $M + aR$ e $M + bR$ contengono propriamente M e dunque non appartengono a $\mathcal{S}$. Segue che contengono prodotti di primi. Ma allora questo vale per

$$(M + aR)(M + bR) \subset M,$$

assurdo. □

Lemma 5.8. *Sia K il campo delle frazioni di R, e sia $I \subsetneq R$ un ideale proprio. Allora esiste $x \in K - R$ tale che $xI \subset R$.*

Dim. Sia $a \in I - \{0\}$. Grazie al Lemma 5.7, esistono primi $P_1, \ldots, P_r$ tali che

$$P_1 \cdots P_r \subset aR. \tag{8}$$

Supponiamo che r sia minimo rispetto alla proprietà (8). Fissiamo un primo P tale che $I \subset P$. (Sappiamo che l'ideale massimale P esiste grazie al Lemma di Zorn.) Segue che P contiene $P_1 \cdots P_r$, e quindi $P \supset P_i$ per qualche i. (Altrimenti, trovo per ogni i un elemento $a_i \in P_i - P$; ma $a_1 \cdots a_r \in P$, impossibile.) Posso supporre che $P \supset P_1$. Essendo P e P_1 massimali, ho che

$$P = P_1.$$

Per la minimalità di r, posso scegliere

$$b \in P_2 \cdots P_r - aR.$$

Infine, pongo $x = b/a \in K$. Noto che $x \notin R$, altrimenti avrei che b appartiene ad aR. Infine, affermiamo che $xI \subset R$. Ciò è equivalente ad affermare che $bI \subset aR$. Questo segue dalla catena di inclusioni

$$bI \subset bP_1 \subset P_1 \cdots P_r \subset aR,$$

dove la seconda inclusione segue dal fatto che b appartiene a $P_2 \cdots P_r$. □

Proposizione 5.9. *Dato un ideale I di R, esiste un ideale J di R tale che IJ è principale.*

Dim. Fissato $a \in I - \{0\}$, definiamo

$$J = \{b \in R : bI \subset aR\}.$$

E' chiaro che J è un ideale di R (non nullo perchè a appartiene a J) e che $IJ \subset aR$. Affermiamo che

$$IJ = aR.$$

(Dunque il risultato che dimostriamo è più preciso dell'enunciato della Proposizione 5.9, in quanto mostra come definire J.) Consideriamo l'insieme

$$L = a^{-1}IJ.$$

E' contenuto in R, poiché $IJ \subset aR$. Inoltre, si tratta chiaramente di un ideale. La nostra affermazione equivale a dire che

$$L = R.$$

In caso contrario, L è un ideale proprio e dunque, grazie al Lemma 5.8, esiste $x \in K - R$ tale che $xL \subset R$. Dimostreremo che x è radice di un polinomio monico a coefficienti in R. Poiché x appartiene a K e R è integralmente chiuso in K, otteniamo che x appartiene a R, una contraddizione. Notiamo anzitutto che

$$J \subset L.$$

Infatti, questo equivale a dire che $aJ \subset IJ$, vero perchè $a \in I$. Segue che

$$xJ \subset xL \subset R.$$

Vale l'inclusione

$$xJ \subset J.$$

Tenuto conto della definizione di J, bisogna verificare che

$$(xJ)I = xIJ \subset aR.$$

Ciò equivale al fatto (noto!) che $xL = x(a^{-1}IJ) \subset R$. Indichiamo ora con $\alpha_1, \ldots, \alpha_n$ un insieme di generatori di J, cioè

$$J = R\alpha_1 + \ldots + R\alpha_n.$$

Otteniamo la relazione

$$x \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \tag{9}$$

dove $M = [a_{ij}]$ è una matrice $n \times n$ a coefficienti in R. Si noti che il vettore $(\alpha_i) \in R^n$ è diverso da zero, poiché L è non nullo. L'equazione (9) implica che x è un autovalore associato all'autovettore (α_i), e quindi soddisfa il polinomio caratteristico $\det(tI - M)$, che è monico (di grado n) a coefficienti in R. (Si noti che questo argomento ricalca la dimostrazione di una parte della Proposizione 2.4.)

□

Definizione 5.10. Definisco *ideale frazionario* di R un R-sottomodulo del campo delle frazioni $\mathrm{Frac}(R)$ di R, non nullo e finitamente generato

Dico che un ideale frazionario M è principale se è generato da un elemento.

Lemma 5.11.

1. Gli ideali frazionari di R sono tutti e soli i sottomoduli di $\mathrm{Frac}(R)$ *delle forma* $xI := \{xi | i \in I\}$ *con* $x \in \mathrm{Frac}(R)$ *non nullo e* $I \subset R$ *un ideale.*

2. Se M è un ideale frazionario ed $N \subseteq M$ è un sottomodulo non nullo, allora anche N è un ideale farzionario.

Dim. (1) Siccome R è noethariano, ogni ideale $I \subset R$ è finitamente genrato. Quindi, dato $x \in \mathrm{Frac}(R)$ non nullo, xI è un R-sottomodulo di $\mathrm{Frac}(R)$ finitamente generato in quanto immagine di I tramite l'omomorfismo di R-moduli $\mathrm{Frac}(R) \to \mathrm{Frac}(R)$ dato da $i \mapsto xi$.

