Alma Mater Studiorum · Università di Bologna

**SCUOLA DI SCIENZE**
**Corso di Laurea in Matematica**

# IDEALI NELL'ANELLO DEGLI INTERI ALGEBRICI

**Tesi di Laurea in Teoria dei Numeri Algebrica**

**Relatore:**
**Chiar.mo Prof.**
**Caselli Fabrizio**

**Presentata da:**
**Vecchi Lorenzo**

**Sessione Unica**
**Anno Accademico 2017/2018**

# Indice

# Introduzione

L'obiettivo principale della Teoria dei Numeri è quello di studiare l'anello degli interi $\mathbb{Z}$, anche in relazione al campo dei razionali, una struttura ricca di proprietà. Il nostro scopo è quello di definire un insieme più generale che sostituisca gli interi quando al posto dei razionali viene considerata una loro generica estensione algebrica $\mathbb{Q} \subset K$: tale insieme, denotato con $O_K$, prende il nome di *anello degli interi algebrici*.
Gli strumenti che utilizzeremo sono quelli propri dell'Algebra Commutativa [1] e della Teoria dei Numeri Algebrica [2]. Fondamentale sarà, ad esempio, la descrizione della struttura dei *domini di Dedekind* (di cui $\mathbb{Z}$ e $O_K$ sono appunto esempi prìncipi): essi hanno la proprietà di essere noetheriani, integralmente chiusi e tali che ogni ideale primo non nullo sia anche massimale.
Uno dei principali risultati sarà la generalizzazione del *teorema fondamentale dell'aritmetica*; poiché vedremo che in generale $O_K$ non è un dominio a fattorizzazione unica, introdurremo un sistema di operazioni sugli ideali di un anello e otterremo un teorema di fattorizzazione unica in ideali primi.
Infine, lo studio della famiglia degli ideali di $O_K$ porterà alla definizione del *gruppo delle classi di ideali*, la cui struttura ci consentirà di descrivere proprietà fondamentali di tale anello, tra cui l'essere o meno un dominio a ideali principali.

# Capitolo 1

# Prime definizioni

Iniziamo la trattazione descrivendo alcuni risultati generali sugli ideali di un anello e introducendo alcune operazioni di base che utilizzeremo abbondantemente per poter dimostrare risultati più complessi nei capitoli successivi.

## 1.1 Ideali

I primi oggetti che introduciamo sono gli *ideali*, una struttura fondamentale dell'Algebra Commutativa.

**Definizione 1.1.1.** Un *ideale* $\mathfrak{a}$ di un anello $A$ è un sottoinsieme di $A$ che è anche un sottogruppo additivo ed è tale che $A\mathfrak{a} \subset \mathfrak{a}$.

**Definizione 1.1.2.** Un ideale $\mathfrak{p}$ si dice *primo* se è diverso da (1) e se

$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ oppure } y \in \mathfrak{p}.$$

Un ideale $\mathfrak{m}$ si dice *massimale* se è diverso da (1) e se non esiste un ideale $\mathfrak{a}$ tale che $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq (1)$. Equivalentemente:

- $\mathfrak{p}$ è primo se e solo se $A/\mathfrak{p}$ è un dominio di integrità;
- $\mathfrak{m}$ è massimale se e solo se $A/\mathfrak{m}$ è un campo.

**Osservazione 1.1.3.** Un ideale massimale è anche primo, ma in generale non vale il viceversa.

**Teorema 1.1.4.** *Ogni anello $A \neq 0$ ha almeno un ideale massimale.*

*Dimostrazione.* La dimostrazione è un'applicazione diretta del Lemma di Zorn. Consideriamo la famiglia di ideali $\Sigma = \{\mathfrak{a} \subset A, \mathfrak{a} \neq (1)\}$ ordinata per inclusione. Data una catena di ideali $(\mathfrak{a}_\alpha)$, definiamo $\bar{\mathfrak{a}} = \bigcup_\alpha \mathfrak{a}_\alpha$. Poiché per ipotesi $1 \notin \mathfrak{a}_\alpha$ per ogni $\alpha$, $1 \notin \bar{\mathfrak{a}} \Rightarrow \bar{\mathfrak{a}} \in \Sigma$. Da questo deduciamo che $\bar{\mathfrak{a}}$ è un maggiorante di $(\mathfrak{a}_\alpha)$ in $\Sigma$. Allora $\Sigma$ ha un elemento massimale. □

**Definizione 1.1.5.** Un anello che ha un solo ideale massimale si chiama *anello locale*.

**Teorema 1.1.6.** *Sia* $\mathfrak{m}$ *un ideale di* $A$ *diverso da* (1) *tale che ogni* $x \in A \setminus \mathfrak{m}$ *è un'unità di* $A$*. Allora* $A$ *è un anello locale e* $\mathfrak{m}$ *è il suo ideale massimale.*

*Dimostrazione.* Se un ideale è diverso da (1), tutti i suoi elementi devono essere non invertibili, quindi deve essere contenuto in $\mathfrak{m}$. Allora $\mathfrak{m}$ è l'unico ideale massimale di $A$, che quindi è locale.

□

## 1.2 Azione di omomorfismi su ideali

Consideriamo ora $f : A \to B$ omomorfismo di anelli. Osserviamo che se $\mathfrak{a}$ è un ideale di $A$, l'insieme $f(\mathfrak{a})$ non è necessariamente un ideale di $B$ (si pensi ad esempio all'immersione di $\mathbb{Z}$ in $\mathbb{Q}$).

**Definizione 1.2.1.** Definiamo l'*estensione* di $\mathfrak{a}$ (denotata con $\mathfrak{a}^e$) come l'ideale generato da $f(\mathfrak{a})$ in $B$:

$$\mathfrak{a}^e = (f(\mathfrak{a})) = \left\{ \sum y_i f(x_i), x_i \in \mathfrak{a}, y_i \in B \right\}.$$

Viceversa se $\mathfrak{b}$ è un ideale di $B$, la sua controimmagine tramite $f$ è sempre un ideale di $A$.

**Definizione 1.2.2.** Definiamo la *contrazione* di $\mathfrak{b}$ come $\mathfrak{b}^c = f^{-1}(\mathfrak{b})$.

**Teorema 1.2.3.** *Siano* $\mathfrak{a}$ *ideale di* $A$ *e* $\mathfrak{b}$ *ideale di* $B$*. Sia* $f$ *un omomorfismo* $f : A \to B$*. Valgono le seguenti affermazioni:*

- $\mathfrak{a} \subset \mathfrak{a}^{ec}$;
- $\mathfrak{b}^{ce} \subset \mathfrak{b}$;
- $\mathfrak{a}^{ece} = \mathfrak{a}^e$;
- $\mathfrak{b}^{cec} = \mathfrak{b}^c$.

*Dimostrazione.* I risultati seguono da semplici considerazioni insiemistiche.

- Se $x \in \mathfrak{a}, f(x) \in f(\mathfrak{a}) \subset \mathfrak{a}^e$. Quindi $\mathfrak{a} \subset \mathfrak{a}^{ec}$.
- $\mathfrak{b}^{ce} = (f(\mathfrak{b}^c)) = (f(f^{-1}(\mathfrak{b}))) \subset (b) = b$.
- $\mathfrak{a}^{ece} = (f(f^{-1}(\mathfrak{a}^e))) = (\mathfrak{a}^e) = \mathfrak{a}^e$.
- $\mathfrak{b}^{cec} = \mathfrak{b}^c \Leftrightarrow \mathfrak{b}^{cece} = \mathfrak{b}^{ce} \Leftrightarrow (\mathfrak{b}^c)^{ece} = (\mathfrak{b}^c)^e$, che è vero dal punto precedente.

□

## 1.3 Anelli di frazioni

La procedura con cui si costruisce il campo dei razionali $\mathbb{Q}$ partendo dall'anello degli interi $\mathbb{Z}$ si estende a qualsiasi anello.
Dato un anello $A$ consideriamo un suo *sottoinsieme moltiplicativo* $S$, ovvero tale che $1 \in S$ e che sia chiuso rispetto alla moltiplicazione. Definiamo su $A \times S$ la relazione di equivalenza

$$(a, s) \equiv (b, t) \Leftrightarrow (at - bs)u = 0 \text{ per qualche } u \in S.$$

**Definizione 1.3.1.** Denotiamo con $\frac{a}{s}$ la classe di equivalenza di $(a, s)$. L'insieme delle classi di equivalenza, denotato come $S^{-1}A$, si chiama *anello di frazioni* di $A$ rispetto a $S$.

**Esempio 1.3.2.** Per $A$ dominio di integrità e $S = A \setminus \{0\}, S^{-1}A = Q(A)$, dove $Q(A)$ indica il campo delle frazioni di $A$.

**Osservazione 1.3.3.** Esiste un morfismo di anelli $f : A \to S^{-1}A, f(x) = \frac{x}{1}$ con le seguenti proprietà:

- $s \in S \Rightarrow f(s)$ è un'unità di $S^{-1}A$;
- $f(a) = 0 \Rightarrow as = 0$ per qualche $s \in S$;
- Ogni elemento di $S^{-1}A$ è della forma $f(a)f(s)^{-1}$ per qualche $a \in A, s \in S$.

Effettivamente, possiamo pensare che l'anello di frazioni $S^{-1}A$ si formi "rendendo invertibili" gli elementi di $S$. Dalla definizione, teoricamente 0 potrebbe appartenere ad $S$, anche se in questo caso $S^{-1}A = \left\{\frac{0}{0}\right\}$, poiché per ogni $a \in A, s \in S$ abbiamo che $a \cdot 0 - 0 \cdot s = 0$ e quindi $(a, s) \equiv (0, 0)$. Per escludere questo caso banale, d'ora in poi considereremo solo i casi in cui $0 \notin S$.

**Esempio 1.3.4.** Sia $\mathfrak{p}$ un ideale primo di $A$. L'insieme $S = A \setminus \mathfrak{p}$ è un sottoinsieme moltiplicativo. Denotiamo $S^{-1}A := A_{\mathfrak{p}}$. Consideriamo l'ideale $\mathfrak{m} = \left\{\frac{a}{s}, a \in \mathfrak{p}\right\}$: esso è l'unico ideale massimale di $A_{\mathfrak{p}}$. Infatti, se consideriamo un elemento $\frac{b}{t} \notin \mathfrak{m}$, allora $b \notin \mathfrak{p} \Leftrightarrow b \in S$, quindi $\frac{b}{t}$ è un'unità di $A_{\mathfrak{p}}$. Il risultato segue da 1.1.6. Allora siamo giustificati a dare la seguente definizione.

**Definizione 1.3.5.** Dato un anello $A$ e un suo ideale primo $\mathfrak{p}$, chiamiamo $S^{-1}A = A_{\mathfrak{p}}$ la sua *localizzazione* rispetto a $\mathfrak{p}$.

**Teorema 1.3.6.** *La localizzazione $A_{\mathfrak{p}}$ di un anello $A$ è un anello locale. Il suo unico ideale massimale è dato da $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$.*

**Esempio 1.3.7.** Sia $A = \mathbb{Z}$, $p \in \mathbb{Z}$ primo e $\mathfrak{p} = (p)$. Allora

- $A_{(p)} = \left\{ \frac{m}{n}, p \not| n \right\}$.
- $\mathfrak{m} = pA_{(p)}$.

**Teorema 1.3.8.** *Sia $A$ un anello e $S^{-1}A$ l'anello di frazioni rispetto a un insieme moltiplicativo $S$. Sia $f$ l'omomorfismo $f : A \to S^{-1}A, f(x) = \frac{x}{1}$. Gli ideali estesi e contratti da $f$ soddisfano le seguenti affermazioni:*

- *Ogni ideale di $S^{-1}A$ è un ideale esteso;*
- *Se $\mathfrak{a}$ è un ideale di $A$, $\mathfrak{a}^e = S^{-1}\mathfrak{a}$. Inoltre $\mathfrak{a}^e = (1) \Leftrightarrow \mathfrak{a} \cap S \neq \emptyset$;*
- *Gli ideali primi di $S^{-1}A$ sono in corrispondenza biunivoca con gli ideali primi di $A$ che non intersecano $S$, $(\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p})$.*

*Dimostrazione.*

- Sia $\mathfrak{b}$ un ideale di $S^{-1}A$ e $\frac{x}{s} \in \mathfrak{b}$. Allora $\frac{x}{1} \in \mathfrak{b}$ e quindi $x \in \mathfrak{b}^c$. Allora $\frac{x}{s} \in \mathfrak{b}^{ce}$. Poiché l'altra inclusione è sempre valida, $\mathfrak{b} = \mathfrak{b}^{ce}$.
- Un'inclusione è ovvia. Per l'altra, se $y \in \mathfrak{a}^e$, allora è della forma $y = \sum a_i/s_i, a_i \in \mathfrak{a}, s_i \in S$; portando tutto a comune denominatore, otteniamo che $y \in S^{-1}\mathfrak{a}$.
  Se $\mathfrak{a} \cap S \neq \emptyset$, sia $s \in \mathfrak{a} \cap S$. Allora $\frac{s}{1} \in \mathfrak{a}^e$ è invertibile. Viceversa, se $\mathfrak{a}^e = S^{-1}A$, $\frac{1}{1} \in \mathfrak{a}^e \Rightarrow \frac{1}{1} = \frac{a}{s}$, per qualche $a \in \mathfrak{a}, s \in S$. Questo, per definizione di anello di frazioni, equivale a chiedere che esista $u \in S$ tale che $u(a - s) = 0$. Concludiamo poiché $\mathfrak{a} \ni ua = us \in S$.
- Se $\mathfrak{q}$ è un ideale primo di $S^{-1}A$, allora $f^{-1}(\mathfrak{q})$ è un ideale primo di $A$. Questo vale per un generico omomorfismo: $x_1 \cdot x_2 \in f^{-1}(\mathfrak{q}) \Leftrightarrow f(x_1 \cdot x_2) \in \mathfrak{q} \Leftrightarrow f(x_1) \cdot f(x_2) \in \mathfrak{q} \Leftrightarrow f(x_1) \in \mathfrak{q}$ oppure $f(x_2) \in \mathfrak{q} \Leftrightarrow x_1 \in f^{-1}(\mathfrak{q})$ oppure $x_2 \in f^{-1}(\mathfrak{q})$.
  Viceversa, consideriamo un ideale primo $\mathfrak{p}$ di $A$ che non interseca $S$ e consideriamo $\frac{x}{s}, \frac{y}{t}$, due elementi di $S^{-1}A$ tali che $\frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st} \in S^{-1}\mathfrak{p}$. Allora $\frac{xy}{st} = \frac{z}{u}$ per qualche $z \in \mathfrak{p}, u \in S$ ed esiste $v \in S$ tale che $v(uxy - zst) = 0$. Poiché $z \in \mathfrak{p}$ allora $vzst \in \mathfrak{p} \Rightarrow uvxy \in \mathfrak{p}$. Ma poiché $\mathfrak{p} \cap S = \emptyset$, necessariamente $xy \in \mathfrak{p} \Leftrightarrow x \in \mathfrak{p}$ oppure $y \in \mathfrak{p}$, ovvero $\frac{x}{s} \in S^{-1}\mathfrak{p}$ oppure $\frac{y}{t} \in S^{-1}\mathfrak{p}$. Quindi $S^{-1}\mathfrak{p}$ è primo.

□

**Osservazione 1.3.9.** La condizione $\mathfrak{p} \cap S = \emptyset$ nel terzo punto del Teorema 1.3.8 è fondamentale; se così non fosse, infatti, per il secondo punto otterremmo che $S^{-1}\mathfrak{p} = S^{-1}A$, che non è primo per definizione.

**Corollario 1.3.10.** *Dato $\mathfrak{p}$ ideale primo di $A$, gli ideali primi di $A_\mathfrak{p}$ sono in corrispondenza biunivoca con gli ideali primi di $A$ contenuti in $\mathfrak{p}$.*

*Dimostrazione.* Basta applicare i risultati precedenti a $S = A \setminus \mathfrak{p}$. □

## 1.4 Anelli noetheriani

Gli anelli *noetheriani* sono probabilmente una delle più importanti classi di anelli dell'Algebra Commutativa. Uno dei motivi per cui tale proprietà è considerata così utile è che essa viene conservata da numerose operazioni di base.

**Definizione 1.4.1.** Un anello $A$ si dice *noetheriano* se vale una delle seguenti condizioni equivalenti:

1. Ogni catena crescente di ideali è stazionaria (ovvero, data $(\mathfrak{a}_m)_{m\geq 1}, \mathfrak{a}_m \subset \mathfrak{a}_{m+1}, \exists n$ tale che $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$);

2. Ogni famiglia non vuota di ideali di $A$ ha un elemento massimale per inclusione;

3. Ogni ideale è finitamente generato.

*Dimostrazione.* Dimostriamo che le condizioni sono equivalenti.
1) $\Rightarrow$ 2). Se per assurdo 2) fosse falsa, esisterebbe una famiglia di ideali senza elemento massimale, e quindi potrebbe essere costruita in maniera induttiva una catena infinita, strettamente crescente, che contraddirebbe la 1).
2) $\Rightarrow$ 3). Consideriamo un ideale $\mathfrak{a}$ e la famiglia $\Sigma$ di tutti i suoi sottoideali finitamente generati. $\Sigma$ non è vuota perché $(0) \in \Sigma$, quindi ha un elemento massimale che chiamiamo $\mathfrak{a}_0$. Se per assurdo $\mathfrak{a}_0 \neq \mathfrak{a}$, consideriamo l'ideale $\mathfrak{a}_0 + Ax, x \in \mathfrak{a}, x \notin \mathfrak{a}_0$. Questo ideale è finitamente generato e contiene $\mathfrak{a}_0$, il che è assurdo. Quindi $\mathfrak{a}_0 = \mathfrak{a}$, che quindi è finitamente generato.
3) $\Rightarrow$ 1). Sia $(\mathfrak{a}_m)_{m\geq 1}$ una catena crescente di ideali di $A$ e sia $\mathfrak{a} = \bigcup_{m=1}^{\infty} \mathfrak{a}_m$. $\mathfrak{a}$ è un ideale e quindi è finitamente generato, da certi $x_1, \ldots, x_r$. Poiché ogni $x_i$ appartiene ad $\mathfrak{a}$, in particolare esisteranno degli $\mathfrak{a}_{n_i}$ per cui $x_i \in \mathfrak{a}_{n_i}$. Sia $n = max_i n_i$. Allora ogni $x_i \in \mathfrak{a}_n$, per cui $\mathfrak{a} = \mathfrak{a}_n$, e quindi la catena è stazionaria. □

**Esempio 1.4.2.**
1. Un campo $K$ è noetheriano. Infatti i suoi unici ideali sono $\{0\} = (0)$ e $K = (1)$.

2. Ogni dominio a ideali principali è noetheriano. In particolare $\mathbb{Z}$ è noetheriano.

Possiamo estendere questa proprietà anche ai moduli.

**Definizione 1.4.3.** Un modulo $M$ è un *modulo noetheriano* se ogni catena crescente di sottomoduli è stazionaria.

**Osservazione 1.4.4.** Questa condizione è equivalente alle seguenti:

- Ogni sottomodulo di $M$ è finitamente generato;
- Ogni famiglia non vuota di sottomoduli di $M$ ha un elemento massimale per inclusione.