Viceversa dato $M \subset \mathrm{Frac}(R)$ un R-sottomodulo non nullo con un numero finito di generatori, diciamo $\alpha_1, \ldots, \alpha_n$, allora possiamo scrivere ciascun $\alpha_i = a_i b_i^{-1}$ con a_i e $b_i \in R$ e b_i non nullo. Sia $b = b_1 \cdots b_n$. È un elemento non nullo di R. L'immagine bM di M tramite l'omomorfismo di R-moduli $\mathrm{Frac}(R) \to \mathrm{Frac}(R)$, $m \mapsto bm$, è un R-sottomodulo di R ovvero un ideale, chiamiamolo I. Concludo che $M = xI$ con $x = b^{-1}$.

(2) Scrviamo $M = xI$ come in (1). Allora $x^{-1}N$ è un R-sottomodulo di $\subset x^{-1}M = I$ e quindi di R, ovvero è un ideale non nullo J di R. Segue che $N = xJ$ e la conclusione segue da (1). □

Definizione 5.12. Sia $\mathcal{I}(R)$ l'insieme degli ideali frazionari di R.

1. Dati $(M, N) \in \mathcal{I}(R) \times \mathcal{I}(R)$ definisco $M \cdot N$ l' R-sottomodulo $M \cdot N$ di $\mathrm{Frac}(R)$ generato dagli elementi della forma mn con $m \in M$ ed $n \in N$;

2. dato $M \in \mathcal{I}(R)$ definisco M^{-1} l' R-sottomodulo $M^{-1} := \{x \in \mathrm{Frac}(R) | xm \in R \forall m \in M\}$ di $\mathrm{Frac}(R)$;

3. pongo $\mathbf{1} = R$.

Proposizione 5.13.

1. l'insieme $\mathcal{I}(R)$, con le operazioni sopra definite e con elemento neutro $\mathbf{1}$*, risulta essere un gruppo abeliano.*

2. Il sottoinsieme $\mathcal{P}(R) \subset \mathcal{I}(R)$ degli ideali farzionari principali è un sottogruppo

Dim. (1) (a) Verifico che il prodotto $M \cdot N$ di due ideali frazionari risulta essere ancora un ideale frazionario. Si tratta ancora di un modulo non nullo. Inoltre è finitamente generato: se $\alpha_1, \ldots, \alpha_n \in M$ e $\beta_1, \ldots, \beta_m$ sono generatori di M ed N rispettivamente, allora $\{\alpha_i\beta_j | i = 1, \ldots, n, j = 1, \ldots, m\}$ sono generatori di $M \cdot N$.

(b) Verifico che l'inverso M^{-1} di un ideale farzionario è ancora un ideale frazionario. Infatti se M è generato come R-modulo da elementi non nulli $\alpha_1 = a_1 b_1^{-1}, \ldots, \alpha_n = a_n b_n^{-1}$ con a_i e $b_i \in R$ e $b_i \neq 0$ per ogni i, allora $(b_1 \cdots b_n) \in M^{-1}$ che quindi M^{-1}non è nullo. Inoltre M^{-1} è contenuto nell' R-sottomodulo di $\mathrm{Frac}(R)$ generato da α_1^{-1}. Quest'ultimo è un ideale frazionario e quindi anche il sottomodulo M^{-1} è un ideale frazionario, grazie al lemma 5.11.

È evidente che il prodotto è commutativo ed associativo e che $\mathbf{1}$ è l'elemento neutro. Per concludere la dimostrazione di (1) resta da verificare che $M \cdot M^{-1} = R$. Per costruzione abbiamo l'inclusione $\subseteq$. Usando il lemma 5.11 scriviamo $M = xI$ con $I \subset R$ un ideale. Grazie alla proposizione 5.9 esiste un ideale J di R tale che $I \cdot J = aR$ per un qualche $a \in \mathrm{Farc}(R)$ non nullo. Quindi $I \cdot \left(a^{-1}J\right) = R$ e $M \cdot \left(x^{-1}a^{-1}J\right) = R$. Conlcudo che $\left(x^{-1}a^{-1}J\right) \subseteq M^{-1}$ e inoltre $R = M \cdot \left(x^{-1}a^{-1}J\right) \subseteq M \cdot M^{-1} \subseteq R$. Deduco allora l'uguaglianza cercata $M \cdot M^{-1} = R$.

(2) Se $M = xR$ e $N = yR$ allora $M \cdot N = xyR$. Inoltre $M^{-1} = x^{-1}R$. L'affermazione segue.

□

Definizione 5.14. Il gruppo abeliano $\mathcal{I}(R)/\mathcal{P}(R)$, degli ideali frazionari di R modulo gli ideali principali, è detto *gruppo delle classi di ideali* di R o *gruppo di Picard* di R, ed è indicato con il simbolo $\mathrm{Pic}(R)$.

Osservazione 5.15. Si può dimostrare che $\mathrm{Pic}(\mathcal{O}_K)$ è finito per ogni campo di numeri K. In particolare, ogni ideale I di $\mathcal{O}_K$ è tale che I^n è principale, con $n = \#(\mathrm{Pic}(\mathcal{O}_K))$.

Teorema 5.16 (Fattorizzazione unica degli ideali)**.** *Ogni ideale frazionario di R si scrive in modo unico come prodotto di primi. (Per convenzione, R è il prodotto vuoto, ovvero $R = P^0$ per ogni primo P.)*

Dim.

Passo 1: Mostriamo che ogni ideale di R si scrive come prodotto di primi, cioè l'insieme $\mathcal{S}$ degli ideali di R che non si possono scrivere come prodotti di primi è vuoto. Se, per assurdo, $\mathcal{S}$ non fosse vuoto, conterrebbe un elemento massimale M. Deve essere che $M \subsetneq R$ è un ideale proprio, poiché $R \notin \mathcal{S}$. Allora M è contenuto in un primo P (cf. la dimostrazione del Lemma 5.8). Segue, per la Proposizione 5.13, che $M = PI$ con $I = P^{-1}M \subseteq R$ un ideale. Lo stesso Corollario afferma che $M \subset I$. Notiamo che l'inclusione è stretta: se fosse $M = I$, allora $I = PI$ da cui, per la Proposizione 5.13, $R = P$, impossibile. Poiché M è massimale, $I \notin \mathcal{S}$. Dunque $I = P_1 \cdots P_r$. Segue $M = PI = PP_1 \cdots P_r$, assurdo.

Grazie al Lemma 5.11 ogni ideale frazionario M si può scrivere come $a^{-1}I$ con I ideale di R e $a \in R$ un elemento non nullo. Quindi $M = (a)^{-1} \cdot I$ e la decomposizione degli ideali (a) ed I di R fornisce la una decomposizione di M.

Passo 2: Dimostriamo l'unicità della fattorizzazione. Supponiamo che valga l'uguaglianza

$$P_1 \cdots P_r = Q_1 \cdots Q_s.$$

Segue che $P_1 \supset Q_1 \cdots Q_s$. Ciò implica che

$$P_1 \supset Q_i$$

per qualche i (vedi la dimostrazione del Lemma 5.8). Posso supporre $i = 1$. Inoltre, l'inclusione $P_1 \supset Q_1$ implica $P_1 = Q_1$. Per la Proposizione 5.13, otteniamo

$$P_2 \cdots P_r = Q_2 \cdots Q_s.$$

Ripetendo induttivamente l'argomento otteniamo $r = s$ e $P_i = Q_i$, a meno di riordinare opportunamente i Q_i.

□

Corollario 5.17. *Gli ideali frazionari nell'anello $\mathcal{O}_K$ degli interi algebrici di un campo di numeri si fattorizzano in modo unico come prodotto di primi.*

Dim. Segue dai Teoremi 5.4 e 5.16. □

Esempio 5.18. Riprendiamo il controesempio alla fattorizzazione unica in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, con $K = \mathbb{Q}[\sqrt{-5}]$, visto in precedenza. Abbiamo le due fattorizzazioni

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

di 6 in $\mathcal{O}_K$ come prodotto di elementi irriducibili, in cui i fattori ai due membri dell'uguaglianza non sono associati (ciò che equivale a dire, grazie all'Esercizio 5.2, che non differiscono per moltiplicazione per ± 1). La fattorizzazione precedente implica la fattorizzazione di ideali (principali)

$$(2\mathcal{O}_K)(3\mathcal{O}_K) = ((1 + \sqrt{-5})\mathcal{O}_K)((1 - \sqrt{-5})\mathcal{O}_K).$$

Osserviamo che questi fattori non sono ideali primi: infatti abbiamo

1. $2\mathcal{O}_K = (2, 1 + \sqrt{-5})^2$,
2. $3\mathcal{O}_K = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$,
3. $(1 + \sqrt{-5})\mathcal{O}_K = (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5})$,
4. $(1 - \sqrt{-5})\mathcal{O}_K = (2, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$,

con i fattori a secondo membro primi. In conclusione, le due fattorizzazioni di 6 producono le stesse fattorizzazioni prime di ideali.

Verifichiamo il primo caso, lasciando il resto al lettore come **esercizio**. Come prima cosa, notiamo che $(a,b)(c,d)$ è generato da (ac,ad,bc,bd). Segue che $(2,1+\sqrt{-5})^2$ è l'ideale $(4,2(1+\sqrt{-5}),-4+2\sqrt{-5})$. Chiaramente, $2\mathcal{O}_K$ contiene questo ideale. Inoltre, si ha che

$$2 = 2(1+\sqrt{-5}) - (-4+2\sqrt{-5}) - 4$$

e quindi vale l'inclusione opposta. Infine, dimostriamo che $(2,1+\sqrt{-5})$ è primo, osservando che

$$\mathcal{O}_K/(2,1+\sqrt{-5}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Infatti, vi è un morfismo suriettivo di anelli

$$\mathcal{O}_K/2\mathcal{O}_K \longrightarrow \mathcal{O}_K/(2,1+\sqrt{-5}),$$

dove $\mathcal{O}_K/2\mathcal{O}_K \simeq (\mathbb{Z}/2\mathbb{Z})^2$; inoltre, $2\mathcal{O}_K$ è contenuto propriamente in $(2,1+\sqrt{-5})$, che a sua volta è contenuto propriamente in $\mathcal{O}_K$ (altrimenti, il suo quadrato sarebbe uguale a $\mathcal{O}_K$).

Osservazione 5.19. Definiamo il massimo comun divisore $MCD(I,J)$ e il minimo comune multiplo $mcm(I,J)$ di due ideali I e J. In considerazione della Proposizione 5.13, $MCD(I,J)$ è il più piccolo ideale contenente I e J; dunque $MCD(I,J) = I+J$. Analogamente, $mcm(I,J)$ è il più grande ideale contenuto in I e J; dunque $mcm(I,J) = I \cap J$.

Osservazione 5.20.

1) Si dimostra che ogni ideale in un dominio di Dedekind è generato da al più due elementi. Più precisamente, se a è un elemento non nullo di un ideale I, esiste b tale che $I = (a,b)$.

2) Si dimostra che un dominio di Dedekind è un UFD se e solo se è un PID.