**Osservazione 1.4.5.** Possiamo quindi dare ulteriori caratterizzazioni. Un anello noetheriano $A$ è un $A$-modulo noetheriano. Viceversa, dato $A$ anello noetheriano, un $A$-modulo finitamente generato è un modulo noetheriano.

**Teorema 1.4.6.** *Dato $A$ noetheriano, si dimostrano le seguenti proposizioni.*

- *Dato un anello $B$, se esiste un omomorfismo di $A$ su $B$, allora $B$ è noetheriano.*
- *$A[x]$ è noetheriano. Per induzione su $n$ allora $A[x_1, \ldots, x_n]$ è noetheriano.*
- *Per ogni sottoinsieme moltiplicativo $S$ di $A$, $S^{-1}A$ (e in particolare $A_\mathfrak{p}$) è noetheriano.*

*Dimostrazione.* Si veda [1] capitolo 7. □

# Capitolo 2

# Anelli integralmente chiusi

Delle proprietà di un dominio di Dedekind, che definiremo nel prossimo capitolo, l'essere integralmente chiuso è sicuramente quella che necessita di uno studio più approfondito. Nonostante si abbiano molti risultati teorici che classificano gli anelli integralmente chiusi e le chiusure integrali, la produzione di esempi concreti e, in particolare, la ricerca di una base integrale diventano velocemente problemi intrattabili al crescere della complessità dell'anello. Per il nostro studio fortunatamente, possiamo accontentarci di manipolare chiusure integrali di estensioni algebriche di grado basso, poiché forniscono già una casistica sufficientemente ampia per avere un'idea chiara del comportamento di tali strutture.

## 2.1 Elementi integrali

**Definizione 2.1.1.** Sia $A$ un dominio e $K$ un campo, $A \subset K$. Diciamo che $y \in K$ è *integrale* su $A$ se soddisfa una delle seguenti condizioni equivalenti:

1. Soddisfa un'equazione del tipo

$$y^n + a_{n-1}y^{n-1} + \ldots + a_0 = 0, a_i \in A,$$

   ovvero è una radice di un polinomio monico di $A[x]$. Questa equazione prende il nome di *equazione integrale*;

2. Esiste un $A$-modulo finitamente generato non nullo $M \subset K$ tale che $yM \subset M$.

*Dimostrazione.* Mostriamo che le due condizioni sono equivalenti.
Se $y$ è soluzione di un'equazione integrale, basta considerare il modulo $M =$

$\langle 1, y \ldots, y^{n-1} \rangle$. Viceversa, assumiamo esista $M = \langle v_1, \ldots, v_n \rangle \neq 0$ tale che $yM \subset M$. Allora:

$$\begin{aligned} yv_1 &= a_{11}v_1 + \ldots + a_{1n}v_n \\ &\vdots \\ yv_n &= a_{n1}v_1 + \ldots + a_{nn}v_n. \end{aligned}$$

Trasportando tutto a sinistra dell'uguale otteniamo l'equazione matriciale

$$\begin{pmatrix} y - a_{11} & & & \\ & y - a_{22} & & -a_{ij} \\ & & \ddots & \\ -a_{ij} & & & y - a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = 0.$$

Moltiplicando a sinistra per la matrice dei cofattori $\mathrm{cof}(A)$, otteniamo che

$$\det(A) I \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = 0,$$

quindi, poiché $M \neq 0$, $\det(A) = 0$. Tale determinante è un elemento di $K$ che può essere visto come un polinomio a coefficienti in $K$ di variabile $y$, grado $n$ e coefficiente direttore 1, quindi monico. Di più, tutti i coefficienti di questo polinomio sono somme e prodotti di $a_{ij}$, i quali però appartengono tutti all'anello $A$, che è chiuso per somme e prodotti. Quindi questo determinante è effettivamente un'equazione integrale per $y$ in $A$. □

**Esempio 2.1.2.** Ricordiamo che un numero $\alpha \in \mathbb{C}$ è chiamato *numero algebrico* se esiste un polinomio non nullo $f(x) \in \mathbb{Q}[x], f(\alpha) = 0$. Se $f(x) \in \mathbb{Z}[x]$ ed è monico, $\alpha$ è integrale su $\mathbb{Z}$ ed è chiamato *intero algebrico*. Ovviamente tutti gli interi algebrici sono numeri algebrici ma non vale il viceversa.

**Teorema 2.1.3.** *Se $r \in \mathbb{Q}$ è un intero algebrico, allora $r \in \mathbb{Z}$.*

*Dimostrazione.* Sia $r = \frac{c}{d}, (c, d) = 1$ un intero algebrico. Allora $r$ è radice di un polinomio intero monico $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Allora

$$\begin{aligned} f(r) = (\frac{c}{d})^n + \ldots + a_0 = 0 \\ \Leftrightarrow c^n + a_{n-1}c^{n-1}d + \ldots + a_0 d^n = 0. \end{aligned}$$

Allora $c^n$ è un multiplo di $d$, ma poiché $(c, d) = 1$, questo è vero se e solo se $d = \pm 1 \Leftrightarrow r = \pm c \in \mathbb{Z}$. □

**Osservazione 2.1.4.** Questo è un caso particolare di 2.2.6 con $K = \mathbb{Q}$; in effetti osserveremo che basterà verificare che il polinomio minimo di $r$ sia a coefficienti interi.

**Definizione 2.1.5.** Dati $A, B$ con $A \subset B$, $B$ si dice *integrale* su $A$ se tutti gli elementi di $B$ sono integrali su $A$.

**Definizione 2.1.6.** Sia $A \subset K$, $K$ campo. L'insieme degli elementi di $K$ integrali su $A$ si chiama *chiusura integrale* di $A$. Banalmente, la chiusura integrale di $A$ è integrale su $A$.

**Teorema 2.1.7.** *La chiusura integrale è un anello.*

*Dimostrazione.* Siano $x, y \in K$ integrali su $A$. Allora esistono $M, N$ $A$-moduli non nulli finitamente generati tali che $xM \subset M$, $yN \subset N$. Consideriamo quindi l'$A$-modulo $MN$: esso è non nullo, finitamente generato ed è invariante tramite moltiplicazione per $x \pm y$ e $xy$. □

**Definizione 2.1.8.** Diciamo che $A$ è *integralmente chiuso in un campo $K$* se contiene la propria chiusura integrale, ovvero se tutti gli elementi di $K$ integrali su $A$ appartengono ad $A$. Diciamo semplicemente che $A$ è *integralmente chiuso* se è integralmente chiuso nel suo campo dei quozienti $Q(A)$.

Abbiamo dunque già mostrato che $\mathbb{Z}$ è integralmente chiuso. Più in generale vale che

**Teorema 2.1.9.** *Ogni UFD è integralmente chiuso.*

*Dimostrazione.* La dimostrazione per un generico UFD è simile a quella data per il Teorema 2.1.3. □

**Lemma 2.1.10.** *Sia $A \subset B$, $x_1, \ldots, x_n \in B$ integrali su $A$. L'anello $A[x_1, \ldots, x_n]$ è un $A$-modulo finitamente generato.*

*Dimostrazione.* Per induzione su $n$.
Passo base ($n = 1$). Dall'equazione integrale di $x$ abbiamo che

$$x^{n+r} = -(a_1 x^{n+r-1} + \ldots + a_n x^r)$$

per ogni $r \geq 0$; quindi tutte le potenze positive di $x$ appartengono all'$A$-modulo generato da $(1, x, \ldots, x^{n-1})$. Ne segue che $A[x]$ come $A$-modulo è generato da $(1, x, \ldots, x^{n-1})$.
Passo induttivo ($n > 1$). Sia $A_r = A[x_1, \ldots, x_r]$. Allora $A_n = A_{n-1}[x_n]$ è un $A_{n-1}$-modulo finitamente generato (poiché $x_n$ è integrale su $A_{n-1}$). Ma per ipotesi induttiva $A_{n-1}$ è un $A$-modulo finitamente generato, quindi $A_n$ è un $A$-modulo finitamente generato. □

**Corollario 2.1.11.** *$A \subset B \subset C$. Se $B$ è integrale su $A$ e $C$ è integrale su $B$, allora $C$ è integrale su $A$.*

*Dimostrazione.* Sia $x \in C$. Esso soddisfa un'equazione del tipo

$$x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0, b_i \in B.$$

Poiché $b_0, \ldots, b_n$ sono integrali su $A$, $D = A[b_0, \ldots, b_{n-1}]$ è un $A$-modulo finitamente generato; inoltre $D[x]$ è finitamente generato su $D$, quindi $D[x]$ è un $A$-modulo finitamente generato. Poiché $x \in D[x]$, abbiamo anche che la condizione $xD[x] \subset D[x]$ è rispettata. □

**Teorema 2.1.12.** *Siano $A \subset B$, $B$ integrale su $A$.*

- *$\mathfrak{b}$ ideale di $B$ e $\mathfrak{a} = \mathfrak{b}^c = A \cap \mathfrak{b}$. Allora $B/\mathfrak{b}$ è integrale su $A/\mathfrak{a}$.*
- *Se $S$ è un sottoinsieme moltiplicativo di $A$, $S^{-1}B$ è integrale su $S^{-1}A$.*

*Dimostrazione.* Consideriamo $x \in B, x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, a_i \in A$.

- Riduciamo l'equazione mod $\mathfrak{b}$ per ottenere un'equazione integrale per $[x]_{\mathfrak{b}}$ a coefficienti in $A/\mathfrak{a}$.
- Dividendo l'equazione per $s^n$, otteniamo $(\frac{x}{s})^n + \frac{a_1}{s}(\frac{x}{s})^{n-1} + \ldots + \frac{a_n}{s^n} = 0$. Questa è un'equazione integrale per $\frac{x}{s} \in B$, a coefficienti in $S^{-1}A$. Allora $\frac{x}{s}$ è integrale su $S^{-1}A$.

□

**Teorema 2.1.13.** *Siano $A \subset B$ domini di integrità, $B$ integrale su $A$. $B$ è un campo se e solo se $A$ è un campo.*

*Dimostrazione.* Supponiamo $A$ sia un campo; $y \in B, y \neq 0$. Sia

$$y^n + a_{n-1}y^{n-1} + \ldots + a_0 = 0,$$

la sua equazione integrale di grado minimo. Poiché $B$ è un dominio di integrità $a_0 \neq 0$, quindi $y^{-1} = -a_0^{-1}(y^{n-1} + \ldots + a_1) \in B$, da cui $B$ è un campo. Viceversa, supponiamo che $B$ sia un campo; $x \in A, x \neq 0$. Ma allora $x$ appartiene anche a $B$ e quindi anche $x^{-1}$, che esiste nel campo $B$, è integrale su $A$. Allora abbiamo un'equazione integrale

$$x^{-m} + a'_{m-1}x^{-m+1} + \ldots + a'_0 = 0,$$

da cui $x^{-1} = -(a'_{m-1} + \ldots + a'_0 x^{m-1}) \in A$; quindi $A$ è un campo. □

**Corollario 2.1.14.** *$A \subset B$, $B$ integrale su $A$. Sia $\mathfrak{q}$ un ideale primo di $B$ e sia $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$. Allora $\mathfrak{q}$ è massimale se e solo se $\mathfrak{p}$ lo è.*

*Dimostrazione.* Per definizione, $A/\mathfrak{p}$ e $B/\mathfrak{q}$ sono entrambi domini di integrità. Da 2.1.12 $B/\mathfrak{q}$ è integrale su $A/\mathfrak{p}$. Concludiamo da 2.1.13 e dalla definizione di ideale massimale. □

## 2.2 Anello degli interi algebrici

Ci concentriamo ora sulla struttura algebrica dell'anello degli interi algebrici, ovvero gli elementi integrali di un campo di numeri. Diamo prima qualche definizione.

**Definizione 2.2.1.** Un *campo di numeri* $K$ è un sottocampo di $\mathbb{C}$, estensione finita di grado $n$ del campo $\mathbb{Q}$.

**Esempio 2.2.2.** $\mathbb{Q}$ stesso è un campo di numeri, poiché estensione di grado 1 di $\mathbb{Q}$.
Un esempio non banale è dato dal campo quadratico $\mathbb{Q}[\sqrt{n}], n \in \mathbb{Z} \setminus \{0, 1\}$ privo di fattori quadratici.

**Definizione 2.2.3.** Dato $K$ campo di numeri, la sua chiusura integrale su $\mathbb{Z}$, denotata con $O_K$, è chiamata *anello degli interi algebrici* di $K$.

**Esempio 2.2.4.** $O_{\mathbb{Q}} = \mathbb{Z}$.

Come avremo modo di approfondire, il nome *interi algebrici* denota un profondo legame tra essi e gli interi di $\mathbb{Z}$: l'esempio precedente mostra appunto che gli interi sono un caso particolare di anello di interi algebrici. Vediamo subito un'altra importante analogia: come i razionali possono essere definiti partendo da rapporti di interi, i campi di numeri algebrici sono il campo delle frazioni degli interi algebrici.

**Teorema 2.2.5.** *Sia $K$ un campo di numeri algebrici. $Q(O_K) = K$. In particolare, $Q(O_{\mathbb{Q}}) = Q(\mathbb{Z}) = \mathbb{Q}$.*

*Dimostrazione.* Un'inclusione è ovvia. Infatti,

$$Q(O_K) = \left\{ \frac{\alpha}{\beta}, \text{ tale che } \alpha, \beta \in O_K, \beta \neq 0 \right\} \subset K.$$

Viceversa, sia $x \in K$; allora $x$ è un numero algebrico, quindi soddisfa un'equazione $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$ con $a_n \neq 0$ e $a_i \in \mathbb{Q}$; a meno di moltiplicazione per una costante, possiamo però considerare $a_i \in \mathbb{Z}$. Si osserva facilmente che moltiplicando per $a_n^{n-1}$ si ottiene un'equazione integrale per $a_n x$. Quindi $a_n x$ è un intero algebrico. Allora, $x = \frac{a_n x}{a_n} \in Q(O_K)$. □

Iniziamo dunque a dare una serie di risultati che ci permetteranno di descrivere questi anelli. Questo primo teorema ci consente di limitare lo studio dell'integralità di un elemento al suo polinomio minimo.

**Teorema 2.2.6.** *Sia $\alpha \in K$. Il suo polinomio minimo $f$ è a coefficienti interi se e solo se $\alpha$ è integrale su $\mathbb{Z}$.*

*Dimostrazione.* Ovviamente se $f$ è a coefficienti interi, esso rappresenta un'equazione integrale di cui $\alpha$ è soluzione. Supponiamo invece per assurdo che $\alpha$ soddisfi un'equazione integrale $g \in \mathbb{Z}[x]$, ma $f \notin \mathbb{Z}[x]$. Il polinomio $g \in (f)$, ideale generato da $f$ in $\mathbb{Q}[x]$. Scomponiamo $g$ nella sua fattorizzazione in polinomi irriducibili $g = \prod g_i$ in $\mathbb{Z}[x]$, osservando che anche tutti i polinomi $g_i$ sono monici. Allora deve esistere almeno un $i$ tale che $f|g_i$, ma questo è assurdo perché $f$ e $g_i$ sono irriducibili e non possono essere associati perché per costruzione sono monici. □

Per quanto dimostrato su un generico elemento integrale in 2.1.10, abbiamo anche che

**Corollario 2.2.7.** *Un elemento $\alpha$ è un intero algebrico se, equivalentemente*

- $\exists M \neq 0$, *$\mathbb{Z}$-modulo finitamente generato contenuto in $\mathbb{C}$, tale che $\alpha M \subset M$.*
- *$\mathbb{Z}[\alpha]$ è uno $\mathbb{Z}$-modulo finitamente generato;*

Enunciamo ora uno dei teoremi fondamentali che utilizzeremo per studiare le chiusure integrali.

**Teorema 2.2.8.** *Sia $A$ un dominio integralmente chiuso e $Q(A)$ il suo campo dei quozienti. Sia $K$ un'estensione algebrica, finita separabile di $Q(A)$ e $B$ la chiusura integrale di $A$ in $K$. Allora esiste una base $v_1, \ldots, v_n$ di $K$ su $Q(A)$ tale che $B \subset \sum_{j=1}^{n} Av_j$.*

Questo teorema, vale per un generico $A$, ma verrà dimostrato nel caso $\mathbb{Z} \subset \mathbb{Q} \subset K$.

*Dimostrazione.* Se $v$ è un elemento di $K$ allora per ipotesi è algebrico su $\mathbb{Q}$ e quindi soddisfa un'equazione della forma

$$a_0 v^r + a_1 v^{r-1} + \ldots + a_n = 0, a_i \in \mathbb{Z}.$$

Moltiplicando per $a_0^{r-1}$ otteniamo un'equazione integrale per $a_0 v := u$. Questo vuol dire che data una qualsiasi base di $K$ su $\mathbb{Q}$, possiamo moltiplicare i suoi elementi per opportuni interi per ottenere una base di $K$ $u_1, \ldots u_n$ integrale su $\mathbb{Z}$. Per proseguire dimostriamo questo semplice Lemma.

**Lemma 2.2.9.** *Definiamo innanzitutto l'applicazione traccia $T$; la traccia $T(\alpha)$ di $\alpha \in K$ è la traccia dell'applicazione lineare $x \mapsto \alpha x$ o, analogamente, fissata una base per $K$ come $\mathbb{Q}$-spazio vettoriale, è la traccia della matrice ad essa associata. La forma bilineare $B(x, y) \mapsto T(xy)$ è non degenere.*

*Dimostrazione.* Consideriamo una $\mathbb{Q}$-base $\omega_1, \ldots, \omega_n$ per $K$; la matrice associata a $B(x, y)$ è allora

$$(B(\omega_i, \omega_j)) = (T(\omega_i \omega_j)).$$

Per un risultato noto della teoria di Galois, (si veda [3] capitolo 14) possiamo scrivere $T(\omega_i\omega_j) = \sum_k \sigma_k(\omega_i)\sigma_k(\omega_j)$, da cui deduciamo che

$$(B(\omega_i, \omega_j)) = \Omega\Omega^T,$$

dove $\Omega_{ij} = \sigma_i(\omega_j)$ è non singolare poiché $\omega_1, \ldots, \omega_n$ sono una base per $K$ e i $\sigma_i$ sono tutti distinti (quindi tutte le righe sono linearmente indipendenti); allora anche la matrice $B$ è non singolare e quindi l'applicazione è non degenere. □

Possiamo quindi considerare la base duale $v_1, \ldots, v_n$ di $K$ su $\mathbb{Q}$, definita da $T(u_i v_j) = \delta_{ij}$. Consideriamo ora $x \in O_K$ della forma $x = \sum_j x_j v_j, x_j \in \mathbb{Q}$. Allora $xu_i \in O_K$ per 2.1.7.