6 Decomposizione di ideali in estensioni di campi di numeri

Sia L/K un'estensione di campi di numeri. Se P è un primo del dominio di Dedekind $\mathcal{O}_K$, in generale l'ideale $P\mathcal{O}_L$ generato da P in $\mathcal{O}_L$ non è primo.

Esempio 6.1. Posto $K = \mathbb{Q}$ e $L = \mathbb{Q}[\sqrt{-5}]$, abbiamo visto nell'Esempio 5.18 che

$$(2\mathbb{Z})\mathcal{O}_L = 2\mathcal{O}_L = (2,1+\sqrt{-5})^2, \quad (3\mathbb{Z})\mathcal{O}_L = 3\mathcal{O}_L = (3,1+\sqrt{-5})(3,1-\sqrt{-5}).$$

Grazie al Teorema 5.16, si ha che

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}. \tag{10}$$

Definizione 6.2.

1) L'esponente $e_i \geq 1,\ i = 1, \ldots, r$ che compare nell'equazione (10) è detto *indice di ramificazione* di Q_i su P, ed è anche indicato con $e(Q_i/P)$.

2) Diciamo che P è *ramificato* in L se $e_i > 1$ per qualche i.

Intendiamo studiare le proprietà della decomposizione prima (10).

Esercizio 6.3. Data L/K estensione di campi di numeri, P primo di $\mathcal{O}_K$ e Q primo di $\mathcal{O}_L$, dimostrare che le seguenti condizioni sono equivalenti:

1) $Q | P\mathcal{O}_L$,

2) $Q \supset P\mathcal{O}_L$,

3) $Q \supset P$,

4) $Q \cap \mathcal{O}_K = P$,

5) $Q \cap K = P$.

Definizione 6.4. Diciamo che Q *giace su* P, o che P *giace sotto* Q, se le condizioni equivalenti dell'Esercizio 6.3 sono verificate.

Il prossimo risultato esclude, tra le altre cose, che la fattorizzazione (10) possa essere vuota (cioè che il numero r di fattori sia 0).

Proposizione 6.5.

1) Ogni primo di $\mathcal{O}_L$ giace su un primo di $\mathcal{O}_K$.

2) Ogni primo di $\mathcal{O}_K$ giace sotto (almeno) un primo di $\mathcal{O}_L$.

Dim. Sia Q un primo di $\mathcal{O}_L$. Per la prima parte, basta verificare che $P := Q \cap \mathcal{O}_K$ è un primo di $\mathcal{O}_K$. Ora, P è un ideale proprio (altrimenti conterrebbe 1 e quindi $Q = \mathcal{O}_L$); inoltre è un ideale primo (per definizione di ideale primo); infine è diverso da zero, poiché se α è un elemento non nullo di Q, $N_{L/K}(\alpha)$ appartiene a $Q \cap \mathcal{O}_K = P$ ed è non nullo per definizione dell'operatore norma. Passiamo alla seconda parte. Dato un primo P di $\mathcal{O}_K$, alla luce dell'Esercizio 6.3 basta dimostrare che $P\mathcal{O}_L$ è contenuto propriamente in $\mathcal{O}_L$ e quindi la sua fattorizzazione prima in $\mathcal{O}_L$ non è vuota. In altre parole, occorre vedere che $1 \notin P\mathcal{O}_L$. Per il Lemma 5.8, esiste $x \in K - \mathcal{O}_K$ tale che $xP \subset \mathcal{O}_K$. Segue che

$$xP\mathcal{O}_L \subset \mathcal{O}_L.$$

Se fosse $1 \in P\mathcal{O}_L$, otterremmo che $x \in \mathcal{O}_L$. Ma allora x apparterrebbe a $K \cap \mathcal{O}_L = \mathcal{O}_K$, impossibile. □

Torniamo alla fattorizzazione (10) e fissiamo un primo $Q = Q_i$ che giace su P. Oltre all'indice di ramificazione $e(Q/P)$, possiamo associare un altro invariante alla coppia (P, Q). Per questo, consideriamo i campi

$$\mathbb{F}_P = \mathcal{O}_K/P, \qquad \mathbb{F}_Q = \mathcal{O}_L/Q,$$

detti *campi residui* di P e Q, rispettivamente. Sia p il primo razionale tale che

$$p\mathbb{Z} = P \cap \mathbb{Q} = Q \cap \mathbb{Q}.$$

Abbiamo omomorfismi suriettivi canonici

$$\mathcal{O}_K/p\mathcal{O}_K \longrightarrow \mathcal{O}_K/P, \qquad \mathcal{O}_L/p\mathcal{O}_L \longrightarrow \mathcal{O}_L/Q.$$

Notiamo che

$$\mathcal{O}_K/p\mathcal{O}_K \simeq (\mathbb{Z}/p\mathbb{Z})^{n_K}, \qquad \mathcal{O}_L/p\mathcal{O}_L \simeq (\mathbb{Z}/p\mathbb{Z})^{n_L},$$

dove $n_K = [K : \mathbb{Q}]$ e $n_L = [L : \mathbb{Q}]$, grazie al Teorema 4.5. Segue che $\mathbb{F}_P$ e $\mathbb{F}_\mathbb{Q}$ sono campi finiti di caratteristica p. Inoltre, poiché $Q \cap \mathcal{O}_K = P$, vi è un morfismo canonico di campi

$$\mathbb{F}_P \longrightarrow \mathbb{F}_\mathbb{Q}.$$

In altre parole, $\mathbb{F}_Q/\mathbb{F}_P$ è un'estensione di campi finiti.

Definizione 6.6. Il *grado di inerzia* $f(Q/P)$ di Q su P è il grado $[\mathbb{F}_Q : \mathbb{F}_P]$.

Lemma 6.7 (Moltiplicatività degli indici di ramificazione e dei gradi di inerzia)**.** *Siano $K_1 \subset K_2 \subset K_3$ campi di numeri, e siano $P_1 \subset P_2 \subset P_3$ primi di $\mathcal{O}_{K_1}$, $\mathcal{O}_{K_2}$ e $\mathcal{O}_{K_3}$, rispettivamente. Allora*

$$e(P_3/P_1) = e(P_3/P_2) \cdot e(P_2/P_1), \qquad f(P_3/P_1) = f(P_3/P_2) \cdot f(P_2/P_1).$$

Dim. **Esercizio.** □

Supponiamo ora che $\mathcal{O}_L$ sia generato da $\mathcal{O}_K$ e da un elemento $\alpha\mathcal{O}_L$ come anello, ovvero che $\mathcal{O}_K[\alpha]$. Non sempre è vero, ma lo è nel caso in cui $K = \mathbb{Q}$ ed L sia un campo cilcotomico oppure una estensione quadratica di $\mathbb{Q}$.

Teorema 6.8. *Supponiamo che $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ e sia $g(X) \in \mathcal{O}_K[X]$ il polinomio minimo di α su K. Sia $P \subset \mathcal{O}_K$ un ideale primo e scriviamo la decomposizione $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}$ come in (10). Sia $\overline{g}(X) \in \mathbb{F}_P[X]$ la riduzione di g modulo $P\mathcal{O}_K[X]$ e scriviamo la decomposizione $\overline{g}(X) = \overline{g}_1(X)^{a_1} \cdots \overline{g}_s(X)^{a_s}$ in fattori irriducibili (non necessariamente monici) in $\mathbb{F}_P[X]$. Allora, a meno di rinumerare tali fattori, abbiamo*

1. *$s = r$;*
2. *$a_i = e_i$ per ogni $i = 1 \cdots, r$;*

3. $Q_i = P\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$ *con* $g_i(X) \in \mathcal{O}_K[X]$ *un polinomio che si riduce su* $\overline{g}_i(X)$ *modulo* $P\mathcal{O}_K[X]$ *e* $Q_i^{e_i} = P\mathcal{O}_L + g_i(\alpha)^{e_i}\mathcal{O}_L$ *per ogni* $i = 1 \cdots, r$.

Dim. Utilizzando l'isomorfismo $\mathcal{O}_K[X]/(g(X)) \cong \mathcal{O}_K[\alpha] = \mathcal{O}_L$ definito dalla valutazione $X \mapsto \alpha$ (vedere Esercizio 2.5) segue che

$$\mathcal{O}_L/P\mathcal{O}_L \cong \mathcal{O}_K[X]/P\mathcal{O}_L + \big(g(X)\big) \cong \mathbb{F}_P[X]/\big(\overline{g}(X)\big) \cong \prod_{i=1}^{s} \mathbb{F}_P[X]/\big(\overline{g}_i(X)\big)^{a_i};$$

l'ultimo isomorfismo di anelli segue dal teorema cinese dei resti.

Gli ideali primi di $\mathcal{O}_L$ che dividono $P\mathcal{O}_L$ sono gli ideali primi che contengono P per l'esercizio 6.3. Questi sono in corrispondenza biunivoca con gli ideali primi del quoziente $\mathcal{O}_L/P\mathcal{O}_L$ grazie all'esercizio 6.9 ovvero con gli deali primi di $\mathbb{F}_P[X]/\big(\overline{g}(X)\big)$ ovvero, utilizzando ancora l'esercizio 6.9, con gli ideali primi di $\mathbb{F}_P[X]$ contenenti $\overline{g}(X)$. Essendo $\mathbb{F}_P[X]$ un PID questi sono tutti e soli gli ideali corrispondenti ai fattori irriducibili di $\overline{g}(X)$, ovvero $\big(\overline{g}_i(X)\big)$ per $i = 1 \ldots, s$.

Questi implica che $r = s$ e che, a meno di riordinare i fattori, $Q_i/P\mathcal{O}_L = \big(\overline{g}_i(X)\big)$ tramite l'isomorfismo descritto precedentemente. Deduco allora, sempre dall'esercizio 6.9, che $Q_i = P\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$.

Osserviamo che per ogni $n \in \mathbb{N}$ abbiamo $P\mathcal{O}_L \subset P\mathcal{O}_L + g_i(\alpha)^n\mathcal{O}_L \subset Q$, con Q ideale primo, se e solo se $P\mathcal{O}_L \subset Q$ e $g_i(\alpha) \in Q_j$, visto che Q è un ideale primo. Quindi questo vale se e solo se $Q = Q_i$. Segue che l'ideale $P\mathcal{O}_L + g_i(\alpha)^n\mathcal{O}_L$ di $\mathcal{O}_L$ ammette una decomposizione come prodotto di ideali primi in cui compare solo il fattore Q_i. In particolare $P\mathcal{O}_L + g_i(\alpha)^{a_i}\mathcal{O}_L = Q_i^{d_i}$ per un qualche intero positivo d_i. Osservo che $Q_i^{a_i} \subset P\mathcal{O}_L + \big(g_i(\alpha)^{a_i}\big) = Q_i^{d_i}$ e quindi, per l'unicità della decomposizione, abbiamo $a_i \geq d_i$.