**Lemma 2.2.10.** *Sia $K$ campo di numeri algebrico di grado $n$ su $\mathbb{Q}$.*
*Se $\alpha \in O_K$, $T(\alpha) \in \mathbb{Z}$.*

*Dimostrazione.* Consideriamo $\alpha\omega_i = \sum_{j=1}^n a_{ij}\omega_j$ per ogni $i$. Allora abbiamo che

$$\alpha^{(k)}\omega_i^{(k)} = \sum_{j=1}^n a_{ij}\omega_j^{(k)} = \sum_{j=1}^n \delta_{jk}\alpha^{(j)}\omega_i^{(j)}, \forall i, k,$$

dove $\alpha^{(k)}$ è il $k$-esimo coniugato di $\alpha$ e $\delta_{ij}$ è l'usuale funzione delta di Kronecker. Definendo le matrici

$$A_0 = (\alpha^{(i)}\delta_{ij}), \Omega = (\omega_i^{(j)}), A = (a_{ij}),$$

otteniamo che $A_0 = \Omega^{-1}A\Omega$, dunque $T(A) = T(A_0)$. La traccia $T(A_0)$ è la somma dei coniugati di $\alpha$ e quindi, a meno del segno, il coefficiente del termine $x^{n-1}$ nel polinomio minimo di $\alpha$. Poiché $\alpha$ è integrale per ipotesi, tale coefficiente è intero. □

Quindi $T(xu_i) \in \mathbb{Z}$, ma

$$T(xu_i) = T(\sum_j x_j u_i v_j) = \sum_j x_j T(u_i v_j) = \sum_j x_j \delta_{ij} = x_i.$$

Quindi $x_i \in \mathbb{Z}$ e quindi $x \in \sum_{j=1}^n \mathbb{Z}v_j$, da cui il teorema. □

Questo teorema è di tipo costruttivo, poiché effettivamente ci consente di costruire esplicitamente lo $\mathbb{Z}$-modulo che contiene la chiusura integrale. Utilizzeremo questo risultato per ridurre la ricerca degli elementi integrali di $\mathbb{Z}$ in $K$ ai soli elementi di questo modulo.
Infine vale il seguente

**Teorema 2.2.11.** *Sia $M$ uno $\mathbb{Z}$-modulo finitamente generato, $\alpha_1, \ldots, \alpha_m$ un insieme di generatori per $M$ e sia $N$ un sottomodulo di $M$. Allora esistono $\beta_1, \ldots, \beta_n \in N$ con $n \leq m$ tali che*

$$N = \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n,$$
$$\beta_i = \sum_{j \geq i} p_{ij}\alpha_j, p_{ij} \in \mathbb{Z}.$$

*Dimostrazione.* Essendo $\mathbb{Z}$ un PID, quindi noetheriano, un modulo su $\mathbb{Z}$ è anch'esso noetheriano. Procediamo quindi per induzione sul numero di generatori di $M$.
Per $m = 0$ il risultato è banale. Supponiamo quindi vero il risultato per tutti gli $\mathbb{Z}$-moduli con $m-1$ o meno generatori e dimostriamolo per $m$. Chiamiamo $M'$ il sottomodulo generato da $\alpha_2, \ldots, \alpha_m$ e $N' = N \cap M'$.
Se $N = N'$, la tesi è vera per l'ipotesi induttiva. Supponiamo allora $N \neq N'$ e consideriamo $A$, l'insieme di tutti gli interi $k$ tali che esistano $k_2, \ldots, k_m$ con $k\alpha_1 + k_2\alpha_2 + \ldots + k_m\alpha_m \in N$. Poichè $N$ è un sottomodulo di uno $\mathbb{Z}$-modulo, deduciamo che $A$ è un sottogruppo di $\mathbb{Z}$. Tutti i sottogruppi additivi di $\mathbb{Z}$ sono della forma $m\mathbb{Z}$ per un certo intero $m$, quindi $A = k_{11}\mathbb{Z}$ per un certo $k_{11}$. Allora sia $\beta_1 = k_{11}\alpha_1 + \ldots + k_{1m}\alpha_m \in N$. Per $\alpha \in N$ allora,

$$\alpha = \sum_{i=1}^{m} h_i\alpha_i,$$

con $h_i \in \mathbb{Z}$ e $h_1 \in A$, quindi $h_1 = ak_{11}$. Allora $\alpha - a\beta_1 \in N'$. Quindi per ipotesi induttiva esistono

$$\beta_i = \sum_{j \geq i} k_{ij}\alpha_j, i = 2, 3, \ldots, n$$

che generano $N'$ su $\mathbb{Z}$ e che soddisfano tutte le condizioni richieste. È chiaro che aggiungere $\beta_1$ fornisce un insieme di generatori per $N$. □

**Definizione 2.2.12.** Dato $K$ campo di numeri algebrico di grado $n$ su $\mathbb{Q}$ e $O_K$ il suo anello degli interi, diciamo che $\omega_1, \ldots, \omega_n$ è una *base integrale* per $K$ se

- $\omega_1, \ldots, \omega_n$ è una $\mathbb{Q}$-base per $K$
- $\omega_i \in O_K, \forall i$
- $O_K = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$.

**Corollario 2.2.13.** *$O_K$ ha una base integrale.*

*Dimostrazione.* Questo risultato è un'immediata conseguenza dei due teoremi precedenti. Consideriamo per comodità di notazione $n = 2$ (il ragionamento può essere facilmente generalizzato a un generico $n$). Per 2.2.8 possiamo scrivere

$$O_K \subset M := \mathbb{Z}v_1 + \mathbb{Z}v_2,$$

dove $v_1, v_2$ è una $\mathbb{Q}$-base di $K$. Allora segue direttamente da 2.2.11 che esistono $\omega_1, \ldots, \omega_r \in O_K$ con $r \leq 2$ tali che

$$O_K = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_r,$$

$$\omega_i = \sum_{j \geq i} p_{ij} v_j, \ p_{ij} \in \mathbb{Z}.$$

Mostriamo innanzitutto che $r = 2$, ovvero che la dimensione di $O_K$ è proprio uguale al grado dell'estensione. Se per assurdo $r < 2$, deve essere $r = 1$, poiché $O_K \neq \{0\}$. Allora, un sistema di generatori di $O_K$ è dato dall'elemento $\omega_1 = p_{11}v_1 + p_{12}v_2$. Poiché però esiste un $m \neq 0, m \in \mathbb{Z}$ tale che $mv_1, mv_2$ è un insieme linearmente indipendente di $O_K$, si ha che

$$mv_1 = a_1\omega_1,$$

$$mv_2 = a_2\omega_1,$$

con $a_1, a_2 \neq 0$. Allora, $a_2(a_1\omega_1) - a_1(a_2\omega_1) = (a_2m)v_1 - (a_1m)v_2 = 0$, che è assurdo perché $v_1, v_2$ è una base. Quindi $r = 2$.
Consideriamo quindi $\omega_1, \omega_2$ sistema di generatori per $O_K$ con

$$\begin{aligned} \omega_1 &= p_{11}v_1 + p_{12}v_2, \\ \omega_2 &= p_{22}v_2, \end{aligned}$$

e mostriamo che è linearmente indipendente. Siano $(a, b) \neq (0, 0)$ tali che $a\omega_1 + b\omega_2 = 0$, o, equivalentemente,

$$ap_{11}v_1 + (ap_{12} + bp_{22})v_2 = 0.$$

Se $a = 0$ (e quindi $b \neq 0$), otteniamo che $bp_{22} = 0 \Leftrightarrow p_{22} = 0$. Allora $\omega_2 = 0$, che è assurdo.

Se $a \neq 0$, allora $p_{11} = 0$. Quindi, $\omega_1, \omega_2$ sono linearmente dipendenti, entrambi multipli di $v_2$. Allora, definendo $p = MCD(p_{12}, p_{22})$ e $\omega = pv_2$ otterremmo che $O_K = \mathbb{Z}v_2$, che è assurdo.
Osserviamo infine che $\omega_1, \omega_2$ è certamente una $\mathbb{Q}$-base di $K$. Allora, $\omega_1, \omega_2$ è una base integrale per $K$. □

Da questo corollario otteniamo inoltre che

**Teorema 2.2.14.** *$O_K$ è noetheriano.*

*Dimostrazione.* Avendo una base integrale, $O_K$ è uno $\mathbb{Z}$-modulo finitamente generato. □

**Teorema 2.2.15.** *$O_K$ è integralmente chiuso.*

*Dimostrazione.* Consideriamo una base integrale per $K$ su $\mathbb{Q}$, $\alpha_1, \ldots, \alpha_n$; allora $O_K = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Se $\alpha \in K$ è integrale su $O_K$, deve esistere

$$M = O_K v_1 + \ldots + O_K v_m, \text{ tale che } \alpha M \subset M.$$

Allora $M = \sum_{i=1}^{n} \sum_{j=1}^{m} \mathbb{Z}\alpha_i v_j$ è uno $\mathbb{Z}$-modulo finitamente generato con $\alpha M \subset M$, quindi $\alpha$ è integrale su $\mathbb{Z}$. Quindi, per definizione, $\alpha \in O_K$. □

### 2.2.1 Estensioni quadratiche

Cerchiamo ora di determinare una base integrale nel caso di estensioni quadratiche semplici $K = \mathbb{Q}[\sqrt{n}]$.

**Osservazione 2.2.16.** Ovviamente $\sqrt{n}$ è integrale su $\mathbb{Z}$, quindi $\mathbb{Z}[\sqrt{n}] \subset O_K$.

**Esempio 2.2.17.** Studiamo la chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{3}]$. Una base di $\mathbb{Q}[\sqrt{3}]$ su $\mathbb{Q}$ è data da $(1, \sqrt{3})$ che, essendo già integrali su $\mathbb{Z}$, possono essere utilizzati come base per la costruzione data dalla dimostrazione del Teorema 2.2.8. Considerando un generico elemento $\alpha = a + b\sqrt{3}$, la sua traccia è data dalla traccia della matrice associata a $x \mapsto \alpha x$. Quindi

$$T(\alpha) = T \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} = 2a.$$

Troviamo quindi la base duale di $(v_1, v_2)$:

$$\begin{cases} T(u_1 \cdot v_1) = 1 \\ T(u_1 \cdot v_2) = 0 \\ T(u_2 \cdot v_1) = 0 \\ T(u_2 \cdot v_2) = 1 \end{cases}$$

Da cui $v_1 = \frac{1}{2}$ e $v_2 = \frac{1}{6}\sqrt{3}$. Allora $O_{\mathbb{Q}[\sqrt{3}]} \subset \left\{ \frac{1}{2}a + \frac{1}{6}b\sqrt{3}, a, b \in \mathbb{Z} \right\}$.

Vogliamo mostrare ora che effettivamente $O_{\mathbb{Q}[\sqrt{3}]} = \mathbb{Z}[\sqrt{3}]$.

**Osservazione 2.2.18.** Consideriamo un elemento $\alpha \in \left\{\frac{1}{2}a + \frac{1}{6}b\sqrt{3}, a, b \in \mathbb{Z}\right\}$ integrale su $\mathbb{Z}$ e mostriamo che necessariamente $a$ è pari e $b$ è multiplo di 6. Infatti, dato $\alpha = \frac{1}{2}a + \frac{1}{6}b\sqrt{3}$, si costruisce facilmente il polinomio minimo $f$

$$f(x) = x^2 - ax + \frac{3a^2 - b^2}{12}.$$

Se $\alpha$ è integrale allora per il Teorema 2.2.6 i coefficienti di $f$ sono interi e in particolare lo deve essere il termine noto. Allora $\exists k \in \mathbb{Z}$ tale che,

$$\begin{aligned} \frac{3a^2 - b^2}{12} &= k \\ \Leftrightarrow b^2 &= 3(a^2 - 4k) \\ &\Rightarrow 3|b. \end{aligned}$$

Inoltre $a$ e $b$ devono essere entrambi pari, poiché riducendo la condizione $3a^2 - b^2 = 12k$ otteniamo

$$a^2 + b^2 \equiv 0 \bmod 4,$$

che ha soluzione se e solo se $a^2 \equiv b^2 \equiv 0 \Leftrightarrow a, b$ sono pari.

Quindi $\mathbb{Z}[\sqrt{3}]$ è integralmente chiuso e una base integrale per $O_{\mathbb{Q}[\sqrt{3}]}$ è data da $(1, \sqrt{3})$.

**Esempio 2.2.19.** Consideriamo ora $K = \mathbb{Q}[\sqrt{5}]$. Per le osservazioni precedenti $\mathbb{Z}[\sqrt{5}] \subset O_K$, ma $\phi = \frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$ è integrale su $\mathbb{Z}$, poiché $\phi^2 - \phi - 1 = 0$. È evidente come in questo caso $(1, \sqrt{5})$ non rappresenti una base integrale.

Vale il seguente teorema

**Teorema 2.2.20.** *Dato $n \neq 0, 1$, privo di fattori quadratici, $\mathbb{Z}[\sqrt{n}]$ è integralmente chiuso se e solo se $n \not\equiv 1 \mod 4$.*

*Dimostrazione.* Generalizziamo l'Esempio 2.2.17.
La chiusura integrale di $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{n}]$ è contenuta nello $\mathbb{Z}$-modulo

$$M = \left\{\frac{1}{2}a + \frac{1}{2n}b\sqrt{n}, a, b \in \mathbb{Z}\right\}.$$

Sia $\alpha \in M$ un elemento integrale su $\mathbb{Z}$. Il polinomio minimo di $\alpha$ è

$$f(x) = x^2 - ax + \frac{na^2 - b^2}{4n}.$$

Inoltre, poiché $f$ deve essere a coefficienti interi, $b$ deve essere multiplo di $n$ (e scriviamo $b = nc$), e $a$ e $c$ devono avere la stessa parità. Allora $\alpha$ è della forma $\alpha = \frac{1}{2}a + \frac{1}{2}c\sqrt{n}$.
Per mostrare la tesi basta verificare che $n \equiv 1 \mod 4$ se e solo se esistono $a$ e $c$ dispari tali che $\alpha$ è integrale su $\mathbb{Z}$.
Supponiamo $n \equiv 1 \mod 4$. Allora si verifica facilmente che $\frac{1+\sqrt{n}}{2}$ è integrale, con equazione integrale $x^2 - x + \frac{1-n}{4} = 0$. Viceversa, supponiamo esistano $a, c$ dispari tali che $\frac{1}{2}(a + c\sqrt{n})$ sia integrale. Il suo polinomio minimo è

$$x^2 - x + \frac{a^2 - nc^2}{4},$$

che è intero se e solo se $a^2 - nc^2 \equiv 0 \mod 4 \Leftrightarrow 1 - n \equiv 0 \mod 4$ (poiché se $a$ e $c$ sono dispari, i loro quadrati sono congrui a 1), da cui la tesi. □

**Esempio 2.2.21.** $\frac{7+5\sqrt{29}}{2}$ è integrale su $\mathbb{Z}$ perché soluzione dell'equazione integrale $x^2 - 7x - 169 = 0$.

Ripercorrendo la dimostrazione di 2.2.20 otteniamo anche il seguente risultato che esaurisce lo studio delle estensioni quadratiche.

**Teorema 2.2.22.** *Dato $n \neq 0, 1$ privo di fattori quadratici, una base integrale per $O_{\mathbb{Q}[\sqrt{n}]}$ è data da:*

- $(1, \frac{1+\sqrt{n}}{2})$, *se* $n \equiv 1 \mod 4$;
- $(1, \sqrt{n})$, *se* $n \equiv 2, 3 \mod 4$.

### 2.2.2 Estensioni algebriche

Studiamo ora un generico campo di numeri $K = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$. Per trovarne una base integrale, dovremo definire un'invariante del campo $K$ chiamata *discriminante*.
Richiamiamo innanzitutto il seguente risultato fondamentale.

**Teorema 2.2.23.** *Se $\alpha$ e $\beta$ sono due numeri algebrici, allora esiste $\theta$, numero algebrico, tale che $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$.*

*Dimostrazione.* Siano $f, g$ rispettivamente i polinomi minimi di $\alpha$ e $\beta$. Vogliamo mostrare che $\exists \lambda \in \mathbb{Q}$ tale che $\theta = \alpha + \lambda\beta$ e $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta) := L$.
Sia quindi $\lambda \in \mathbb{Q}$ arbitrario. Chiaramente $L \subset \mathbb{Q}(\alpha, \beta)$. Definiamo $\phi(x) = f(\theta - \lambda x) \in L[x]$. Osserviamo che $\phi(\beta) = f(\alpha) = 0$. Ora possiamo scegliere $\lambda \in \mathbb{Q}$ imponendo che $\beta$ sia l'unica radice comune di $\phi$ e $g$; effettivamente se imponiamo $\phi(\beta_i) \neq 0$ per tutte le radici $\beta_i$ di $g$ diverse da $\beta$, otteniamo un

sistema di disuguaglianze che rende non accettabili solo un numero finito di valori di $\lambda$. Quindi $MCD(\phi(x), g(x)) = (x-\beta) \in L[x]$ e quindi $\beta$, appartiene a $L$. Concludiamo poiché $\theta \in L$ implica che $\theta - \lambda\beta = \alpha \in L$. □

**Corollario 2.2.24.** *Il teorema può essere facilmente generalizzato con un procedimento induttivo per una generica estensione* $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Dato un campo di numeri algebrico $K$ con $[K : \mathbb{Q}] = n$, questo risultato ci consente di lavorare con una base più "comoda" rispetto alle altre, ovvero $(1, \theta, \ldots, \theta^{n-1})$.
Possiamo ora introdurre il discriminante.

**Definizione 2.2.25.** Dato un campo di numeri algebrici $K$ di grado $n$ su $\mathbb{Q}$, sappiamo dalla teoria di Galois (si veda [3] capitolo 14) che esistono $n$ $\mathbb{Q}$-isomorfismi distinti

$$\sigma_i : K \to \mathbb{C},\ i = 1, \ldots, n$$

(dove poniamo per convenzione $\sigma_1 = id$). Definiamo il *discriminante* di $K$ su $\mathbb{Q}$ come

$$\begin{aligned} d_{K/\mathbb{Q}} &: K^n \to \mathbb{C} \\ d_{K/\mathbb{Q}}(a_1, \ldots, a_n) &= [\det(\sigma_i(a_j))]^2 \end{aligned}$$

**Teorema 2.2.26.** $d_{K/\mathbb{Q}}(a) := d_{K/\mathbb{Q}}(1, a, \ldots, a^{n-1}) = \prod_{i>j}(\sigma_i(a) - \sigma_j(a))^2$.

*Dimostrazione.* Definiamo la matrice $\Omega := (\sigma_i(a^{j-1}))$. Allora

$$\Omega = \begin{pmatrix} 1 & a & \cdots & a^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(a) & \cdots & (\sigma_n(a))^{n-1} \end{pmatrix}$$

che è una matrice di Vandermonde, il cui determinante è quindi

$$\det(\Omega) = \prod_{i<j}(\sigma_i(a) - \sigma_j(a)),$$

da cui segue il risultato cercato. □

**Lemma 2.2.27.** *Supponiamo che* $u_i = \sum_{j=1}^{n} a_{ij} v_j, a_{ij} \in \mathbb{Q}, v_j \in K$.

$$d_{K/\mathbb{Q}}(u_1, \ldots, u_n) = (\det(a_{ij}))^2 d_{K/\mathbb{Q}}(v_1, \ldots, v_n).$$

*Dimostrazione.* Per definizione $d_{K/\mathbb{Q}}(u_1, \ldots, u_n) = \det(\sigma_i(u_j))^2$. Ma

$$\sigma_i(u_j) = \sigma_i(\sum_{k=1}^{n} a_{jk} v_k) = \sum_{k=1}^{n} a_{jk} \sigma_i(v_k).$$

Se definiamo le matrici $U = (\sigma_i(u_j))$, $A = (a_{ij})$, $V = (\sigma_i(v_j))$, è chiaro che $U = VA^T$, da cui otteniamo il risultato per il teorema di Binet. □

**Lemma 2.2.28.** *Nelle ipotesi del Lemma 2.2.27 si dimostra che se* $u_1, \ldots, u_n$ *e* $v_1, \ldots, v_n$ *sono basi integrali, si ha* $\det A = 1$.

*Dimostrazione.* Si veda [2] capitolo 4. □

Questo ci permette di dare la seguente definizione.

**Definizione 2.2.29.** Dato un campo di numeri $K$ di grado $n$ su $\mathbb{Q}$ e una base integrale di $K$ $(\omega_i)$, definiamo il *discriminante* di $K$ come

$$d_K = \det(\sigma_i(\omega_j))^2.$$

**Lemma 2.2.30.** $d_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n) = \det(Tr(\omega_i \omega_j))$.

*Dimostrazione.* Definiamo la matrice $M := (\sigma_i(\omega_j))$. Allora è chiaro che

$$d_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n) = \det(M^T M).$$

Ma l'elemento di posto $(i, j)$ di $M^T M$ è proprio

$$\sum_{k=1}^{n} \sigma_k(\omega_i)\sigma_k(\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i \omega_j) = Tr(\omega_i \omega_j),$$

che conclude la dimostrazione. L'ultima uguaglianza sfrutta il fatto che la traccia di un elemento $\alpha$ è il coefficiente di $x^{n-1}$ nel proprio polinomio minimo, che dalla teoria di Galois è proprio uguale alla somma dei suoi coniugati (si veda ad esempio [3] capitolo 14). □

**Corollario 2.2.31.** $d_K \in \mathbb{Z}$.

*Dimostrazione.* $M = (Tr(\omega_i \omega_j))$ è una matrice intera poiché $Tr(\omega_i \omega_j) \in \mathbb{Z}$ da 2.2.10; allora è intero anche il suo determinante. □

**Esempio 2.2.32.** Studiamo ancora il campo $K = \mathbb{Q}(\sqrt{3})$. Sappiamo che una sua base integrale è data da $(1, \sqrt{3})$. L'estensione $\mathbb{Q} \subset K$ è normale di grado 2 e il rispettivo gruppo di Galois è formato da due elementi $\{\sigma_1 = id, \sigma_2\}$, con $\sigma_2(\sqrt{3}) = -\sqrt{3}$. Allora il discriminante vale

$$d_{\mathbb{Q}(\sqrt{3})} = \det \begin{pmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix}^2 = (-2\sqrt{3})^2 = 12.$$

Supponiamo ora vero il seguente risultato

**Lemma 2.2.33.** *Consideriamo $K, L$ due campi di numeri algebrici di grado rispettivamente $m$ e $n$. Se $(d_K, d_L) = 1$ allora $[KL : \mathbb{Q}] = mn$.*

*Dimostrazione.* Si veda [2] capitolo 4. □

Vale il teorema

**Teorema 2.2.34.** *Dati $K, L$ due campi di numeri algebrici di grado rispettivamente $m$ e $n$ tali che $(d_K, d_L) = 1$, siano $(\alpha_1, \ldots, \alpha_m)$ una base integrale di $O_K$ e $(\beta_1, \ldots, \beta_n)$ una base integrale di $O_L$. Allora $(\alpha_i\beta_j)$ è una base integrale per $O_{KL}$.*

*Dimostrazione.* $(\alpha_i\beta_j)$ è una $\mathbb{Q}$-base per $KL$ su $\mathbb{Q}$ per il Lemma 2.2.33. Allora ogni $\omega \in O_{KL}$ può essere scritto come

$$\omega = \sum_{i,j} \frac{m_{ij}}{r} \alpha_i \beta_j,$$

dove $r, m_{ij} \in \mathbb{Z}$ e $MCD(r, m_{ij}) = 1$. Per concludere basta mostrare che $r|d_K$; se così è, allora per simmetria $r|d_L$ e quindi divide anche il loro $MCD$, che è uguale a 1 per ipotesi. Mostriamo quindi che $r|d_K$.
Ogni $\sigma_k : K \to \mathbb{C}$ può essere esteso a $KL$ con $\sigma_{k_{|L}} \equiv id$ imponendo $\sigma_k(\beta_j) = \beta_j$ ([3] capitolo 14). Allora

$$\sigma_k(\omega) = \sum_{i,j} \frac{m_{ij}}{r} \sigma_k(\alpha_i)\beta_j.$$

Poniamo $x_i = \sum_j \frac{m_{ij}\beta_j}{r}$. Per ognuno degli $m$ omomorfismi $\sigma_k$ otteniamo quindi l'equazione

$$\sum_{i=1}^{m} \sigma_k(\alpha_i) x_i = \sigma_k(\omega).$$

Risolvendo per gli $x_i$ otteniamo che $x_i = \frac{\gamma_i}{\delta}$, con

$$\delta = \det(\sigma_k(\alpha_j))$$

$$\gamma_i = \sum_l (-1)^{l+i} A_{li} \sigma(\omega),$$

dove $(A_{li})$ è la matrice dei complementi algebrici di $\sigma_i(\alpha_j)$. Poiché $\delta^2 = d_K$ otteniamo

$$\delta\gamma_i = \sum_{j=1}^{n} \frac{\delta^2 m_{ij}}{r} \beta_j \in O_K,$$

poiché $\delta$ e ciascun $\gamma_i$ sono interi algebrici. Quindi ne segue che i $\frac{d_K m_{ij}}{r}$ sono interi e, quindi, data l'ipotesi di coprimalità tra $m_{ij}$ e $r$, $r|d_K$. □

**Esempio 2.2.35.** Troviamo una base integrale per $\mathbb{Q}(\sqrt{3},\sqrt{5})$.
Poniamo $K=\mathbb{Q}(\sqrt{3})$ e $L=\mathbb{Q}(\sqrt{5})$. Con calcoli analoghi a quelli fatti per trovare $d_K=12$, si mostra che $d_L=5$ e quindi i due discriminanti sono coprimi. Allora, dal teorema precedente, prese $(1,\sqrt{3})$ base integrale per $K$ e $(1,\frac{1+\sqrt{5}}{2})$ base integrale per $L$, una base per $O_{KL}$ è data da

$$(1,\sqrt{3},\frac{1+\sqrt{5}}{2},\sqrt{3}\frac{1+\sqrt{5}}{2}).$$

**Osservazione 2.2.36.** Consideriamo ora $\mathbb{Q}(\sqrt{3},\sqrt{7})$ e poniamo $K=\mathbb{Q}(\sqrt{3})$ e $L=\mathbb{Q}(\sqrt{7})$. Dal Teorema 2.2.20 sappiamo che i rispettivi anelli degli interi algebrici sono $\mathbb{Z}[\sqrt{3}]$ e $\mathbb{Z}[\sqrt{7}]$, ma i discriminanti dei due campi non sono coprimi, per cui il Teorema 2.2.34 non vale. Effettivamente in questo caso $\sqrt{21}\in\mathbb{Q}(\sqrt{3},\sqrt{7})$ e $21\equiv 1 \bmod 4$, per cui $\mathbb{Z}[\sqrt{3},\sqrt{7}]$ non è integralmente chiuso.

Per concludere la discussione, diamo, senza dimostrarlo, un algoritmo generale per la costruzione esplicita di una base integrale per un qualsiasi campo di numeri.

**Teorema 2.2.37.** *Sia $\mathbb{Q}\subset K$ un'estensione algebrica di grado $n$. Supponiamo di avere $a_1,\dots,a_n\in O_K$ linearmente indipendenti su $\mathbb{Q}$. Poniamo*

$$\Delta := d_{K/\mathbb{Q}}(a_1,\dots,a_n).$$

*Per ogni $i$ scegliamo il più piccolo naturale $d_{ii}$ tale che per qualche $d_{ij}\in\mathbb{Z}$*

$$\omega_i=\Delta^{-1}\sum_{j=1}^{i} d_{ij}a_j\in O_K.$$

*Allora, $\omega_1,\dots,\omega_n$ è una base integrale di $O_K$.*

*Dimostrazione.* Si veda [2] capitolo 4. □

**Osservazione 2.2.38.** Osserviamo che, nonostante a livello teorico il problema e la sua risoluzione siano ben chiari, questo algoritmo è chiaramente inefficiente e non può essere utilizzato nella pratica, se non in casi molto specifici. Lo sviluppo di un algoritmo generale efficiente esula dallo scopo di questo elaborato e pertanto non verrà trattato.

### 2.2.3 Ideali in $O_K$

Diamo ora alcuni risultati generali sugli ideali di un anello integralmente chiuso e applichiamoli agli ideali dell'anello $O_K$ degli interi algebrici di un campo di numeri $K$.

**Teorema 2.2.39.** *Sia $\mathfrak{a}$ un ideale $\neq 0$ di $O_K$. $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$.*

*Dimostrazione.* Sia $\alpha \neq 0$ un intero algebrico appartenente ad $\mathfrak{a}$. Se consideriamo il suo polinomio minimo, $\alpha$ soddisfa un'equazione integrale

$$\alpha^r + a_{r-1}\alpha^{r-1} + \ldots + a_0 = 0, a_i \in \mathbb{Z}.$$

Poiché consideriamo il polinomio minimo, in particolare irriducibile, sicuramente $a_0 \neq 0$. Allora $a_0 = -(\alpha^r + \ldots + a_1\alpha)$. Ma $a_0 \in \mathbb{Z}$ mentre il secondo membro dell'equazione è un elemento di $\mathfrak{a}$. □

**Teorema 2.2.40.** *Dato $\mathfrak{p} \neq (0)$ ideale primo di $O_K$, esso contiene uno e un solo primo $p \in \mathbb{Z}$.*

*Dimostrazione.* Da 2.2.39, sicuramente $\mathfrak{p}$ contiene un intero. Poiché dalla definizione di ideale primo, se $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ oppure $b \in \mathfrak{p}$, sicuramente $\mathfrak{p}$ deve contenere un intero primo. Se per assurdo ne contenesse due, diciamo $p$ e $q$, allora dovrebbe contenere anche il loro $MCD$, contraddicendo l'ipotesi $\mathfrak{p} \neq (1)$. □

**Teorema 2.2.41.** *Sia $\mathfrak{p} \neq 0$ ideale primo di $O_K$. Allora $\mathfrak{p}$ è massimale.*

*Dimostrazione.* Dal Teorema 2.2.40, esiste $p \in \mathfrak{p}$. Allora $\mathfrak{p}^c = \mathfrak{p} \cap \mathbb{Z} = (p)$, $p$ intero primo. Inoltre, abbiamo $\mathbb{Z} \subset O_K$; $O_K$ integrale su $\mathbb{Z}$. Allora, poiché $\mathbb{Z}/(p) \cong \mathbb{Z}_p$ è un campo, $(p) \subset \mathbb{Z}$ è massimale. Concludiamo dal Corollario 2.1.14. □

# Capitolo 3

# Domini di Dedekind

## 3.1 Domini a valutazione discreta

**Definizione 3.1.1.** Una *valutazione* su un campo $K$ è un omomorfismo di gruppi $(K^*, \cdot) \to (\mathbb{R}, +)$ tale che per ogni $x, y \in K$ si ha

$$v(x+y) \geq \min(v(x), (v(y)).$$

Possiamo estendere $v$ a una funzione $K \to \mathbb{R} \cup \{\infty\}$ definendo $v(0) := \infty$. L'immagine di $v$ in $\mathbb{R}$ prende il nome di *gruppo dei valori*. L'insieme

$$A = \{x \in K, v(x) \geq 0\}$$

è l'*anello di valutazione di* $K$ rispetto a $v$. Il suo *gruppo delle unità* è dato da

$$A^* = \{x \in K, v(x) = 0\}.$$

**Esempio 3.1.2.** Sia $K = \mathbb{Q}$ e $v : K^* \to \mathbb{R}$, con $v(x) = r$ se $x = 3^r \frac{m}{n}$ e $3 \not| m, n$. Informalmente, data una frazione $x$ ridotta ai minimi termini, $v(x)$ indica la più grande potenza di 3 che possiamo raccogliere "fattorizzando" numeratore e denominatore di $x$; essa è positiva, negativa (o nulla) a seconda che il numeratore o il denominatore (o nessuno dei due) siano multipli di 3. Consideriamo $x = 3^m \frac{a}{b}$ e $y = 3^n \frac{c}{d}$, dove supponiamo $v(x) = m > n = v(y)$: abbiamo che

$$v(x+y) = v(3^n(\frac{3^{m-n}ad + bc}{bd}) = n \geq \min(m, n) = \min(v(x), v(y)),$$

dove la disuguaglianza è verificata poiché, essendo 3 primo, $3|bd$ se e solo se $3|b$ oppure $3|d$, il che non si verifica per la scelta iniziale di $x$ e $y$. Allora $v$ è una valutazione. In questo caso abbiamo anche un'uguaglianza poiché, analogamente $3|3^{m-n}ad + bc \Leftrightarrow 3|bc$ (e quindi $v(\frac{3^{m-n}ad+bc}{bd}) = 0$).

**Esempio 3.1.3.** Osserviamo cosa succede se definiamo la stessa valutazione con i multipli di 6, ovvero $v(x) = r$ se $x = 6^r \frac{m}{n}, 6 \nmid m, n$. Essa non è una valutazione poiché

$$v(\frac{1}{4} + \frac{1}{9}) = v(\frac{13}{36}) = -2 < 0 = v(\frac{1}{4}) = v(\frac{1}{9}).$$

Si può notare facilmente che la proprietà che definisce le valutazioni non è rispettata perché 6 non è primo.

**Lemma 3.1.4.** *Sia $A$ un dominio e $Q(A)$ il suo campo delle frazioni. Se $A$ è un anello di valutazione di $Q(A)$ allora per ogni $x \neq 0$, $x \in A$ oppure $x^{-1} \in A$ (o entrambi).*

*Dimostrazione.* Poiché $v$ è un omomorfismo di gruppi $v(1) = 0$. Allora

$$0 = v(1) = v(x \cdot x^{-1}) = v(x) + v(x^{-1}).$$

Se $v(x) < 0 \Rightarrow v(x^{-1}) > 0$. Osserviamo che se $v(x) = 0$, (quindi è un'unità), sia $x$ che $x^{-1}$ appartengono ad $A$. □

**Definizione 3.1.5.** Diciamo che $v$ è una *valutazione discreta* se il gruppo dei valori è isomorfo a $\mathbb{Z}$. In questo caso $A$ si chiama *anello a valutazione discreta* (DVR).

**Esempio 3.1.6.** La funzione definita in 3.1.2 è una valutazione discreta. Il suo gruppo dei valori è $\mathbb{Z}$ e il suo anello di valutazione è l'insieme

$$A = \left\{ x \in \mathbb{Q}, x = 3^r \frac{m}{n},\ r \geq 0 \text{ e } 3 \nmid n \right\}.$$

**Definizione 3.1.7.** Sia $A$ un DVR. Un elemento $\pi \in A$ tale che $v(\pi) = 1$ è chiamato *uniformatore*. Osserviamo che un uniformatore esiste sempre, poiché $v$ è una mappa suriettiva dall'anello di valutazione $A$ a $\mathbb{Z}_{\geq 0}$.

**Teorema 3.1.8.** *Sia $A$ un DVR. Allora $A$ è un PID.*

*Dimostrazione.* Fissato un uniformatore $\pi$, ogni $x \in K^*$ è scritto in maniera univoca come

$$x = u\pi^n,$$

dove $n = v(x)$ e $u = x/\pi^n \in A^*$ sono univocamente determinati.
Affermiamo che per ogni ideale $\mathfrak{a}$ esiste un $n \geq 0$ tale che

$$\mathfrak{a} = (\pi^n),\ \text{dove } n = min_{x \in \mathfrak{a}} v(x).$$

Che $(\pi^n) \subset \mathfrak{a}$ è ovvio, poiché dato $x \in (\pi^n)$ con $x = u\pi^n$ si ha $\pi^n = x \cdot u^{-1} \in \mathfrak{a}$. Viceversa, dati $x, y \in \mathfrak{a}$, possiamo scrivere $x = u_1\pi^{v(x)} = (u_1\pi^{v(x)-n})\pi^n$ e $y = u_2\pi^{v(y)} = (u_2\pi^{v(y)-n})\pi^n$ cosicché $x, y \in (\pi^n)$ e

- $x \pm y \in (\pi^n)$,
- $a \cdot x \in (\pi^n), \forall a \in A$.

□

**Osservazione 3.1.9.** Quindi tutti gli ideali non nulli di $A$ sono del tipo

$$(\pi^n) = \{x \in A, v(x) \geq n\}, n \geq 0.$$

La famiglia degli ideali di $A$ è totalmente ordinata e l'ideale

$$\mathfrak{m} = (\pi) = \{x \in A, v(x) > 0\}$$

è l'unico ideale massimale e l'unico ideale primo non nullo di $A$. Questo significa che i DVR sono anelli locali.
Nell'Esempio 3.1.2 l'ideale massimale è $(3)A$.

**Teorema 3.1.10.** *Sia $A$ un DVR. Allora $A$ è integralmente chiuso.*

*Dimostrazione.* Sia $x \in Q(A)$ integrale su $A$. Allora soddisfa un'equazione del tipo

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, a_i \in A.$$

Se $x \in A$ non c'è nulla da provare. Altrimenti, $x^{-1} \in A$ dal Lemma 3.1.4: quindi, $x = -(a_{n-1} + a_{n-2}x^{-1} + \ldots + a_0 x^{1-n}) \in A$. □

Diamo quindi la seguente caratterizzazione per i DVR

**Teorema 3.1.11.** *Sia $A$ un dominio. Sono equivalenti le seguenti affermazioni:*

- *$A$ è un DVR;*
- *$A$ è un PID con uno e un solo ideale primo non nullo;*
- *$A$ è un anello locale, noetheriano, integralmente chiuso, tale che ogni ideale primo non nullo è massimale.*

*Dimostrazione.* Si veda [1] capitolo 9. □

**Osservazione 3.1.12.** Un campo $K$ non è un DVR perché non ha un ideale primo non nullo.

## 3.2 Domini di Dedekind

**Definizione 3.2.1.** Sia $A$ un dominio. $A$ è detto *dominio di Dedekind* se è

- noetheriano,
- integralmente chiuso,
- tale che ogni ideale primo $\mathfrak{p} \neq 0$ è massimale.

**Esempio 3.2.2.** Un generico campo $K$ è un dominio di Dedekind. Mostriamo che $K$ soddisfa le tre proprietà:

- $K$ è noetheriano come già osservato in 1.4.2.
- $K$ è banalmente integralmente chiuso. Infatti poiché il campo dei quozienti $Q(K) = K$, $x - a = 0$ è una valida equazione integrale a coefficienti in $K$ per ogni $a \in K$.
- Essendo (0) e (1) gli unici ideali di $K$, la condizione è soddisfatta.

Osserviamo che l'unica condizione per cui $K$ è un dominio di Dedekind e non un DVR, è quindi l'esistenza e unicità di un ideale primo non nullo (come osservato in 3.1.12), che qui non è richiesta.