Analogamente abbiamo che $\prod_i Q_i^{d_i} \subset P\mathcal{O}_L$ in quanto $\prod_i g_i(\alpha)^{a_i} \equiv g(\alpha) \equiv 0$ modulo $P\mathcal{O}_L$. Segue allora dall'unicità della decomposizione in primi che $d_i \geq e_i$. Infine dall'uguaglianza $P\mathcal{O}_K = Q_1^{e_1} \cdots Q_r^{e_r}$ segue che $\big(g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r}\big) \in P\mathcal{O}_L$. Quindi $\overline{g}_1(\alpha)^{e_1} \cdots \overline{g}_r(\alpha)^{e_r} \equiv 0$ in $\mathcal{O}_L/P\mathcal{O}_L \cong \mathbb{F}_P[X]/\big(\overline{g}(X)\big)$ ovvero $e_i \geq a_i$ per ogni i. Concludo allora che $a_i = d_i = e_i$ per ogni $i = 1, \ldots, r$. □

Esercizio 6.9. Sia R un anello, I un ideale e $\pi\colon R \to R/I$ l'applicazione quoziente. Sia $\mathcal{T}_I$ l'insieme degli ideali di R contenenti I. Sia $\mathcal{S}$ l'insieme degli ideali di R/I. Dimostrare che le applicazioni $\mathcal{T}_I \to \mathcal{S}$ definita da $J \mapsto J/I$ e $\mathcal{S} \to \mathcal{T}_I$ definita da $\overline{J} \mapsto \pi^{-1}(\overline{J})$ sono ben definite ed una l'inversa dell'altra. Verificare che tali applicazioni inviano ideali primo in ideale primo.

Teorema 6.10. *Con le notazioni del Teorema precedente, sia* $n = [L : K]$*:*

i. Abbiamo $e(Q_i/P) = e_i$ *e* $f(Q_i/P) = \deg \overline{g}_i(X)$ *per ogni* $i = 1, \ldots, r$ *e quindi vale la formula* $\sum_{i=1}^{r} e(Q_i/P)f(Q_i/P) = n$.

ii. Il primo P *ramifica se e solo se* $\operatorname{mcd}\big(\overline{g}(X), \overline{g}'(X)\big) \in \mathbb{F}_P[X]$ *non è un'unità se e solo se* $\operatorname{disc}_{L/K}\big(1, \ldots, \alpha^{n-1}\big) \equiv 0$ *modulo* P.

Dim. i) L'uguaglianza $e(Q_i/P) = e_i$ segue dal Teorema 6.8. Grazie ad esso otteniamo anche che $f(Q_i/P)$, ovvero il grado dell'estensione $\mathbb{F}_P \subset \mathcal{O}_L/Q_i \cong \mathbb{F}_P[X]/\big(\overline{g}_i(X)\big)$, coincide con il grado del polinomio $\overline{g}_i(X)$.

Infine, il grado $[L : K]$ coincide con il grado di $g(X)$ che si scrive come $\sum_{i=1}^{r} e_i \deg \overline{g}_i(X)$. Quindi la formula segue.

ii) Segue dal Teorema 6.8 che P ramifica se e solo se esiste un fattore irriducibile $h(X)$ di $\overline{g}(X)$ tale che $h(X)^2$ divide $\overline{g}(X)$. In questo caso $\overline{g}(X) = h(X)^2\ell(X)$ e il polinomio derivato $\overline{g}'(X)$ coincide con

$$\overline{g}'(X) = 2h(X)h'(X)\ell(X) + h(X)^2\ell'(X)$$

e, dunque, $h(X)$ divide $\mathrm{mcd}(\overline{g}(X), \overline{g}'(X)\big) \in \mathbb{F}_P[X]$. Viceversa, sia $h(X)$ un polinomio irriducibile che divide $\mathrm{mcd}(\overline{g}(X), \overline{g}'(X)\big)$ Scrivo $\overline{g}(X) = h(X)q(X)$. Calcolando $\overline{g}'(X) = h'(X)q(X) + h(X)q'(X)$ segue che $h(X)$ divide $h'(X)q(X)$ in quanto divide $\overline{g}'(X)$. Siccome $\mathbb{F}_P$ è un campo perfetto e $h(X)$ è irriducibile, allora $\mathrm{mcd}(h(X), h'(X)) = 1$. Segue che $h(X)$ divide $q(X)$ e quindi $h(X)^2$ divide $\overline{g}(X)$.

Sia dato $\beta \in \mathcal{O}_L$. Ricordiamo dalla proposizione 3.7 che $N_{L/K}(\beta)$ è, a meno di segno, il coefficiente costante del polinomio caratteristico dell'operatore moltiplicazione per β rispetto alla base $\{1, \ldots, \alpha^{n-1}\}$ di L come K-spazio vettoriale o equivalentemente di $\mathcal{O}_L$ come $\mathcal{O}_K$-modulo. Riducendo modulo P otteniamo allora che $N_{L/K}(\beta)$ modulo P è il coefficiente costante del polinomio caratteristico della matrice dell'operatore moltiplicazione per la classe $\overline{\beta}$ di β modulo $P\mathcal{O}_L$ sull'$\mathbb{F}_P$-spazio vettoriale $\mathcal{O}_L/P\mathcal{O}_L$. Quindi $N_{L/K}(\beta) \equiv 0$ modulo P se e solo se la moltiplicazione per $\overline{\beta}$ ha nucleo non banale ovvero se e solo se non è un isomorfismo. Questo è equivalente a richiedere che $\overline{\beta}$ non sia un'unità. Usando l'identificazione $\mathcal{O}_L/P\mathcal{O}_L \cong \mathbb{F}_P[X]/\big(\overline{g}(X)\big)$ e $\beta = g'(\alpha)$, abbiamo che $N_{K/\mathbb{Q}}(g'(\alpha)) \equiv 0$ modulo P se e solo se $\mathrm{mcd}\big(\overline{g}(X), \overline{g}'(X)\big) \neq 1$ in $\mathbb{F}_P[X]$ ovvero $\overline{g}(X)$ ha zeri doppi. Visto che $\mathrm{disc}_{L/K}\big(1, \ldots, \alpha^{n-1}\big)$ coincide con $N_{L/K}(g'(\alpha))$ a meno di segno grazie alla Proposizione 3.9, la seconda equivalenza risulta mostrata.