**Teorema 3.2.3.** *Sia $K$ un campo di numeri algebrici. Il suo anello degli interi algebrici $O_K$ è un dominio di Dedekind.*

*Dimostrazione.* Abbiamo dimostrato che $O_K$ soddisfa le tre proprietà in 2.2.14, 2.2.15 e 2.2.41. □

Vale anche il seguente risultato generale

**Teorema 3.2.4.** *Se $A$ è un PID allora è un dominio di Dedekind.*

*Dimostrazione.* Mostriamo che soddisfa le tre proprietà:

- Ogni ideale è generato da un solo elemento, quindi è finitamente generato. Per definizione allora $A$ è noetheriano.
- Un PID è in particolare un UFD, che abbiamo già dimostrato essere integralmente chiuso.
- Consideriamo un ideale primo $\mathfrak{p} = (p) \neq 0$ e $(x) \supseteq (p)$.
  $\Rightarrow p \in (x) \Rightarrow p = xy$ per un certo $y$
  $\Rightarrow xy \in (p) \Rightarrow x \in (p)$ oppure $y \in (p)$

- Se $x \in (p)$ allora $(x) = (p)$.
- Se $y \in (p)$ allora $y = pq$ per un certo $q$. Quindi $p = xy = xqp \Rightarrow xq = 1 \Rightarrow (x) = (1)$.

Allora $\mathfrak{p}$ è massimale.

□

**Osservazione 3.2.5.** Non vale il viceversa. Consideriamo ad esempio $A = \mathbb{Z}[\sqrt{-5}]$. Dato che $-5 \equiv 3 \bmod 4$, da 2.2.20 $A = O_{\mathbb{Q}[\sqrt{-5}]}$, e quindi è un dominio di Dedekind. Ma poiché $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}) \in A$, sono due distinte fattorizzazioni in irriducibili, $A$ non è un UFD, e quindi neanche un PID.

Vale però il seguente risultato

**Osservazione 3.2.6.** Sia $A$ un dominio di Dedekind e un UFD. Allora $A$ è un PID.

*Dimostrazione.* Sia $\mathfrak{p}$ un ideale primo non nullo di $A$ e sia $a$ un suo elemento non nullo. Per definizione di ideale primo, esiste allora un fattore primo $p \in \mathfrak{p}$ di $a$. Allora $(p)$ è un ideale primo non nullo, e $(p) \subset \mathfrak{p}$. Poiché $(p)$ è un ideale massimale ($A$ è di Dedekind) e $\mathfrak{p}$ è un ideale proprio, segue che $(p) = \mathfrak{p}$. Quindi ogni ideale primo di $A$ è prncipale.
Sia ora $\mathfrak{a}$ un ideale proprio di $A$. Se $\mathfrak{a} = (0)$ è principale. Supponiamo quindi che $\mathfrak{a}$ sia non nullo e sia $0 \neq a \in \mathfrak{a}$. Allora sia $\Sigma$ l'insieme degli ideali principali propri di $A$ contenenti $\mathfrak{a}$. $\Sigma$ non è vuoto perché esiste un ideale massimale $\mathfrak{m}$ contenente $\mathfrak{a}$. Quindi $\mathfrak{m}$ è primo, quindi principale per quanto dimostrato in precedenza. Inoltre deve esistere anche un elemento minimale di $\Sigma$ poiché altrimenti esisterebbe una catena discendente non stazionaria di ideali principali, e questo è assurdo poiché $A$ è un UFD. Sia $\mathfrak{b} = (b)$ un elemento minimale di $\Sigma$. Sia $\mathfrak{c} = \{x \in A, bx \in \mathfrak{a}\}$; esso è un ideale contenente $\mathfrak{a}$ tale che $b\mathfrak{c} = \mathfrak{a}$. Se $\mathfrak{c}$ fosse un ideale proprio di $A$ si avrebbe $\mathfrak{c} \subset (d)$ per qualche $d \in A$. Allora avremmo che $\mathfrak{a} \subset (bc) \subset (b) = \mathfrak{b}$, che contraddice l'ipotesi di minimalità di $\mathfrak{b}$. Allora $\mathfrak{c} = A$ e $bA = \mathfrak{a}$, quindi $\mathfrak{a} = (b)$ è principale. Allora $A$ è un PID. □

Diamo infine un'importante caratterizzazione dei domini di Dedekind tramite i DVR.

**Teorema 3.2.7.** *Sia $A$ un dominio noetheriano. $A$ è un dominio di Dedekind se e solo se per ogni ideale primo $\mathfrak{p} \neq 0$ la sua localizzazione $A_{\mathfrak{p}}$ è un DVR.*

*Dimostrazione.* Innanzitutto consideriamo il caso in cui $A$ sia un campo: come mostrato nell'Esempio 3.2.2, $A$ è un dominio di Dedekind e, poiché $A$ non ha ideali primi non nulli, l'equivalenza vale banalmente. Consideriamo allora il caso in cui $A$ non sia un campo ma sia un dominio di Dedekind. Da 1.4.6 e 2.1.12, sappiamo che la localizzazione di $A$ conserva le proprietà di essere noetheriani e integralmente chiusi. Se consideriamo infine gli ideali primi di $A_{\mathfrak{p}}$, essi sono in corrispondenza biunivoca con gli ideali primi contenuti in $\mathfrak{p}$ per 1.3.10. Ma poiché $A$ è di Dedekind, ogni ideale primo non nullo è massimale, quindi non possono esistere ideali primi contenuti strettamente in $\mathfrak{p}$. Quindi $\mathfrak{p}A_{\mathfrak{p}}$ è l'unico ideale primo e massimale di $A_{\mathfrak{p}}$, da cui la tesi. Viceversa,

- $A$ è noetheriano per ipotesi,
- Sia $a \in Q(A)$ integrale su $A$: esso è integrale anche su ogni $A_{\mathfrak{p}}$, poiché $A \subset A_{\mathfrak{p}}$ tramite l'immersione $a \mapsto \frac{a}{1}$. Per ipotesi tutti gli $A_{\mathfrak{p}}$ sono integralmente chiusi, quindi $a \in \bigcap_{\mathfrak{p}} A_{\mathfrak{p}} = A$, da cui concludiamo che $A$ è integralmente chiuso.
- Se consideriamo una catena di ideali primi in $A$, $(0) \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$, essa viene estesa a una catena della stessa lunghezza in $A_{\mathfrak{p}_n}$. Poiché per ipotesi $A_{\mathfrak{p}_n}$ è un DVR, in particolare ogni ideale primo non nullo è massimale, quindi $n = 1$ e $\mathfrak{p}_1$ è massimale in $A$.

□

**Esempio 3.2.8.** Consideriamo l'anello $\mathbb{Z}$ e il suo ideale primo $\mathfrak{p} = (3)$. $\mathbb{Z}$ è un dominio di Dedekind per 3.2.4, quindi $\mathbb{Z}_{(3)}$ è un DVR. Come osservato nell'Esempio 1.3.7,

$$\mathbb{Z}_{(3)} = \left\{ \frac{m}{n} \in \mathbb{Q}, 3 \not| n \right\},$$
$$\mathfrak{m} = (3)\mathbb{Z}_{(3)}.$$

Effettivamente questo è il DVR definito dalla valutazione discreta dell'Esempio 3.1.2.

**Esempio 3.2.9.** Analogamente, consideriamo ora $A = \mathbb{Z}[\sqrt{3}]$. Il suo ideale (5) è massimale poiché

$$\mathbb{Z}[\sqrt{3}]/(5) \cong \mathbb{Z}[x]/(5, x^2 - 3) \cong \mathbb{Z}_5[x]/x^2 - 3,$$

che è un'estensione di grado 2 di $\mathbb{Z}_5$ e quindi isomorfa al campo $\mathbb{F}_{5^2}$, poiché $x^2 - 3$ è un polinomio irriducibile di $\mathbb{Z}_5[x]$. Come osservato in 3.2.3 $A$ è un dominio di Dedekind, quindi (5) è un ideale primo e $A_{(5)}$ è un DVR. Possiamo definire una valutazione discreta identica alla precedente.

**Esempio 3.2.10.** Consideriamo $A = \mathbb{Z}[\sqrt{5}]$: sappiamo che esso non è integralmente chiuso per il Teorema 2.2.20, quindi in particolare non è un dominio di Dedekind. Allora, per il Teorema 3.2.7, deve esistere un ideale primo non nullo $\mathfrak{p}$ tale che la localizzazione $A_\mathfrak{p}$ non sia un $DVR$. Consideriamo l'ideale $\mathfrak{p} = (2, 1+\sqrt{5})$: innanzitutto osserviamo che esso non è principale poiché $MCD(2, 1+\sqrt{5}) = 1 \notin \mathfrak{p}$. Esso è inoltre primo poiché

$$\mathbb{Z}[\sqrt{5}]/\mathfrak{p} \cong \mathbb{Z}_2,$$

considerando ad esempio l'omomorfismo $\phi : (a + b\sqrt{5}) \mapsto [a + b]_2$. Localizziamo dunque rispetto a $\mathfrak{p}$:

$$A_\mathfrak{p} = \left\{ \frac{a+b\sqrt{5}}{c+d\sqrt{5}} \text{ tale che } c + d\sqrt{5} \notin \mathfrak{p} \right\}.$$

Osserviamo infine che $\phi = \frac{1+\sqrt{5}}{2} \notin A_\mathfrak{p}$ e $\phi^{-1} = \frac{2}{1+\sqrt{5}} = \frac{-1+\sqrt{5}}{2} \notin A_\mathfrak{p}$. Per il Lemma 3.1.4, $A_\mathfrak{p}$ non è un $DVR$.

# Capitolo 4

# Il teorema di fattorizzazione unica

## 4.1 Ideali frazionari

**Definizione 4.1.1.** Sia $A$ un dominio e $Q(A)$ il suo campo di frazioni. Un $A$-sottomodulo $\mathcal{M}$ di $Q(A)$ è un *ideale frazionario* di $A$ se esiste $x \neq 0$ in $A$ tale che $x\mathcal{M} \subset A$. Dato un ideale frazionario $\mathcal{M}$ denotiamo anche

$$(A : \mathcal{M}) = \{x \in Q(A) \text{ tali che } x\mathcal{M} \subset A\}.$$

**Osservazione 4.1.2.** In particolare, tutti gli ideali in senso stretto che abbiamo considerato finora (e che d'ora in poi chiameremo *ideali interi*) sono ideali frazionari: basta considerare $x = 1$.

**Osservazione 4.1.3.** Ogni ideale frazionario è della forma $\mathcal{M} = x^{-1}\mathfrak{a}$, dove $x \in (A : \mathcal{M})$ e $\mathfrak{a}$ è un ideale intero.

**Teorema 4.1.4.** *Ogni $A$-sottomodulo finitamente generato di $Q(A)$ è un ideale frazionario. Viceversa, se $A$ è noetheriano, ogni suo ideale frazionario è un $A$-sottomodulo finitamente generato.*

*Dimostrazione.* Sia $\mathcal{M}$ generato da $x_1, \ldots, x_n \in Q(A)$. Scriviamo $x_i = \frac{y_i}{z}$, con $y_i, z \in A$. Allora, $z\mathcal{M} \subset A$.
Viceversa, sia $\mathcal{M}$ un ideale frazionario. Per l'Osservazione 4.1.3, esiste un ideale intero $\mathfrak{a}$ tale che $\mathcal{M} = x^{-1}\mathfrak{a}$. Poiché $A$ è noetheriano, $\mathfrak{a}$ è finitamente generato da $(v_1, \ldots, v_n)$. Allora $\mathcal{M}$ è finitamente generato da $x^{-1}v_1, \ldots, x^{-1}v_n$. □

**Corollario 4.1.5.** *Ogni ideale frazionario di $O_K$ è finitamente generato come $O_K$-modulo.*

**Osservazione 4.1.6.** Come dimostrato nel Teorema 2.2.5, $Q(O_K) = K$; allora per ideali frazionari di $O_K$ l'Osservazione 4.1.3 può essere riformulata nel seguente modo: ogni ideale frazionario di $O_K$ può essere scritto come $M = x^{-1}\mathfrak{a}$, dove $x$ è un intero di $\mathbb{Z}$ (invece che un elemento di $O_K$) e $\mathfrak{a}$ è un ideale intero.

**Teorema 4.1.7.** *La famiglia degli ideali frazionari di $A$ è chiusa per somma e prodotto.*

*Dimostrazione.* Siano $\mathcal{M}$ e $\mathcal{N}$ due ideali frazionari e siano $x, y \neq 0$ in $A$ tali che $x\mathcal{M}, y\mathcal{N} \subset A$. Allora,

$$xy(\mathcal{M}\mathcal{N}) = (x\mathcal{M})(y\mathcal{N}) \subset A,$$

$$xy(\mathcal{M} + \mathcal{N}) = y(x\mathcal{M}) + x(y\mathcal{N}) \subset yA + xA \subset A.$$

□

**Definizione 4.1.8.** Dati due ideali $\mathfrak{a}$ e $\mathfrak{b}$ di $A$, definiamo anche l'*ideale quoziente generalizzato* come

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in Q(A), x\mathfrak{b} \subset \mathfrak{a}\}.$$

Esso è inoltre un ideale frazionario.

**Definizione 4.1.9.** Un $A$-sottomodulo $\mathcal{M}$ di $Q(A)$ è un *ideale invertibile* se esiste un sottomodulo $\mathcal{N}$ di $Q(A)$ tale che $\mathcal{M}\mathcal{N} = A$.

**Lemma 4.1.10.** *Tale sottomodulo $\mathcal{N}$ è unico e uguale a $(A : \mathcal{M})$.*

*Dimostrazione.* Effettivamente abbiamo che

$$\mathcal{N} \subset (A : \mathcal{M}) = (A : \mathcal{M})\mathcal{M}\mathcal{N} \subset A\mathcal{N} = \mathcal{N}.$$

□

**Corollario 4.1.11.** *Un ideale invertibile $\mathcal{M}$ è un ideale frazionario.*

*Dimostrazione.* Da 4.1.10 otteniamo che $\mathcal{M} \cdot (A : \mathcal{M}) = A$. Quindi esistono $x_1, \ldots, x_n \in \mathcal{M}$ e $y_1, \ldots, y_n \in (A : \mathcal{M})$ tali che $\sum_i x_i y_i = 1$. Allora, ogni $x \in \mathcal{M}$ può essere scritto come $x = \sum_i (y_i x) x_i$, con $y_i x \in A$, per cui $\mathcal{M}$ è generato da $x_1, \ldots, x_n$. Allora $\mathcal{M}$ è un sottomodulo finitamente generato di $Q(A)$ e quindi un ideale frazionario per definizione. □

**Esempio 4.1.12.** Ogni ideale frazionario principale $(u)$ è invertibile, con inverso $(u^{-1})$.

Le operazioni di somma, prodotto e quoziente generalizzato rispettano la localizzazione.

**Lemma 4.1.13.** *Siano $\mathcal{M}$ e $\mathcal{N}$ due ideali frazionari di un dominio noetheriano $A$ e sia $\mathfrak{p}$ un ideale primo di $A$. Allora $\mathcal{M}_\mathfrak{p}$ e $\mathcal{N}_\mathfrak{p}$ sono ideali frazionari di $A_\mathfrak{p}$ e valgono*

$$(\mathcal{M}+\mathcal{N})_\mathfrak{p} = \mathcal{M}_\mathfrak{p} + \mathcal{N}_\mathfrak{p},$$
$$(\mathcal{M}\cdot\mathcal{N})_\mathfrak{p} = \mathcal{M}_\mathfrak{p} \cdot \mathcal{N}_\mathfrak{p},$$
$$(\mathcal{M}:\mathcal{N})_\mathfrak{p} = (\mathcal{M}_\mathfrak{p} : \mathcal{N}_\mathfrak{p}).$$

*Dimostrazione.* Osserviamo innanzitutto che $\mathcal{M}_\mathfrak{p} = \mathcal{M}A_\mathfrak{p}$ è un $A_\mathfrak{p}$-modulo finitamente generato (dai generatori di $\mathcal{M}$ come $A$-modulo), e quindi è un ideale frazionario di $A_\mathfrak{p}$. Allora per la somma abbiamo che

$$(\mathcal{M}+\mathcal{N})_\mathfrak{p} = (\mathcal{M}+\mathcal{N})A_\mathfrak{p} = \mathcal{M}A_\mathfrak{p} + \mathcal{N}A_\mathfrak{p};$$

analogamente, per il prodotto,

$$(\mathcal{M}\cdot\mathcal{N})_\mathfrak{p} = (\mathcal{M}\cdot\mathcal{N})A_\mathfrak{p} = \mathcal{M}_\mathfrak{p}\cdot\mathcal{N}_\mathfrak{p}.$$

Infine consideriamo il quoziente generalizzato

$$(\mathcal{M}:\mathcal{N})_\mathfrak{p} = \{x \in Q(A), x\mathcal{N} \subset \mathcal{M}\}_\mathfrak{p} = \left\{x \in Q(A), x\mathcal{N}_\mathfrak{p} \subset \mathcal{M}_\mathfrak{p}\right\} = (\mathcal{M}_\mathfrak{p} : \mathcal{N}_\mathfrak{p}).$$

□

Otteniamo quindi un altra caratterizzazione dei DVR e la rispettiva controparte "globale" sui domini di Dedekind.

**Teorema 4.1.14.** *Sia $A$ un dominio locale. Allora $A$ è un DVR se e solo se ogni suo ideale frazionario non nullo è invertibile.*

*Dimostrazione.* Sia $A$ un DVR e $\mathfrak{m} = (x)$ il suo ideale massimale. Consideriamo un suo ideale frazionario $\mathcal{M} \neq 0$. Allora esiste $y \in A$ tale che $y\mathcal{M} \subset A$, per cui $y\mathcal{M}$ è un ideale intero e quindi della forma $y\mathcal{M} = (x^r)$. Allora $\mathcal{M} = (x^{r-v(y)})$.
Viceversa, consideriamo un ideale intero non nullo $\mathfrak{a} \subset A$ che per ipotesi è invertibile e frazionario. Allora esistono (in numero finito) $x_1, \ldots, x_n \in \mathfrak{a}$ e $y_1, \ldots, y_n \in (A : \mathfrak{a})$ tali che $1 = \sum_{i=1}^n x_i y_i$. Allora ogni $x \in \mathfrak{a}$ può essere scritto come

$$x = \sum_{i=1}^n (x_i y_i)x = \sum_{i=1}^n x_i(y_i x),$$

con $y_i x \in \mathfrak{a} \cdot (A : \mathfrak{a}) = A$. Allora $\mathfrak{a}$ è finitamente generato da $x_1, \ldots, x_n$ e quindi $A$ è noetheriano. Allora è sufficiente provare che ogni ideale intero è una potenza di $\mathfrak{m}$. Supponiamo per assurdo che ciò sia falso. Definiamo la famiglia $\Sigma$ degli ideali non nulli che non sono una potenza di $\mathfrak{m}$ e sia $\mathfrak{a}$ un suo elemento massimale. Allora, $\mathfrak{a} \neq \mathfrak{m}$, quindi $\mathfrak{a} \subset \mathfrak{m}$, da cui $\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{m} = A$ è un ideale intero proprio tale che $\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{a}$. Se $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a} \Leftrightarrow \mathfrak{a} = \mathfrak{m}\mathfrak{a}$, allora $\mathfrak{a} = 0$. Quindi deve essere $\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{a}$ e, per massimalità di $\mathfrak{a}$, $\mathfrak{m}^{-1}\mathfrak{a}$, e quindi $\mathfrak{a}$ sono potenze di $\mathfrak{m}$, da cui l'assurdo. □

**Teorema 4.1.15.** *Sia $A$ un dominio. Allora $A$ è un dominio di Dedekind se e solo se ogni suo ideale frazionario non nullo è invertibile.*

*Dimostrazione.* Sia $\mathcal{M}$ un ideale frazionario non nullo. Poiché $A$ è noetheriano $\mathcal{M}$ è finitamente generato. Per ogni ideale primo non nullo $\mathfrak{p}$ di $A$, $\mathcal{M}_\mathfrak{p}$ è un ideale frazionario non nullo di $A_\mathfrak{p}$, quindi invertibile per il teorema precedente. Allora $\mathcal{M}_\mathfrak{p} \cdot (A_\mathfrak{p} : \mathcal{M}_\mathfrak{p}) = A_\mathfrak{p}$. Se definiamo $\mathfrak{a} = \mathcal{M}(A : \mathcal{M})$, otteniamo da 4.1.13 che $\mathfrak{a}_\mathfrak{p} = A_\mathfrak{p}$. Dal Teorema 1.3.8 questo è possibile solo se $\mathfrak{a} \cap (A - \mathfrak{p}) \neq \emptyset$, ma poiché A è un Dominio di Dedekind, $\mathfrak{p}$ è massimale, quindi $\mathfrak{a} = A$.
Viceversa, se ogni ideale intero non nullo è invertibile, allora è finitamente generato e quindi $A$ è noetheriano. Sia $\mathfrak{b}$ un ideale intero non nullo di $A_\mathfrak{p}$ e sia $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{a} \cap A$. Per ipotesi $\mathfrak{a}$ è invertibile e vale $\mathfrak{a} \cdot (A : \mathfrak{a}) = A$; quindi $\mathfrak{b} = \mathfrak{a}_\mathfrak{p}$ è invertibile poiché $A_\mathfrak{p} = (\mathfrak{a} \cdot (A : \mathfrak{a}))_\mathfrak{p} = \mathfrak{a}_\mathfrak{p} \cdot (A_\mathfrak{p} : \mathfrak{a}_\mathfrak{p})$. □

Abbiamo quindi dimostrato che la famiglia degli ideali frazionari non nulli di un dominio di Dedekind forma un gruppo moltiplicativo.

**Definizione 4.1.16.** Sia $A$ dominio di Dedekind. Il gruppo $\mathcal{I}$ dei suoi ideali frazionari non nulli è il *gruppo degli ideali* di $A$.
Consideriamo l'omomorfismo $\psi : K^* \to \mathcal{I}$ definito da $\psi : u \mapsto (u)$, dove $(u)$ è un ideale frazionario. Definiamo $\mathcal{P} = Im(\psi)$ *gruppo degli ideali frazionari principali* di $A$.
Infine, il gruppo quoziente $\mathcal{H} = \mathcal{I}/\mathcal{P}$ è chiamato *gruppo delle classi di ideali* di $A$.

## 4.2 Fattorizzazione unica in $O_K$

Come è stato osservato nell'Esempio 3.2.5, i domini di Dedekind non sono generalmente a fattorizzazione unica. Effettivamente, ciò significa che in generale passare dagli interi agli interi algebrici di $K$ ci fa perdere una proprietà fondamentale dell'aritmetica di $\mathbb{Z}$. L'obiettivo di questa sezione sarà quindi

quello di ritrovare risultati analoghi a quelli noti per $\mathbb{Z}$, operando però sugli ideali.

**Teorema 4.2.1.** *Ogni ideale proprio di $O_K$ contiene un prodotto di ideali primi non nulli.*

*Dimostrazione.* Sia $\Sigma$ l'insieme degli ideali che non contiene un prodotto di ideali primi. Se $\Sigma$ non è vuoto, poiché $O_K$ è noetheriano ha un elemento massimale che chiamiamo $\mathfrak{a}$. Allora $\mathfrak{a}$ non è primo perché appartiene a $\Sigma$, quindi esistono $x, y \in O_K$ tali che $xy \in \mathfrak{a}$ ma $x, y \notin \mathfrak{a}$. Allora $\mathfrak{a} \subsetneq (\mathfrak{a}, x)$, $\mathfrak{a} \subsetneq (\mathfrak{a}, y)$, ma $(\mathfrak{a}, x), (\mathfrak{a}, y) \notin S$ perché $\mathfrak{a}$ è massimale. Quindi $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (\mathfrak{a}, x)$ e $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset (\mathfrak{a}, y)$ con $\mathfrak{p}_i$ e $\mathfrak{q}_j$ primi. Infine, poiché per ipotesi $xy \in \mathfrak{a}$,

$$\mathfrak{a} = (\mathfrak{a}, xy) = (\mathfrak{a}, x)(\mathfrak{a}, y) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Quindi $\mathfrak{a}$ contiene un prodotto di ideali primi e non appartiene a $\Sigma$, da cui l'assurdo. □

**Lemma 4.2.2.** *Sia $\mathfrak{p}$ un ideale primo di $O_K$. Esiste $z \in K \setminus O_K$ tale che $z\mathfrak{p} \subset O_K$.*

*Dimostrazione.* Sia $x \in \mathfrak{p}$. Da 4.2.1, $(x)$ contiene un prodotto di ideali primi, diciamo $\mathfrak{p}_1 \cdots \mathfrak{p}_r$, con $r$ il più piccolo intero che soddisfi tale proprietà. Allora, $\mathfrak{p} \supset (x) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$, quindi esiste $i$ tale che $\mathfrak{p} \supset \mathfrak{p}_i$ e, senza perdere di generalità, possiamo supporre che $i = 1$. Poiché $\mathfrak{p}_1$ è un ideale primo di un Dominio di Dedekind, è anche massimale, quindi $\mathfrak{p} = \mathfrak{p}_1$.
Consideriamo quindi $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (x)$ (poiché avevamo scelto $r$ minimo), e scegliamo $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r, b \notin (x)$. Osserviamo che questo implica che $z = bx^{-1} \notin O_K$. Infine,

$$\begin{aligned} z\mathfrak{p} = bx^{-1}\mathfrak{p} &\subset (\mathfrak{p}_2 \cdots \mathfrak{p}_r)(x^{-1}\mathfrak{p}_1) \\ &= x^{-1}(\mathfrak{p}_1 \cdots \mathfrak{p}_r) \\ &\subset x^{-1}xO_K = O_K. \end{aligned}$$

□

**Teorema 4.2.3.** *Sia $\mathfrak{p}$ un ideale primo di $O_K$. Allora $\mathfrak{p}$ è un ideale invertibile con inverso $\mathfrak{p}^{-1} = (O_K : \mathfrak{p}) = \{x \in K, x\mathfrak{p} \subset O_K\}$.*

*Dimostrazione.* Mostriamo che $\mathfrak{p}\mathfrak{p}^{-1} = O_K$. Sappiamo che $1 \in \mathfrak{p}^{-1}$, quindi $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset O_K$. Poiché $O_K$ è un dominio di Dedekind, $\mathfrak{p}$ è massimale, quindi o concludiamo che $\mathfrak{p}\mathfrak{p}^{-1} = O_K$, oppure $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. In questo caso allora per ogni $x \in \mathfrak{p}^{-1}$, $x\mathfrak{p} \subset \mathfrak{p}$, e poiché $\mathfrak{p}$ è uno $\mathbb{Z}$-modulo finitamente generato, deduciamo usando 2.2.7 che $x$ è un intero algebrico, quindi $\mathfrak{p}^{-1} \subset O_K$ e, poiché $1 \in \mathfrak{p}^{-1}$, $\mathfrak{p}^{-1} = O_K$. Da 4.2.2, questo è assurdo. □

Enunciamo infine il teorema di fattorizzazione unica.

**Teorema 4.2.4.** *Ogni ideale di $O_K$ può essere scritto in maniera unica come prodotto di ideali primi.*

*Dimostrazione.* Mostriamo innanzitutto che una tale fattorizzazione esiste. Sia $\Sigma$ l'insieme degli ideali che non possono essere scritti come prodotto di ideali primi. Supponiamo per assurdo che $\Sigma$ non sia vuoto, allora, poiché $O_K$ è noetheriano, esiste un elemento massimale $\mathfrak{a}$, che banalmente non è primo. Allora esiste un ideale primo (e massimale) $\mathfrak{p}$ tale che $\mathfrak{a} \subset \mathfrak{p}$. Consideriamo $\mathfrak{p}^{-1}\mathfrak{a} \subsetneq \mathfrak{p}^{-1}\mathfrak{p} = O_K$. Quindi, $\mathfrak{p}^{-1}\mathfrak{a}$ è un ideale di $O_K$ che contiene $\mathfrak{a}$ e quindi non appartiene a $\Sigma$ per massimalità di $\mathfrak{a}$. Allora

$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

$$\mathfrak{a} = \mathfrak{p}\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

da cui l'assurdo.
Supponiamo ora di avere due fattorizzazioni in ideali primi di $\mathfrak{a}$,

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Allora $\mathfrak{q}_1 \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Quindi esiste $\mathfrak{p}_i \subset \mathfrak{q}_1$, e supponiamo senza perdere di generalità che $i = 1$. Ma $\mathfrak{p}_1$ è massimale quindi $\mathfrak{q}_1 = \mathfrak{p}_1$. Moltiplicando entrambi i membri per $(\mathfrak{p}_1)^{-1}$ e usando $\mathfrak{p}^{-1}\mathfrak{p} = O_K$ da 4.2.3, otteniamo che

$$\mathfrak{q}_2 \cdots \mathfrak{q}_s = \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Procedendo ricorsivamente, si ottiene anche che $r = s$ e che gli ideali primi sono unici a meno di permutazione. □

Il seguente risultato fornisce uno strumento molto potente per fattorizzare gli ideali.

**Teorema 4.2.5.** *Supponiamo esista $\theta \in K$ tale che $O_K = \mathbb{Z}[\theta]$ e sia $f$ il polinomio minimo di $\theta$. Sia $p$ un primo di $\mathbb{Z}$. Consideriamo la fattorizzazione di $f$ in polinomi irriducibili* mod $p$*:*

$$f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r} \mod p.$$

*Allora,*

$$pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

*dove $i$ $\mathfrak{p}_i = (p, f_i(\theta))$ sono ideali primi.*

*Dimostrazione.* Innanzitutto ricordiamo che $f(x) \in \mathbb{Z}[x]$ per 2.2.6. Inoltre si osserva facilmente che $(p, f_1(\theta))^{e_1} \cdots (p, f_r(\theta))^{e_r} \subset (p)$.
Per ognuno dei polinomi $f_i$, essendo irriducibili, $\mathbb{F}_p[x]/f_i(x)$ è un campo; inoltre $\mathbb{Z}[x]/(p) \cong \mathbb{F}_p[x]$, quindi $\mathbb{Z}[x]/(p, f_i(x)) \cong \mathbb{F}_p[x]/(f_i(x))$ è un campo. Consideriamo ora la funzione

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}[\theta]/(p, f_i(\theta)),$$

e studiamone il nucleo $Ker(\phi) = \{n(x) : n(\theta) \in (p, f_i(\theta))\}$. Sicuramente $(p, f_i(x)) \subset Ker(\phi)$.
Viceversa, consideriamo $n \in Ker(\phi)$ e dividiamolo per $f_i$ in $\mathbb{Z}_p[x]$ ottenendo

$$n(x) = q(x)f_i(x) + r_i(x), \ \deg(r_i) < \deg(f_i).$$

Se $r_i = 0$ abbiamo concluso. Altrimenti, poiché per ipotesi $n(\theta) \in (p, f_i(\theta))$, anche $r_i(\theta) \in (p, f_i(\theta))$ per cui possiamo scrivere

$$r_i(\theta) = pa(\theta) + f_i(\theta)b(\theta),$$

sfruttando il fatto che $O_K = \mathbb{Z}[\theta]$.
Il polinomio definito come $h(x) := r_i(x) - pa(x) - f_i(x)b(x)$ è tale per cui $h(\theta) = 0$, quindi esiste un polinomio $g$ tale che $h(x) = f(x)g(x)$. Allora

$$r_i(x) = p\tilde{a}(x) + f_i(x)\tilde{b}(x) \in (p, f_i(x)).$$

Quindi $Ker(\phi) = (p, f_i(x))$, da cui

$$\mathbb{Z}[\theta]/(p, f_i(\theta)) \cong \mathbb{Z}[x]/(p, f_i(x)) \cong \mathbb{F}_p[x]/(f_i(x))$$

e quindi è un campo. Allora $(p, f_i(\theta))$ è un ideale massimale e quindi primo. Supponiamo ora vero il seguente lemma:

**Lemma 4.2.6.** *Sia $f$ il polinomio minimo di $\theta$, $p$ un primo di $\mathbb{Z}$. Siano $f = \prod_i f_i \bmod p$, con gli $f_i$ irriducibili in $\mathbb{F}_p[x]$ e $d_i := deg(f_i)$. Consideriamo la fattorizzazione (unica) di $pO_K = \mathfrak{q}_1^{e'_1} \cdots \mathfrak{q}_r^{e'_r}$. Allora*

$$[K : \mathbb{Q}] = \deg(f) = \sum_i e'_i d_i.$$

Quindi supponiamo che i fattori primi di $pO_K$ siano tutti e soli i $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ e quindi possiamo scrivere $pO_K = \mathfrak{p}_1^{e'_1} \cdots \mathfrak{p}_r^{e'_r}$; se riusciamo a dimostrare che $e_i = e'_i$ possiamo concludere per unicità della fattorizzazione.

Poiché $f(\theta) = 0$ e per costruzione $f(x) - f_1(x)^{e_1} \cdots f_r(x)^{e_r} \in p\mathbb{Z}[x]$, osserviamo che $f_1(\theta)^{e_1} \cdots f_r(\theta)^{e_r} \in p\mathbb{Z}[\theta] = pO_K$.
Quindi per definizione, $\mathfrak{p}_i^{e_i} \subset pO_K + (f_i(\theta)^{e_i})$ e il loro prodotto

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subset pO_K = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e'r},$$

da cui otteniamo che $e_i \geq e_i'$ per ogni $i$. Ma effettivamente, definendo $d_i = deg(f_i)$, $\sum_i e_i d_i = deg(f)$, quindi per il lemma $\sum_i e_i d_i = \sum_i e_i' d_i$, quindi $e_i = e_i'$, da cui la tesi. □

Osserviamo come quindi ora possiamo calcolare facilmente la fattorizzazione in ideali primi, almeno nel caso delle estensioni quadratiche.

**Esempio 4.2.7.** Consideriamo $O_K = \mathbb{Z}[\sqrt{3}]$. Il polinomio minimo di $\theta = \sqrt{3}$ è ovviamente $f(x) = x^2 - 3$. Fattorizziamo gli ideali (2), (5) e (11).

- $f(x) \equiv (x+1)^2 \bmod 2$, quindi $(2) = (2, 1+\sqrt{3})^2 = (1+\sqrt{3})^2$, poiché $2 = (1+\sqrt{3})(-1+\sqrt{3})$.
- $f(x) \equiv x^2 - 3 \bmod 5$. Essendo irriducibile, ne deduciamo che (5) è un ideale primo. Questa è una conferma di quanto avevamo ottenuto nell'Esempio 3.2.9.
- $f(x) = (x-5)(x+5) \bmod 11$, quindi $(11) = (11, -5+\sqrt{3})(11, 5+\sqrt{3})$. Ma $(11, -5+\sqrt{3}) = (1+2\sqrt{3})$, poiché

  $$MCD(11, -5+\sqrt{3}) = 1 + 2\sqrt{3} = 11 + 2 \cdot (-5 + 2\sqrt{3});$$

  analogamente $(11, 5+\sqrt{3}) = (1-2\sqrt{3})$. Allora effettivamente $(11) = (1+2\sqrt{3})(1-2\sqrt{3})$.

**Osservazione 4.2.8.** Sappiamo che $\mathbb{Z}[\sqrt{3}]$ è un PID, e in particolare un UFD. Dato un ideale (principale) $\mathfrak{a} = (u)$ e la fattorizzazione (unica) del suo generatore $u = p_1 \cdots p_r$, la fattorizzazione in ideali primi di $\mathfrak{a}$ è data da

$$(u) = (p_1) \cdots (p_r).$$

**Esempio 4.2.9.** Osserviamo infine come la fattorizzazione in ideali primi sia unica anche in Domini di Dedekind che non sono UFD. Riprendiamo il caso $\mathbb{Z}[\sqrt{-5}]$, dove avevamo notato che

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

Da questa fattorizzazione otteniamo che

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

Riduciamo il polinomio minimo $f$ di $\theta = \sqrt{-5}$.

- $x^2 + 5 \equiv x^2 + 1 \equiv (x+1)^2 \bmod 2$;
- $x^2 + 5 \equiv x^2 - 1 \equiv (x+1)(x-1) \bmod 3$.

Quindi

$$(2) = (2, 1+\sqrt{-5})^2 := \mathfrak{p}_1^2,$$
$$(3) = (3, 1+\sqrt{-5})(3, -1+\sqrt{-5}) := \mathfrak{q}_1\mathfrak{q}_2.$$

Verifichiamo che per (2) effettivamente vale l'uguaglianza. Ricordando che

$$(a,b)(c,d) = (ac, bc, ad, bd),$$

otteniamo che

$$\mathfrak{p}_1^2 = (2, 1+\sqrt{-5})^2 = (4, -4+2\sqrt{-5}, 2+2\sqrt{-5}),$$

quindi ovviamente $\mathfrak{p}_1^2 \subset (2)$; viceversa

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

quindi $(2) \subset \mathfrak{p}_1^2$. Infine $\mathfrak{p}_1$ è primo poiché $\mathfrak{p}_1 \cap \mathbb{Z} = (2)$ (mentre si verifica facilmente che $1 \notin \mathfrak{p}_1$). Effettivamente,dato l'omomorfismo

$$\phi : (a + b\sqrt{-5}) \mapsto [a+b]_2,$$

si verifica che

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_1 \cong \mathbb{Z}_2,$$

che è un campo. Analogamente per (3) otteniamo:

$$\mathfrak{q}_1\mathfrak{q}_2 = (9, 3+3\sqrt{-5}, -3+3\sqrt{-5}, -6),$$

quindi $\mathfrak{q}_1\mathfrak{q}_2 \subset (3)$; inoltre $3 = 9 + (-6)$, da cui l'inclusione opposta e quindi l'uguaglianza. Infine, dato l'omomorfismo $\phi_1 : (a + b\sqrt{-5}) \mapsto [a-b]_3$, otteniamo

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{q}_1 \cong \mathbb{Z}_3,$$

mentre considerando $\phi_2 : (a + b\sqrt{-5}) \mapsto [a+b]_3$ otteniamo

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{q}_2 \cong \mathbb{Z}_3.$$

Ciò significa che $\mathfrak{q}_1$ e $\mathfrak{q}_2$ sono primi e massimali. Analogamente si verifica che

$$(1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{q}_1,$$
$$(1-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{q}_2,$$

da cui si osserva che la fattorizzazione di (6) è effettivamente unica.

**Osservazione 4.2.10.** Nell'esempio precedente, $\mathfrak{p}_1, \mathfrak{q}_1$ e $\mathfrak{q}_2$ sono esempi di ideali non principali; in effetti sappiamo che tali ideali devono esistere nell'anello $\mathbb{Z}[\sqrt{-5}]$, perché esso non è un UFD e quindi neanche un PID.