□

Osservazione 6.11. Il Teorema vale in generale senza l'ipotesi che $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Per la dimostrazione, vedi il libro di Marcus.

Applicazione: Applichiamo il Teorema 6.10 al caso dei campi quadratici. Sia $K = \mathbb{Q}[\sqrt{d}]$, con $d \in \mathbb{Z} - \{0, 1\}$ privo di fattori quadratici. Dato un primo razionale p, il Teorema 6.10 mostra che sono possibili le 3 seguenti fattorizzazioni dell'ideale $p\mathcal{O}_K$:

$$p\mathcal{O}_K = \begin{cases} Q^2 & \text{(cioè } p \text{ è ramificato in } K) \\ Q \ \text{ primo} & \text{(diciamo che } p \text{ è } \textit{inerte} \text{ in } K) \\ Q_1Q_2 \ \ (Q_1 \neq Q_2) & \text{(diciamo che } p \textit{ si decompone} \text{ in } K) \end{cases}$$

Corollario 6.12.

1. Se $p|d$, si ha $p\mathcal{O}_K = (p, \sqrt{d})^2$.

2. Se d è dispari, si ha

$$2\mathcal{O}_K = \begin{cases} (2, 1+\sqrt{d})^2 & \text{se } d \equiv 3 \pmod 4 \\ (2, \frac{1+\sqrt{d}}{2})(2, \frac{1-\sqrt{d}}{2}) & \text{se } d \equiv 1 \pmod 8 \\ \text{primo} & \text{se } d \equiv 5 \pmod 8 \end{cases}$$

dove i fattori nel caso $d \equiv 1 \pmod 8$ sono distinti.

3. Se p è dispari e $p \nmid d$, si ha

$$p\mathcal{O}_K = \begin{cases} (p, n+\sqrt{d})(p, n-\sqrt{d}) & \text{se } d \equiv n^2 \pmod p \\ \text{primo} & \text{se } d \text{ non è un quadrato modulo } p \end{cases}$$

dove i fattori nel caso $d \equiv n^2 \pmod p$ sono distinti.

In particolare, l'ideale massimale $p\mathbb{Z}$ è ramificato in $K = \mathbb{Q}[\sqrt{d}]$ se e solo se p divide d, risp. $4d$ per $d \equiv 1 \pmod 4$, risp. $d \equiv 2, 3 \pmod 4$.

Dim. Applichiamo direttamente il Teorema 6.8.

Consideriamo innanzitutto il caso $d \equiv 2, 3$ modulo 4. Grazie alla Proposizione 2.9 abbiamo $\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - d)$. Il polinomio $X^2 - d$ in $\mathbb{F}_p[X]$

i. è irriducibile se $p \neq 2$ e d non è un quadrato modulo p;

ii. si decompone come il prodotto di due fattori irriducibili coprimi $(X-n)(X+n) \in \mathbb{F}_p[X]$ se p non divide d e $d \equiv n^2$ modulo p;

iii. si scrive come $X^2 \in \mathbb{F}_p[X]$ se p divide d;

iv. si scrive come $(X+1)^2$ se $p = 2$ e 2 non divide d.

Se $d \equiv 1$ modulo 4 allora $\mathcal{O}_K \cong \mathbb{Z}[\alpha]$ con $\alpha = \frac{1+\sqrt{d}}{2}$ che ha polinomio minimo $g(X) = X^2 - X + m$ con $m := \frac{1-d}{4}$. Osserviamo che $4g(X) = Y^2 - d$ con $Y = 2X - 1$.

Il polinomio $g(X)$ in $\mathbb{F}_p[X]$

i. è irriducibile in quanto uguale a $4^{-1}(Y^2 - d)$ se $p \neq 2$ e d non è un quadrato modulo p. Osservo che questa scrittura ha senso visto che 2 è invertibile modulo p;

ii. si decompone come il prodotto di due fattori irriducibili coprimi $4^{-1}(Y-n)(Y+n) \in \mathbb{F}_p[X]$ se p non divide d e $d \equiv n^2$ modulo p;

iii. si scrive come $4^{-1}Y^2$ se p divide d;

iv. si scrive come $X(X+1)^2$ se $p = 2$ e 2 divide m ovvero $d \equiv 1$ modulo 8;

v. si scrive come X^2+X+1 che è irriducibile se $p=2$ e 2 non divide m ovvero $d \equiv 5$ modulo 8.

□

Un altro caso interessante è il caso dell'n-esimo campo ciclotomico K in cui $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. In questo caso il polinomio minimo di ζ_n è l'n-esimo polinomio ciclotomico $\Phi_n(X)$, che divide X^n-1. Il Teorema 6.8 permette di determinare come $p\mathcal{O}_K$ si decompone, dato un primo p di $\mathbb{Z}$, in termini della decomposizione della riduzione di $\Phi_n(X)$ modulo p. Vediamone un esempio per n primo.