**Osservazione 4.2.11.** La fattorizzazione ottenuta è anche indipendente dalla scelta di $\theta$, purché rappresenti la stessa estensione.
Consideriamo ad esempio la fattorizzazione dell'ideale (11) in $\mathbb{Z}[1+\sqrt{3}] = \mathbb{Z}[\sqrt{3}]$. Il polinomio minimo di $\theta$ è $f(x) = x^2 - 2x - 2 = 0$, che ridotto mod 11 diventa

$$f(x) \equiv (x-6)(x+4) \bmod 11;$$

di conseguenza la fattorizzazione di (11) è ancora

$$(11) = (11, -5+\sqrt{3})(11, 5+\sqrt{3}) = (1+2\sqrt{3})(1-2\sqrt{3}).$$

Il Teorema 4.2.5 ci permette di lavorare anche con estensioni di $\mathbb{Z}$ non integralmente chiuse considerandole nella loro chiusura integrale.

**Esempio 4.2.12.** Consideriamo $O_{\mathbb{Q}(\sqrt{5})} = \left\{a + b\frac{1+\sqrt{5}}{2}; a, b \in \mathbb{Z}\right\} = \mathbb{Z}[\phi]$, dove $\phi^2 - \phi - 1 = 0$. Possiamo quindi applicare il Teorema 4.2.5.
Fattorizziamo l'ideale (11):

$$f(x) \equiv (x+3)(x+7) \mod 11,$$

da cui otteniamo

$$(11) = (11, \frac{7+\sqrt{5}}{2})(11, \frac{15+\sqrt{5}}{2}).$$

Osserviamo inoltre che

$$11 = \frac{7+\sqrt{5}}{2} \cdot \frac{7-\sqrt{5}}{2},$$

$$MCD(11, \frac{15+\sqrt{5}}{2}) = \frac{1+3\sqrt{5}}{2} = 3 \cdot \frac{15+\sqrt{5}}{2} - 2 \cdot 11 \in (11, \frac{15+\sqrt{5}}{2}).$$

Concludiamo quindi che

$$(11) = (\frac{7+\sqrt{5}}{2})(\frac{1+3\sqrt{5}}{2}).$$

**Osservazione 4.2.13.** Sappiamo che $\mathbb{Z}[\sqrt{5}]$ non è un UFD. In effetti abbiamo che

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

Fattorizziamo ora l'ideale $(4) = (2)(2)$ in $\mathbb{Z}[\phi]$:

$$f(x) = x^2 - x - 1 \bmod 2,$$

quindi $(2)$ è un ideale primo. Questo significa anche che

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

Effettivamente, osservando che $\phi^{-1} = \phi - 1 \in O_K$,

$$2 = (1+\sqrt{5})\phi^{-1},$$

$$1+\sqrt{5} = 2 \cdot \phi,$$

quindi $(2)O_K = (1+\sqrt{5})O_K$. Inoltre $1 \notin (2)$, per cui $(2)$ è effettivamente primo e $\mathbb{Z}[\phi]/(2)$ è un campo.

**Osservazione 4.2.14.** Sapendo che $\mathfrak{p} = (2)$ è un ideale primo in $A = O_{Q(\sqrt{5})} = \mathbb{Z}[\phi]$, studiamo ora la localizzazione $A_\mathfrak{p}$ :

$$A_\mathfrak{p} = \left\{ \frac{a+b\phi}{c+d\phi}, c, d \text{ non entrambi pari} \right\}.$$

Definendo la valutazione $v : \mathbb{Z}[\phi] \to \mathbb{R}$ nella maniera canonica, notiamo che

- $v$ è una valutazione discreta;
- $v(2) = 1$, quindi come ci aspettavamo $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$;
- $v(1+\sqrt{5}) = v(2\phi) = 1$ (poiché $\phi \notin (2)$);
- $v(\phi) = v(1+\sqrt{5}) - v(2) = 1 - 1 = 0 = v(\phi^{-1})$,per cui $\phi$ (e $\phi^{-1}$) appartengono al gruppo delle unità $A_\mathfrak{p} \setminus \mathfrak{p}A_\mathfrak{p}$.

A prima vista può apparire controintuitivo che $\phi$ appartenga al DVR $A_\mathfrak{p}$, poiché effettivamente il suo denominatore è divisibile per 2: in realtà, in base a come abbiamo definito $A_\mathfrak{p}$,

$$\phi = \frac{0 + 1 \cdot \phi}{1 + 0 \cdot \phi} \in A_\mathfrak{p}.$$

La fattorizzazione unica può essere estesa anche agli ideali frazionari. Useremo la seguente notazione: dati $\mathfrak{p}$ e $\mathfrak{q}$ ideali primi

$$\mathfrak{p}/\mathfrak{q} = \frac{\mathfrak{p}}{\mathfrak{q}} := \mathfrak{q}^{-1}\mathfrak{p}.$$

**Teorema 4.2.15.** *Ogni ideale frazionario $\mathcal{M}$ di $O_K$ può essere scritto in maniera unica nella forma*

$$\mathcal{M} = \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_r}{\mathfrak{q}_1 \cdots \mathfrak{q}_s},$$

*dove i $\mathfrak{p}_i$ e i $\mathfrak{q}_j$ sono ideali primi che possono essere ripetuti ma $\mathfrak{p}_i \neq \mathfrak{q}_j$ per ogni $i, j$.*

*Dimostrazione.* Proviamo innanzitutto che tale fattorizzazione esiste. Sia $x \in \mathbb{Z}$ un elemento non nullo tale che $\mathfrak{b} = x\mathcal{M} \subset O_K$. Dal Teorema 4.2.4 possiamo scrivere $(x) = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ e $\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, dove i $\mathfrak{p}_i$ e $\mathfrak{q}_j$ sono ideali primi. Allora

$$\mathcal{M} = \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_r}{\mathfrak{q}_1 \cdots \mathfrak{q}_s}.$$

Cancellando eventuali ideali primi comuni a numeratore e denominatore otteniamo anche che $\mathfrak{p}_i \neq \mathfrak{q}_j$.
Per provare l'unicità consideriamo un'altra fattorizzazione

$$\mathcal{M} = \frac{\mathfrak{a}_1 \cdots \mathfrak{a}_n}{\mathfrak{b}_1 \cdots \mathfrak{b}_m},$$

con $\mathfrak{a}_i \neq \mathfrak{b}_j$. Allora

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n \mathfrak{q}_1 \mathfrak{q}_s = \mathfrak{b}_1 \cdots \mathfrak{b}_m \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Per l'unicità della fattorizzazione di ideali interi, e poiché $\mathfrak{a}_i \neq \mathfrak{b}_j$ e $\mathfrak{p}_i \neq \mathfrak{q}_j$, a meno di permutazioni otteniamo che $\mathfrak{a}_i = \mathfrak{p}_i$ e $\mathfrak{b}_j = \mathfrak{q}_j$ per ogni $i, j$. □

**Osservazione 4.2.16.** La fattorizzazione unica consente di trovare facilmente l'inverso di un ideale frazionario. Dato

$$\mathcal{M} = \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_r}{\mathfrak{q}_1 \cdots \mathfrak{q}_s},$$

si verifica facilmente che definendo

$$\mathcal{M}^{-1} = \frac{\mathfrak{q}_1 \cdots \mathfrak{q}_s}{\mathfrak{p}_1 \cdots \mathfrak{p}_r},$$

$$\mathcal{M}\mathcal{M}^{-1} = O_K.$$

Ritrovando la fattorizzazione in elementi primi, possiamo ridefinire e calcolare il massimo comune divisore di due elementi.

**Definizione 4.2.17.** Ricordiamo che per due ideali $\mathfrak{a}$ e $\mathfrak{b}$, diciamo che $\mathfrak{a}$ *divide* $\mathfrak{b}$ (e scriviamo $(\mathfrak{a}|\mathfrak{b})$ se $\mathfrak{a} \supset \mathfrak{b}$.

**Definizione 4.2.18.** Dati due ideali $\mathfrak{a}$ e $\mathfrak{b}$, diciamo che un ideale $\mathfrak{d}$ è il loro *massimo comune divisore*, $\mathfrak{d} = MCD(\mathfrak{a}, \mathfrak{b})$, se

- $\mathfrak{d}|\mathfrak{a}$ e $\mathfrak{d}|\mathfrak{b}$,
- Se $\mathfrak{e}|\mathfrak{a}$ e $\mathfrak{e}|\mathfrak{b}$ allora $\mathfrak{e}|\mathfrak{d}$.

**Teorema 4.2.19.** *Dati due ideali di $O_K$ e le loro fattorizzazioni in ideali primi $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ e $\mathfrak{b} = \prod_{i=1}^{r} \mathfrak{p}_i^{f_i}$ con $e_i, f_i \in \mathbb{Z}_{\geq 0}$ , esiste ed è unico $\mathfrak{d} = MCD(\mathfrak{a}, \mathfrak{b})$ e vale*

$$\mathfrak{d} = \mathfrak{a} + \mathfrak{b} = \prod_{i=1}^{r} \mathfrak{p}_i^{min(e_i, f_i)},$$

*ovvero si moltiplicano fra loro i fattori primi comuni presi all'esponente più basso.*

*Dimostrazione.* Mostriamo che $\mathfrak{a}+\mathfrak{b}$ soddisfa le due proprietà della definizione di $MCD$.
Banalmente $\mathfrak{a} \subset \mathfrak{a} + \mathfrak{b}$ e $\mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}$, quindi $\mathfrak{a} + \mathfrak{b}|\mathfrak{a}$ e $\mathfrak{a} + \mathfrak{b}|\mathfrak{b}$.
Inoltre, se $\mathfrak{e}|\mathfrak{a}$ e $\mathfrak{e}|\mathfrak{b}$, allora per definizione $\mathfrak{a} \subset \mathfrak{e}$ e $\mathfrak{b} \subset \mathfrak{e}$, quindi $\mathfrak{a}+\mathfrak{b} \subset \mathfrak{e}$, ovvero $\mathfrak{e}|\mathfrak{a} + \mathfrak{b}$.
Mostriamo ora che anche $\mathfrak{d} := \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$, con $a_i = min(e_i, f_i)$ soddisfa le due proprietà della definizione di $MCD$.

$$\begin{aligned}
\mathfrak{a} &= \prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \\
&= \prod_{i=1}^{r} \mathfrak{p}_i^{e_i - a_i} \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \\
&= \prod_{i=1}^{r} \mathfrak{p}_i^{e_i - a_i} \mathfrak{d}, \ e_i - a_i \geq 0 \ \forall i.
\end{aligned}$$

Quindi, $\mathfrak{d} \supset \mathfrak{a}$, da cui $\mathfrak{d}|\mathfrak{a}$. Analogamente si prova che $\mathfrak{d}|\mathfrak{b}$.
Supponiamo ora che $\mathfrak{e} = \prod_{i=1}^{r} \mathfrak{p}_i^{k_i}$ divida $\mathfrak{a}$ e $\mathfrak{b}$. Supponiamo che esista un $i$ per cui $k_i > e_i$ e senza perdere di generalità supponiamo $i = 1$. Sappiamo che $\mathfrak{p}_1^{k_1}|\mathfrak{e}$, quindi $\mathfrak{p}_1^{k_1}|\mathfrak{a}$, ovvero $\mathfrak{p}_1^{k_1} \supset \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Da cui

$$\begin{aligned}
(\mathfrak{p}_1^{-1})^{e_1} \mathfrak{p}_1^{k_1} &\supset \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}, \\
\mathfrak{p}_1 &\supset \mathfrak{p}_1^{k_1 - e_1} \supset \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}, \\
\mathfrak{p}_1 &\supset \mathfrak{p}_j,
\end{aligned}$$

per qualche $j \neq 1$. Ma poiché $\mathfrak{p}_j$ è massimale, $\mathfrak{p}_1 = \mathfrak{p}_j$, ma questo è assurdo. Allora, $k_i \leq e_i$ per ogni $i$ e ogni ideale primo della fattorizzazione di $\mathfrak{e}$ deve essere anche nella fattorizzazione di $\mathfrak{a}$. Analogamente per $\mathfrak{b}$. Allora $k_i \leq min(e_i, f_i)$, per cui $\mathfrak{e}|\mathfrak{d}$. □

**Esempio 4.2.20.** Riprendiamo i calcoli fatti in 4.2.9 per gli ideali di $\mathbb{Z}[\sqrt{-5}]$.

$$MCD((2)O_K, (3)O_K) = (1)O_K = O_K,$$

$$MCD((1+\sqrt{-5})O_K, (-1+\sqrt{-5})O_K) = (2, 1+\sqrt{-5}).$$

Per concludere, mostriamo che possiamo riottenere anche il Teorema Cinese del Resto.

**Teorema 4.2.21.**
- *Siano $\mathfrak{a}$ e $\mathfrak{b}$ due ideali di $O_K$ tali che $MCD(\mathfrak{a}, \mathfrak{b}) = O_K$. Dati $a, b \in O_K$ possiamo risolvere il sistema*

$$\begin{cases} x \equiv a \ mod \ \mathfrak{a} \\ x \equiv b \ mod \ \mathfrak{b}. \end{cases}$$

- *Siano $\mathfrak{p}_1 \cdots, \mathfrak{p}_r$ ideali primi distinti di $O_K$. Dati $a_i \in O_K$ e $e_i \in \mathbb{Z}_{>0}$, esiste $x$ tale che $x \equiv a_i \ mod \ \mathfrak{p}_i^{e_i}$ per ogni $i = 1, \ldots, r$.*

*Dimostrazione.* Poiché $\mathfrak{a} + \mathfrak{b} = O_K$, devono esistere $m \in \mathfrak{a}, n \in \mathfrak{b}$ tali che $m + n = 1$. Sia $x := bm + an$. Allora otteniamo che $x \equiv an$ mod $\mathfrak{a}$, ma $n = 1 - m \equiv 1$ mod $\mathfrak{a}$, quindi concludiamo che $x \equiv a$ mod$\mathfrak{a}$. Analogamente si prova che $x \equiv b$ mod $\mathfrak{b}$.
Per dimostrare il secondo punto, procediamo per induzione sul numero di ideali primi $r$. Se $r = 1$ non c'è nulla da provare. Se invece $r > 1$, supponiamo di risovere $x \equiv a_i$ mod $\mathfrak{p}_i^{e_i}$ per $i = 1, \ldots, r-1$. Dal punto precedente abbiamo che

$$\begin{cases} x \equiv a \text{ mod } \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{r-1}^{e_{r-1}} \\ x \equiv a_r \text{ mod } \mathfrak{p}_r^{e_r} \end{cases},$$

che possiamo risolvere perché gli ideali primi sono tutti distinti, quindi $\mathfrak{p}_1^{e_i} \cdots \mathfrak{p}_{r-1}^{e_{r-1}} + \mathfrak{p}_r^{e_r} = O_K$. Allora $x - a_i \in \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{r-1}^{e_{r-1}}$, $x \equiv a_r$ mod $\mathfrak{p}_r^{e_r}$. Quindi abbiamo provato che $x - a_i \in \mathfrak{p}_i^{e_i} \Leftrightarrow x \equiv a_i$ mod $\mathfrak{p}_i^{e_i}$ per ogni $i$. □

# Capitolo 5

# Il gruppo delle classi di ideali di $O_K$

L'obiettivo principale di questo capitolo è provare la finitezza di $\mathcal{H}$, il gruppo delle classi di ideali di $O_K$.

## 5.1 Norma di elementi in $O_K$

Analogamente alla traccia, definita in 2.2.9, definiamo la norma di un elemento.

**Definizione 5.1.1.** Sia $K$ un campo di numeri algebrici. Dato $\alpha \in K$, definiamo la sua *norma* $N(\alpha) = \det(\Phi_\alpha)$, dove $\Phi_\alpha : K \to K$, $\Phi_\alpha(x) = \alpha x$.

Ricordiamo inoltre la definizione di anello euclideo:

**Definizione 5.1.2.** L'anello $O_K$ è *euclideo* se la norma è tale che, dati $a, b \in O_K$ esistono $q, r \in O_K$ tali che

- $a = bq + r$,
- $|N(r)| < |N(b)|$.

Ovvero, se è possibile definire un algoritmo di divisione euclidea.

In generale, $O_K$ non è euclideo (ad esempio $\mathbb{Z}[\sqrt{-5}]$ non è UFD), ma vale sempre il seguente risultato.

**Lemma 5.1.3.** *Sia dato un campo di numeri algebrici $K$. Esiste una costante $H_K$ tale che dato $\alpha \in K$ esistono $\beta \in O_K$ e un intero $t$ con $|t| \leq H_K$ tali che*

$$N(t\alpha - \beta) < 1.$$

*Tale costante di $K$ è chiamata costante di Hurwitz.*

*Dimostrazione.* Per semplicità di calcoli, dimostriamo il lemma solo nel caso di un'estensione quadratica, considerando $(1, \theta)$ come base integrale di $O_K$. Dato $\alpha \in K$ possiamo trovare $m \in \mathbb{Z}$ tale che $m\alpha \in O_K$, e quindi possiamo scrivere

$$\alpha = c_1 + c_2\theta,$$

con $c_1, c_2 \in \mathbb{Q}$.
Consideriamo il più piccolo intero positivo $L$ tale che

$$L > 1 + |\theta|.$$

Mostriamo che $L^2$ è una costante che soddisfa tale proprietà, e quindi una stima per eccesso di $H_K$.
Dividiamo l'intervallo $[0, 1]$ in $L$ sottointervalli di lunghezza $\frac{1}{L}$: questo induce una suddivisione del quadrato $[0, 1]^2$ in $L^2$ sottoquadrati. Consideriamo la funzione

$$\phi : \alpha\mathbb{Z} \to [0, 1]^2,$$

definita da $\phi : t\alpha \mapsto (\{tc_1\}, \{tc_2\})$, dove $t$ è un intero e $\{x\} = x - \lfloor x \rfloor$ è la parte frazionaria di $x$. Assegniamo a $t$ valori da 0 a $L^2$ (così da avere $L^2 + 1$ valori distinti per $t$ con $|t| < L^2$); per il principio della piccionaia, devono esistere due valori distinti $t_1, t_2$ tali che $t_1\alpha$ e $t_2\alpha$ sono nello stesso sottoquadrato e quindi

$$|\{t_1c_i\} - \{t_2c_i\}| < \frac{1}{L}, \text{ per } i = 1, 2.$$

Sia

$$\beta = (\lfloor t_1c_1 \rfloor - \lfloor t_2c_2 \rfloor) + (\lfloor t_1c_2 \rfloor - \lfloor t_2c_2 \rfloor)\theta,$$

così che, posto $t = t_1 - t_2$,

$$\begin{aligned} |N(t\alpha - \beta)| =& |N((\{t_1c_1\} - \{t_2c_1\}) + (\{t_1c_2\} - \{t_2c_2\})\theta)| \\ \leq& |(\{t_1c_1\} - \{t_2c_1\})^2 - (\{t_1c_2\} - \{t_2c_2\})^2\theta^2)| \\ \leq& \frac{1}{L^2} + \frac{1}{L^2}|\theta^2| = \frac{1 + |\theta^2|}{L^2} < \frac{1 + |\theta|^2}{(1 + |\theta|)^2} < 1. \end{aligned}$$

□

**Osservazione 5.1.4.** Generalizzando a un'estensione di grado $n$ con base integrale $(\omega_1, \ldots, \omega_n)$, si può considerare $L$ il più piccolo intero positivo tale che

$$L^n > \prod_{j=1}^{n} (\sum_{i=1}^{n} |\omega_i^{(j)}|),$$

dove $\omega_i^{(j)}$ indica come al solito l'immagine di $\omega_i$ tramite il $j$-esimo isomorfismo $\sigma$ dell'estensione $\mathbb{Q} \subset K$.

**Osservazione 5.1.5.** Usando basi integrali diverse si ottengono diverse stime $L^n$ di $H_K$, dove ovviamente più $L$ è piccolo, migliore è la stima. Noi porremo $H_K = \prod_{j=1}^{n}(\sum_{i=1}^{n} |\omega_i^{(j)}|)$ come definito nell'Osservazione 5.1.4.

**Esempio 5.1.6.** Consideriamo $K = \mathbb{Q}(\sqrt{2})$. Sia $L = 3 > 1 + \sqrt{2}$, quindi $H_K < 9$. Sia $\alpha = \frac{3+2\sqrt{2}}{5+\sqrt{2}}$, che può essere scritto come $\alpha = \frac{11}{23} + \frac{7}{23}\sqrt{2}$. Osserviamo che per $t_1 = 8$ e $t_2 = 2$, $(\{t_1c_1, t_1c_2\}), (\{t_2c_1, t_2c_2\}) \in [\frac{2}{3}, 1]\times[\frac{1}{3}, \frac{2}{3}]$. Allora imponendo $\beta = (\lfloor 8c_1 \rfloor - \lfloor 2c_1 \rfloor) + (\lfloor 8c_2 \rfloor - \lfloor 2c_2 \rfloor)\sqrt{2} = 3 + 2\sqrt{2}$, otteniamo

$$\begin{aligned} |N(t\alpha - \beta)| =& |N((\frac{66}{23} + \frac{42}{23}\sqrt{2}) - (3 + 2\sqrt{2}))| \\ =& |N(-\frac{3}{23} - \frac{4}{23}\sqrt{2})| = |\frac{9}{529} - \frac{32}{529}| \\ =& |-\frac{1}{23}| < 1. \end{aligned}$$

**Corollario 5.1.7.** *Dati $\alpha, \beta \in O_K$, esistono $t \in \mathbb{Z}, |t| \leq H_K$ e $\omega \in O_K$ tali che $|N(\alpha t - \beta\omega)| < |N(\beta)|$.*

*Dimostrazione.* Applicando il Lemma 5.1.3 sostituendo $\alpha$ con $\alpha/\beta$, concludiamo che esiste $t \in \mathbb{Z}, |t| \leq H_K$ e $\omega \in O_K$ tali che

$$|N(t\alpha/\beta - \omega)| < 1,$$

da cui concludiamo che $|N(t\alpha - \omega\beta)| < |N(\beta)|$. □

## 5.2 Norma di ideali in $O_K$

In questa sezione estendiamo la definizione di norma agli ideali. Come nel caso della norma di un elemento, la norma di un ideale ci dà indicazioni sulla "grandezza" dell'ideale e sulla sua divisibilità per altri ideali.

**Definizione 5.2.1.** Sia $\mathfrak{a}$ un ideale di $O_K$. Definiamo la sua *norma* come

$$N(\mathfrak{a}) = |O_K/\mathfrak{a}|,$$

oppure $N(\mathfrak{a}) = 0$ se $\mathfrak{a} = 0$.

**Teorema 5.2.2.** *Siano $\mathfrak{a} \subsetneq \mathfrak{b}$ ideali di $O_K$. Allora $N(\mathfrak{a}) > N(\mathfrak{b})$.*

*Dimostrazione.* Definiamo una funzione

$$\phi : O_K/\mathfrak{a} \to O_K/\mathfrak{b},$$

come $\phi([x]_{\mathfrak{a}}) = [x]_{\mathfrak{b}}$. Tale funzione non è iniettiva, poiché dato $y \in \mathfrak{b} - \mathfrak{a}$,

$$[y]_{\mathfrak{a}} \neq 0,\ \phi([y]_{\mathfrak{a}}) = 0.$$

Allora, poiché entrambi sono insiemi finiti, $|O_K/\mathfrak{b}| < |O_K/\mathfrak{a}|$, da cui la tesi. □

**Teorema 5.2.3.** *La norma di ideali è moltiplicativa. Ovvero, dati due ideali* $\mathfrak{a}$ *e* $\mathfrak{b}$*,*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

*Dimostrazione.* Consideriamo $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ e verifichiamo che

- $N(\mathfrak{a}) = \prod_{i=1}^{r} N(\mathfrak{p}_i^{e_i})$,
- $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$ per ogni $e \geq 0$.

Quindi vogliamo mostrare che la norma è moltiplicativa per prodotti e potenze di ideali primi; infatti se questo è vero possiamo concludere per l'unicità della fattorizzazione.

- Esaminiamo il caso $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$ (la dimostrazione può essere generalizzata con un procedimento induttivo). Consideriamo

  $$\begin{aligned} \phi : O_K &\to O_K/\mathfrak{p}_1^{e_1} \oplus O_K/\mathfrak{p}_2^{e_2} \\ x &\mapsto (x_1, x_2), \end{aligned}$$

  dove $x_i \equiv x \bmod \mathfrak{p}_i^{e_i}$. La funzione è suriettiva per il teorema cinese del resto. Inoltre, $Ker(\phi) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} = \mathfrak{a}$.

- Sia $\mathfrak{p}^e \subsetneq \mathfrak{p}^{e-1}$ e sia $\alpha \in \mathfrak{p}^{e-1} \setminus \mathfrak{p}^e$, quindi $\alpha \in \mathfrak{p}^{e-1}, \alpha \notin \mathfrak{p}^e$. Allora $\mathfrak{p}^e \subset (\alpha) + \mathfrak{p}^e \subset \mathfrak{p}^{e-1}$. Quindi $\mathfrak{p}^{e-1} | (\alpha) + \mathfrak{p}^e$. Poiché $(\alpha) + \mathfrak{p}^e \neq \mathfrak{p}^e$, $\mathfrak{p}^{e-1} = (\alpha) + \mathfrak{p}^e$, per la fattorizzazione unica. Sia ora

  $$\begin{aligned} \phi : O_K &\to \mathfrak{p}^{e-1}/\mathfrak{p}^e \\ \gamma &\mapsto \gamma\alpha \mod \mathfrak{p}^e, \end{aligned}$$

  un omomorfismo suriettivo. Osserviamo che $\gamma \in Ker(\phi) \Leftrightarrow \gamma\alpha \in \mathfrak{p}^e \Leftrightarrow \gamma \in \mathfrak{p}$, poiché $\alpha \in \mathfrak{p}^{e-1} \setminus \mathfrak{p}^e$ e $\mathfrak{p}$ è primo. Allora

  $$O_K/\mathfrak{p} \cong \mathfrak{p}^{e-1}/\mathfrak{p}^e.$$

  Ora,

  $$\begin{aligned} N(\mathfrak{p}^2) =& |O_K/\mathfrak{p}^2| \\ =& |O_K/\mathfrak{p}||\mathfrak{p}/\mathfrak{p}^2| \\ =& |O_K/\mathfrak{p}||O_K/\mathfrak{p}| \\ =& N(\mathfrak{p})^2, \end{aligned}$$

  e il processo si generalizza facilmente per induzione.

□

La definizione di norma può essere estesa agli ideali frazionari nel seguente modo.

**Definizione 5.2.4.** Sia $\mathcal{M}$ un ideale frazionario. Per l'unicità della fattorizzazione esso può essere scritto in maniera unica come $\mathcal{M} = \frac{\mathfrak{a}}{\mathfrak{b}} = \mathfrak{a}\mathfrak{b}^{-1}$ con $\mathfrak{a}$ e $\mathfrak{b}$ ideali interi che non hanno fattori primi comuni. Definiamo

$$N(\mathcal{M}) = \frac{N(\mathfrak{a})}{N(\mathfrak{b})}.$$

La definizione è ben posta: considerati due generici ideali interi $\mathfrak{c}$ e $\mathfrak{d}$ tali che $\mathcal{M} = \mathfrak{c}\mathfrak{d}^{-1}$, per la moltiplicatività della norma $\frac{N(\mathfrak{c})}{N(\mathfrak{d})} = \frac{N(\mathfrak{a})}{N(\mathfrak{b})}$.

## 5.3 Finitezza di $\mathcal{H}$

Una delle conseguenze più importanti del teorema di fattorizzazione unica in ideali primi è che per ogni anello degli interi algebrici, il gruppo delle classi di ideali è finito.

**Definizione 5.3.1.** Diamo la seguente relazione di equivalenza: dati due ideali frazionari $\mathcal{M}$ e $\mathcal{N}$ di $K$, essi appartengono alla stessa *classe di ideali*, e scriviamo $\mathcal{M} \sim \mathcal{N}$, se esistono $\alpha, \beta \in O_K$ tali che

$$(\alpha)\mathcal{M} = (\beta)\mathcal{N}.$$

**Osservazione 5.3.2.** In un anello di interi algebrici, il quoziente del gruppo degli ideali frazionari $\mathcal{I}$ rispetto a questa relazione di equivalenza è effettivamente il gruppo delle classi di ideali $\mathcal{H}$ definito in 4.1.16.

**Definizione 5.3.3.** Su $\mathcal{H}$ possiamo definire il seguente *prodotto*: dati $\mathcal{C}_1$ e $\mathcal{C}_2$ in $\mathcal{H}$, il loro prodotto è la classe di equivalenza di $\mathcal{M}\mathcal{N}$, dove $\mathcal{M}$ e $\mathcal{N}$ sono due rappresentanti di $\mathcal{C}_1$ e $\mathcal{C}_2$, rispettivamente. Effettivamente $\mathcal{H}$ dotato di questo prodotto è un gruppo moltiplicativo, dove l'identità è la classe di equivalenza degli ideali principali.

**Teorema 5.3.4.** *Ogni classe di ideali ha un rappresentante intero.*

*Dimostrazione.* Sia $\mathcal{M} = \frac{\mathfrak{a}}{\mathfrak{b}}$ un ideale frazionario di $K$, con $\mathfrak{a}, \mathfrak{b} \subset O_K$. Da 2.2.39, sappiamo che esiste $z \in \mathfrak{b} \cap \mathbb{Z}$, per cui $\mathfrak{b} \supset (z) \Rightarrow \mathfrak{b} | (z)$. Questo implica che esiste un ideale intero $\mathfrak{c} \subset O_K$ tale che

$$\mathfrak{b}\mathfrak{c} = (z).$$

Allora,

$$(z)\mathcal{M} = (z)\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\mathfrak{bca}}{\mathfrak{b}} = \mathfrak{ca} \subset O_K.$$

Quindi $\mathcal{M} \sim \mathfrak{ca} \subset O_K$. □

**Osservazione 5.3.5.** Il Teorema 5.3.4 fornisce anche un procedimento per calcolare esplicitamente l'inverso di una classe $\mathcal{C} \subset \mathcal{H}$. Sia $\mathfrak{a} \subset O_K$ rappresentante intero della classe $\mathcal{C}$; allora, deve esistere un intero $z$ e un ideale intero $\mathfrak{b}$ tale che $\mathfrak{ab} = (z)$ e quindi è principale. Quindi, la classe che contiene $\mathfrak{b}$ è l'inverso di $\mathcal{C}$.

**Teorema 5.3.6.** *Dato un campo di numeri algebrici $K$, esiste una costante $C_K$ tale che ogni ideale $\mathfrak{a} \subset O_K$ è equivalente a un ideale $\mathfrak{b} \subset O_K$ con $N(\mathfrak{b}) \leq C_K$.*

*Dimostrazione.* Sia $\mathfrak{a}$ un ideale di $O_K$ e sia $0 \neq \beta \in \mathfrak{a}$ tale che $|N(\beta)|$ sia minima. Per il Corollario 5.1.7, per ogni $\alpha \in \mathfrak{a}$ possiamo trovare $t \in \mathbb{Z}, |t| < H_K$ e $\omega \in O_K$ tali che

$$|N(t\alpha - \omega\beta)| < |N(\beta)|.$$

Inoltre, poiché $\alpha, \beta \in \mathfrak{a}$, allora $(t\alpha - \omega\beta) \in \mathfrak{a}$ e per minimalità di $|N(\beta)|$ concludiamo che $t\alpha = \omega\beta$. Se ora poniamo

$$M = \prod_{|t| \leq H_K} t,$$

otteniamo che $M\mathfrak{a} \subset (\beta)$, per cui $(\beta)|M\mathfrak{a}$, quindi esiste $\mathfrak{b} \subset O_K$ tale che

$$(M)\mathfrak{a} = (\beta)\mathfrak{b}.$$

Osservando che $\beta \in \mathfrak{a}$, $M\beta \in (\beta)\mathfrak{b}$, per cui $(M) \subset \mathfrak{b}$.
Se quindi poniamo $C_K = N((M))$, abbiamo che per ogni ideale $\mathfrak{a}$, esiste $\mathfrak{b}$ tale che $\mathfrak{a} \sim \mathfrak{b}$ e $|N(\mathfrak{b})| \leq C_K$. □

**Lemma 5.3.7.** *Sia $x$ un intero positivo. La famiglia di ideali*

$$\{\mathfrak{a} \subset O_K \text{ tali che } N(\mathfrak{a}) \leq x\}$$

*è finita.*

*Dimostrazione.* Dimostriamo che il lemma vale per gli ideali primi. Per 2.2.40, ogni ideale primo $\mathfrak{p}$ contiene esattamente un primo $p \in \mathbb{Z}$, quindi $\mathfrak{p}$ è un ideale primo nella fattorizzazione di $(p) = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$; inoltre, $N(\mathfrak{p}) = p^t$

per un certo intero $t \geq 1$ (perché $O_K/\mathfrak{p}$ è un campo). In effetti gli ideali primi di norma $p^t$ sono tutti e soli gli ideali primi che compaiono nella fattorizzazione di $(p)$. Allora, $N((p)) = \prod_{i=1}^{r} N(\mathfrak{p}_i)^{e_i} = p^n$ per un certo $n$ con $r \leq n$. Questo significa che il numero di ideali $r$ di norma $p^t$ è finito, e allora dato un intero positivo $x$, anche il numero di ideali primi di norma minore o uguale a $x$ è finito.
Se ora generalizziamo a tutti gli ideali interi, per mostrare che il risultato vale basta considerare la fattorizzazione in ideali primi e osservare che la norma di ideali è moltiplicativa. □

Questo ultimo risultato ci permette infine di dimostrare il teorema di finitezza delle classi.

**Teorema 5.3.8.** *Il numero delle classi di equivalenza di ideali in un anello di interi algebrici è finito.*

*Dimostrazione.* Per il Teorema 5.3.4 ogni classe di ideali ha un rappresentante intero. Questo ideale intero, per il Teorema 5.3.6, è equivalente a un altro ideale intero di norma minore o uguale a una certa costante $C_K$. Concludiamo infine per il Lemma 5.3.7. □

**Definizione 5.3.9.** Dato un campo di numeri algebrici $K$, definiamo il suo *numero delle classi* $h(K) = |\mathcal{H}|$.

Si può dimostrare che possiamo prendere come stima della costante $C_K$ di 5.3.6 il più grande intero positivo minore o uguale a $H_K$. Questo ci permette di calcolare il numero delle classi di alcuni campi di numeri algebrici.

**Esempio 5.3.10.** Calcoliamo il numero delle classi di $K = \mathbb{Q}(\sqrt{-5})$. Utilizzando l'Osservazione 5.1.4 e usando come base integrale $(1, \sqrt{-5})$ otteniamo che $H_K = (1 + \sqrt{-5})^2$ e quindi $C_K = 10$. Quindi, ogni classe di ideali $\mathcal{C} \in \mathcal{H}$ ha un rappresentante intero $\mathfrak{a}$ con $N(\mathfrak{a}) \leq 10$. Supponiamo che la fattorizzazione di $\mathfrak{a}$ sia $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, con $\mathfrak{p}_i$ ideali primi di $O_K$.
Consideriamo $\mathfrak{p}_1$ e l'unico primo $p \in \mathfrak{p} \cap \mathbb{Z}_{\geq 0}$. Allora $\mathfrak{p}_1 | (p)$ e quindi $N(\mathfrak{p}_1)$ è una potenza di $p$. Osserviamo che $N(\mathfrak{a}) + \prod_{i=1}^{n} N(\mathfrak{p}_i) \leq 10$, quindi $N(\mathfrak{p}_i) \leq 10$ per ogni $i$ ( e in particolare per $i = 1$. Allora, $p \leq 10$, quindi le uniche opzioni sono $p = 2, 3, 5$ oppure 7. Riprendiamo i calcoli dell'Esempio 4.2.9 e otteniamo che

$$\begin{aligned}
(2) &= (2, 1 + \sqrt{-5})^2, \\
(3) &= (3, 1 + \sqrt{-5})(3, -1 + \sqrt{-5}), \\
(5) &= (\sqrt{-5})^2, \\
(7) &= (7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5}).
\end{aligned}$$

Ne segue che $\mathfrak{p}_1$, e quindi anche ogni ideale primo $\mathfrak{p}_i$, deve essere uguale a uno degli ideali primi che compaiono in queste fattorizzazioni. Osserviamo che $(\sqrt{-5})$ è principale e quindi è un rappresentante intero della classe delle unità di $\mathcal{H}$, mentre tutti gli altri non lo sono, ma in effetti

$$\begin{aligned}(3, 1+\sqrt{-5})(1-\sqrt{-5}) =&(3)(2, 1+\sqrt{-5}),\\ (3, -1+\sqrt{-5})(1+\sqrt{-5}) =&(3)(2, 1+\sqrt{-5}),\\ (7, 3+\sqrt{-5})(3-\sqrt{-5}) =&(7)(2, 1+\sqrt{-5}),\\ (7, 3-\sqrt{-5})(3+\sqrt{-5}) =&(7)(2, 1+\sqrt{-5}),\end{aligned}$$

quindi sono tutti equivalenti fra loro. Allora, un ideale $\mathfrak{a}$ è principale o appartiene alla classe di questi ideali primi. Per cui concludiamo che $h(K) = 2$.

**Esempio 5.3.11.** Consideriamo $K = \mathbb{Q}(\sqrt{3})$. Con calcoli analoghi si ottiene $C_K = 7$ e

$$\begin{aligned}(2) =&(1+\sqrt{3})^2,\\ (3) =&(\sqrt{3})^2,\end{aligned}$$

mentre (5) e (7) sono già primi. Tutti gli ideali sono principali, quindi $h(K) = 1$. In effetti $\mathbb{Z}[\sqrt{3}]$ è un PID, quindi avremmo potuto semplicemente osservare che ogni ideale frazionario è equivalente ad un ideale intero, e quindi principale.

**Esempio 5.3.12.** Consideriamo $\mathbb{Q}(\sqrt{5})$ e $O_K = \mathbb{Z}[\phi]$, dove $\phi^2 - \phi - 1 = 0$. Osserviamo che $H_K = (1 - |\frac{1+\sqrt{5}}{2}|)(1 + |\frac{1-\sqrt{5}}{2}|) = 3 + \sqrt{5}$. Allora $C_K = 5$. Poiché (2) e (3) sono ideali primi e $(5) = (\sqrt{5})^2$, otteniamo che $h(K) = 1$.

# Bibliografia

[1] Atiyah-MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley 1969.

[2] Esmonde-Murty, *Problems in Algebraic Number Theory*, Springer 1999.

[3] Artin, *Algebra*, Prentice-Hall 1991.