Corollario 6.13. *Se $n=p$ è un primo, allora $p\mathbb{Z}$ è l'unico primo che ramifica in $\mathcal{O}_K$ e $p\mathcal{O}_K = Q^{p-1}$ con $Q=(p,\zeta_p-1)$ ideale primo di $\mathcal{O}_K$.*

Dim. Visto che $X^p-1 \equiv (X-1)^p$ modulo p, il polinomio $\Phi_p(X) \equiv (X-1)^p$ in $\mathbb{F}_p[X]$.

Se ℓ è un primo che non divide p allora il polinomio X^p-1 modulo ℓ, e quindi $\Phi_n(X)$, non ha zeri doppi. Infatti il polinomio derivato è pX^{p-1} che è coprimo con X^p-1. Quindi ℓ non ramifica in $\mathcal{O}_K$.

□

7 La legge di reciprocità quadratica di Gauss

Sia p un primo dispari e sia $d \in \mathbb{Z}$ un intero non divisibile per p. Definiamo il *simbolo di Legendre*

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{se } d \text{ è un quadrato modulo } p \\ -1 & \text{se } d \text{ non è un quadrato modulo } p \end{cases}$$

Teorema 7.1 (Legge di reciprocità quadratica)**.** *Se $q \neq p$ è un primo dispari, si ha*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{se } p \text{ o } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{se } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Esempio 7.2. Poiché 857 è un primo $\equiv 1 \pmod 4$ e $\equiv 3 \pmod 7$, il Teorema 7.1 implica che

$$\left(\frac{7}{857}\right) = \left(\frac{857}{7}\right) = \left(\frac{3}{7}\right) = -1.$$

Teorema 7.3.

1) (Primo supplemento) Si ha $\left(\frac{-1}{p}\right) = 1$ se e solo se $p \equiv 1 \pmod 4$.

2) (Secondo supplemento) Si ha

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod 8 \\ -1 & \text{se } p \equiv \pm 3 \pmod 8 \end{cases}$$

Osservazione 7.4. Il primo supplemento segue dal fatto che -1 è un quadrato modulo p se e solo se $\mathbb{F}_p^\times$ contiene un elemento di ordine 4. Non dimostriamo il secondo supplemento.

Dim del Teorema 7.1. Sia $\zeta = e^{2\pi i/p}$. Si ricordi l'isomorfismo canonico

$$(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow G := \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}), \qquad k \mapsto (\sigma_k : \zeta \mapsto \zeta^k).$$

Allora $\left(\frac{q}{p}\right) = 1$ se e solo se σ_q appartiene al sottogruppo $G^{(2)} := \{g^2 : g \in G\}$ dei quadrati degli elementi di G. La teoria di Galois identifica $G/G^{(2)}$ con il gruppo di Galois dell'unico sottocampo quadratico K di $\mathbb{Q}[\zeta]$, in modo tale che la proiezione naturale di G su $G/G^{(2)}$ corrisponde alla restrizione a K degli automorfismi di $\mathbb{Q}[\zeta]$. Ne viene che $\left(\frac{q}{p}\right) = 1$ se e solo se $\sigma_q|_K = \mathrm{id}_K$. Equivalentemente, $\left(\frac{q}{p}\right) = -1$ se e solo se $\sigma_q|_K$ genera $\mathrm{Gal}(K/\mathbb{Q})$. In questo caso, indicato con Q un primo di $\mathcal{O}_K$ che giace su $q\mathbb{Z}$, si ha che $\sigma_q|_K$ induce l'automorfismo di Frobenius $\phi_q : x \mapsto x^q$ sul campo residuo $\mathbb{F}_Q = \mathcal{O}_K/Q$. Inoltre, $\sigma_q|_K$ e ϕ_q hanno lo stesso ordine (uguale a 2). Poiché ϕ_q genera $\mathrm{Gal}(\mathbb{F}_\mathbb{Q}/\mathbb{F}_q)$, questo equivale a dire che il grado di inerzia $f(Q/q\mathbb{Z})$ è uguale a 2. In conclusione,

$$\left(\frac{q}{p}\right) = -1 \text{ se e solo se } q\mathbb{Z} \text{ è inerte in } K.$$

Sappiamo che $K = \mathbb{Q}[\sqrt{\pm p}]$ per $p \equiv \pm 1 \pmod 4$. In particolare, $q\mathbb{Z}$ non è ramificato in K. Grazie alla Proposizione 6.12, otteniamo che

$$\left(\frac{q}{p}\right) = -1 \text{ se e solo se } \left(\frac{\pm p}{q}\right) = -1, \text{ con } p \equiv \pm 1 \pmod 4.$$

Infine, grazie al primo supplemento, si ha

$$\left(\frac{-p}{q}\right) = \pm\left(\frac{p}{q}\right) \text{ se } q \equiv \pm 1 \pmod 4.$$

□

Esercizio 7.5. Dato un primo p, dimostrare che l'equazione

$$x^2 - x + 5 = 0 \pmod p$$

non ha soluzioni se $p = 2$ o $p \in \{2, 3, 8, 10, 12, 13, 14, 15, 18\} \pmod{19}$, ha un'unica soluzione se $p = 19$, ha due soluzioni se $p \in \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \pmod{19}$.

Riferimenti bibliografici

[Ma] Marcus, Daniel A. Number fields. Universitext. Springer-Verlag, New York-Heidelberg, 1977. viii+279 pp.

[Mi] Milne, J.S. Fields and Galois Theory (note disponibili sulla pagina web dell'autore: http://www.jmilne.org/math/CourseNotes/ft.html)